ID Register: 52431421-12

Telefónica Comments on EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles

On 28 January 2020, EDPB adopted a set of **Guidelines on processing personal data in the context of connected vehicles and mobility related applications** and invited interested stakeholders to present comments. Telefónica welcomes this opportunity to comment on these draft guidelines and stresses the importance of clear rules and uniform interpretation in order to ensure trust of individuals and data subjects.

As EDPB acknowledges, connected vehicles generate increasing amounts of data. This data is processed in a complex ecosystem, not limited to the traditional automotive industry but to many other players such as e-communications network and service providers, road infrastructure managers, infotainment providers, manufacturers, insurance companies, etc. In this complex ecosystem, well established data protection principles need to be re-assessed as they cannot be automatically applied like in a more simple B2C environment. Connected vehicles is a good touchstone for a future proof, modern and technologically neutral regulation which must provide ready to go and practical answers while ensuring privacy, applicable in different and complex environments such as that.

With the following comments Telefónica wishes to provide some clarifications on some elements raised by the draft EDPB Guidelines in order to reach a balanced text, that provides real guidance for DPAs, industry and citizens.

Specific comments

Issue of consent

Telefónica believes that the draft Guidelines put **too much focus on consent** as the sole legal ground for processing personal data derived from connected vehicles. This is due to the assumption that a connected car is a "terminal equipment", thus Article 5.3. (the Cookie Rule) of the ePrivacy Directive 2002/58/EC applies.

- However, the outdated ePrivacy Directive is in process of being reviewed for more than 3 years to adapt to the quick changes of the technological development. In the actual all-connected paradigm, everything will be suitable to be connected to the

network so, everything will be deemed to be a terminal equipment, and then subject to a rule designed for a very different case such as cookies in Internet. EDPS Guidelines should then consider relying on principles set forth by the GDPR such as the risk-based approach and the flexible applicability of the most suitable legal processing ground for the concrete case. It could happen then that the forced application of the ePrivacy Directive to the case will be outdated once the future ePrivacy rules enter into force, conditioning and hampering innovation in the interim period.

- In parallel, Paragraph 14 of the draft Guidelines requires that in addition to Article 5.3. ePrivacy Directive, any processing of personal data obtained by accessing information in the terminal equipment must additionally have a legal ground under Article 6 GDPR. This is very confusing, as EDPB seems to require 2 legal grounds for processing, based on Art.5.3 ePD and Art.6 GDPR.

- When EDPB refers to consent, given the different daily situations where such consent should then apply, it is not clear to whom the request for consent will be addressed and how the service providers identify and distinguish between car driver's, passengers', car owner's personal data. In a B2B2C environment like connected cars, there will be multiple service providers (data controllers and data processors) and multiple data subjects.

- EDPB reminds that consent must be easily withdrawn. Indeed, a personal data processing based on consent must be easily withdrawn. However, implementation of consent and its correspondent withdrawal will be operationally ineffective and unpractical to fit in a complex ecosystem such as connected cars.

- The EDPB guidelines contradict themselves when developing on use cases where it is mentioned that performance of contract (Article 6.1.b. GDPR) can be considered the relevant legal ground and this "*would not have the effect of lowering the additional protection provided by Article 5.3. ePrivacy Directive*" (Paragraph 106). Telefónica cannot agree more. However, it is important here to stress that consent does not provide "*additional protection*", much on the contrary. GDPR already provides important safeguards regarding information, transparency, right to object, possibility to withdraw consent at any time, the need for Privacy Impact Assessments and finally heavy sanctions for infringing companies. The current ePrivacy Directive is based on the wrong assumption that consent provides better protection for the data subject independently of the concrete use case. The proposed ePrivacy Regulation maintains the same wrong approach ("*consent is a better legal ground than any other GDPR legal ground*"). This implies that trying to be even more protective for consumers, the future ePrivacy Regulation will have a negative effect on European consumers and citizens, creating "consent fatigue", as with cookies consent, thus, lack of protection, reducing the ability for European industry to create the best in class products for them.

Connected cars is a clear example, where "consent" cannot be the legal ground of reference. Other legal grounds present in GDPR, like "performance of contract" or "legitimate interest" are more valid legal grounds in complex ecosystems.

Compatible Further Processing

EDPB considers that GDPR's principle of **Compatible Further Processing** is not possible in a context of connected vehicles "since it would undermine the data protection standard of the ePrivacy Directive".

GDPR introduced the principle of Compatible Further Processing as a way to balance high privacy protection and Big Data innovation. In the context of connected cars, where all is about data, compatible further processing really finds its *reason d'être.*

Regarding the possibility to apply the principle of Compatible Further Processing, again, the same arguments as above should be repeated. By no means, GDPR risk based approach could undermine the privacy standard of the outdated ePrivacy Directive. Much on the contrary, GDPR, its legal grounds for processing personal data, its risk-based approach, the innovative principle of compatible further processing, all these elements provide strong privacy protection that can adapt to emerging technologies and new uses of data, especially where they are bringing real benefits for individuals and society at large, like connected vehicles. GDPR embedded risk-based approach allows for consideration of risks and harms to individuals and to calibrate compliance based on these risks and harms.

Cloud

EDPB considers data stored in the cloud may not be adequately secured and recommends local data processing whenever possible to mitigate risks of cloud computing. To substantiate this argument, EDPB refers to an old Article 29 WP Opinion on Cloud Computing dated 2012.

Telefónica considers this reference to Cloud alarmist and erroneous. Cloud can be so secure or insecure as any other storage in-site. Cloud providers are subject to GDPR and have to comply with its provisions, in their different roles as data controllers or data processors.

It is a fact that Europe is too dependent of US-based big Cloud providers. This is why the Commission in its recent Digital Package and its Data Strategy released on 19th February is calling for a European Cloud federation, stimulating interconnection of currently fragmented public and private Cloud capacities in Europe and fostering synergies with already ongoing Member States' initiatives such as Gaia-X. These are right steps to counterbalance this over-dependence on non-EU based Cloud providers. On the

contrary, EDPB simple and wrong assumption “Cloud is not secure” is misleading and is going against all efforts done to make European citizens confident in digital.

EU Data Strategy

Furthermore, it is necessary to raise the question on how EDPB Guidelines will fit within the ambitious European Data Strategy. The aim of the Data Strategy is to create a genuine single market for data, personal and non-personal data, where public and private sectors can access huge amounts of high-quality data to boost growth and create value. Mobility, and in particular automotive sector, is one of the strategic sectors identified and is at the forefront of the debate on data sharing. Can this ambition happen based on a narrow “consent requirement” for any kind of processing of personal data within connected cars? EDPB Guidelines force organisations to revert to consent, even when this is not appropriate and creates consent fatigue for individuals. This approach is unrealistic in a data-driven society and economy and not in line with GDPR.

By 2025, the vast majority of data will not be created by humans, but by objects and machines, what we call the Internet of Things. These objects, smart sensors in our cities, hospitals, factories or connected vehicles, will create nearly 90% of total data. This is a huge potential source of growth for Europe, which has the largest industrial market in the world, with leading players, particularly in the 4.0 industry. This potential processing should not rely exclusively on the outdated Cookie Rule set out in the ePrivacy Directive.

If we want Europe to become a global data hub for data, both personal and industrial, benefiting all European economic players – SMEs, start-ups, large groups – and, more importantly, all European citizens, we need a flexible and risk-based approach to any data personal processing that grants data controllers a margin of appreciation of the safeguards and the mitigation measures to take following an assessment of the risks for individuals. Accountability is a key principle of GDPR and ensures that the framework remains future-proof, does not hinder innovation and guarantees high level of privacy protection for individuals.

Concluding remarks

EDPB Guidelines are misleading as they start by the assumption that a connected car is considered a terminal equipment, thus ePrivacy Directive applies. This is all correct, but it shows how a sector-specific ePrivacy Directive is not able to respond to technological developments and challenges.

The idea that consent is the only and best way to ensure that individuals’ rights are protected is questionable. While consent can be appropriate in many instances, connected cars is a clear example where consent shows its strong limitations due to complex relations B2B2C. Overreliance on consent can lead to “consent fatigue”, thus rendering poor privacy outcomes for individuals. Asking users to continuously evaluate

notices and provide consent shifts responsibility from service providers to users, which may undermine and potentially even weaken the notion of consent. A telecom provider is accountable for ensuring that any data processing is being conducted in a lawful manner, and documenting and demonstrating that accountability, all against the backdrop of potential enforcement and significant fines.

Under the impression “ePrivacy Directive provides more protection”, it is the contrary as outdated ePrivacy rules are unable to reach a balance between high privacy protection and data innovation. Other legal grounds such legitimate interest and performance of contract are better fit to achieve such balance. However, both do not exist so far in ePrivacy Directive.

Therefore, EDPB should look at GDPR only, not only for car manufacturers, but also for other stakeholders, e-communications providers, entertainment providers, road infrastructure managers, insurance companies, etc. GDPR Risk Based Approach plays an important role, leaving the data controller the assessment on whether any data should be processed or not, depending on the context, the purpose and the scope. For this, in a connected cars environment, consent is not a sustainable option, but other legal grounds such GDPR’s Legitimate Interest are necessary.

19 March 2020