HERE Comments on EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications

HERE Technologies is a worldwide leading provider of location data and services, headquartered in the EU. From high-definition maps for automated driving, to our open B2B Platform, designed to enable data exchange and foster innovation, HERE is a fully data-driven company. Our innovations have led the development and deployment of advanced connected and automated vehicles solutions. Today, 100 million vehicles are equipped with HERE systems (4 of 5 vehicles on European and North American roads). With HERE, journeys become faster, more efficient and safer; fleets optimize deliveries; supply chains become more predictable; and services become location intelligent. Our vision is to create an autonomous world for everyone, by facilitating the exchange of data as a critical prerequisite for innovation, future business models, societal well-being and economic growth at global scale.

On 7 February 2020 the European Data Protection Board (EDPB) opened a public consultation on Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. These guidelines include recommendations specifically in the context of connected vehicles as well as a sample of case studies relevant for the policy area of privacy protection considering applicable EU law. HERE is fully committed to respect privacy and ensure data protection and look forward to the EDPB future revision of these guidelines based on stakeholders' input.

HERE welcomes the approach from EDPB to work through a transparent process of public consultation and considers appropriate to refer to best practice on privacy-by-design and data protection impact assessments. We generally agree that the EDPB guidelines are necessary as data processing is taking place in a complex ecosystem, which is not limited to the traditional players of the automotive industry, but also shaped by the emergence of new players belonging to the digital economy. Due to the increasing amounts of data being processed in the context of connected vehicles and mobility related applications, guidelines are especially helpful to ensure common understandings of the rights and obligations placed on each actor in the ecosystem, from automotive manufacturers, suppliers to service providers and end-users.

However, we do believe that some assumptions are ill-suited to the demands of Europe's emerging digital and mobility infrastructure. If the current draft refers to the existing e-privacy Directive, we consider that formal publication of the guidelines should also be considered in the light of the proposed e-privacy regulation. Indeed, when it comes to connected vehicles, we are particularly concerned by the interplay between GDPR and ePrivacy Directive while a GDPR review is foreseen and a new draft ePrivacy Regulation is under discussion. The risk being to have outdated guidelines very soon, if published in their current form.

Moreover, some of the proposed requirements risk running against the recently launched EU Data Strategy, and thereby hamper innovation and have a negative impact on the current functioning and further development of location services in Europe.

Also, we do call for consistency with guidelines from National Data Protection Authorities (DPAs). Several member States, like in Germany and France, have already issued guidelines on the processing of personal data in the context of connected vehicles. While we welcome the objective to have harmonized EU-wide guidelines, we regret the disparity between both.

This paper highlights issues that are of particular concern to HERE Technologies.

1. Consent management

HERE Technologies believes that the current consent scheme provided by the General Data Protection Regulation (GDPR), to which these guidelines refer to, which requires an informed consent related to specific processing operations, is ill-suited to the demands of Europe's emerging digital and mobility infrastructure. Consent plays an important role but is neither the only nor the default legal ground. It should hence not be emphasised as the primary legal basis for processing, nor should the other legal bases be interpreted and applied as exceptions or in an unreasonably narrow way. We urge the Commission to undertake a broader assessment of consent and the other legal bases as part of its evaluation of the GDPR's effective implementation.

In the dynamic and multi-actor environments of machine to machine (M2M), vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications, the current consent scheme will prove too static and cumbersome. Accordingly, it threatens to be an obstacle to realizing the overwhelmingly positive impact of these and other technologies on society. Also, it is of utmost importance to re-consider the requirements for a valid consent in a manner that would also enable fast-paced multi-actor data transactions in context of M2M, V2V and V2I.

The granting of consent is a crucial part of mastering relationships with individuals. The provisions on granting consent as proposed in the e-Privacy revision– referring to GDPR – do not, however, sufficiently take into account the specific complexities of data management in relation to M2M, V2V and V2I in a road traffic and mobility context. In particular, HERE would like to emphasize the practical impossibility of obtaining valid consents for collecting and processing personal data, as prescribed by the GDPR, in connected vehicle scenarios. Communication in such scenarios will invariably involve high-frequency data transfers between multiple, and in many cases, previously unknown, actors.

Consider, for example, an individual end-user is driving his or her car while making use of location services. In such a scenario, multiple actors which are unknown to the driver, such as other cars (V2V) or infrastructure parts (V2I), transmit and receive numerous data sets in split-seconds. This makes it practically impossible for the individual driver to grant consent, on a truly informed basis, each time before the data are processed.

Furthermore, it is neither feasible nor sensible to provide individuals with just-in-time choices in scenarios as this could significantly reduce safety. Safety functions in vehicles, especially those in highly automated vehicles, increasingly require high-frequency data communication between a vehicle and multiple other actors. Just-in-time notices could distract the driver, overloading him or her with multiple simultaneous requests to provide consent. This would pose safety risks to the driver and other road users.

Under the GDPR, consent must be related to specific processing operations. A general broad consent is invalid, which makes it impossible to obtain valid consent for processing personal data in V2V scenarios with high-frequency communication between multiple actors. This would include for example location data in real-time which would presumably be in the individual's best interest.

In that regard, HERE Technologies would like to underline that the WP29 UNECE acknowledges that consent from end-users is not workable in the context of self-driving cars and other devices and recommends the introduction of a specific exception allowing objects such as self-driving cars and devices to warn each other about their vicinity or other risks.

HERE Technologies asks for workable concepts for granting consent, in these guidelines and under the GDPR as well as the proposed ePrivacy Regulation. These should take into account the specific circumstances of M2M exchange of data in the mobility context (V2V and V2I), which is characterized by multiple unknown actors communicating among each other with high-frequency. The obtaining of consent at the device configuration stage is seen as an ideal solution to help ensure a user-friendly process. HERE Technologies proposes the same approach in the context of V2V and V2I communications. We believe that instead of having to give consent in an ad-hoc fashion every time a website wants requires to track a user -- which is problematic in the context of connected vehicles -- users should be able to configure their device settings up front to either accept specific tracking or not, or grant this right only to selected parties, be it truly trusted partners or third-party providers simply offering an indispensable service.

Device configurations regarding connectivity functions embedded in the vehicle present the most reliable solution to reach the driver as the privacy protected individual. For example, individual drivers could pre-select their privacy settings through an online or app-based dashboard. Each individual's privacy profile would be recognized by the vehicle and the vehicle would then automatically adjust its communications and sensor technologies to accommodate the privacy choices of individual drivers.

HERE Technologies considers that this approach presents a practical solution for the challenge of adopting specific consent requirements to fast-paced multi-stakeholder communication in the connected vehicle. We also believe it would provide the appropriate level of transparency and choice to the users while allowing the full deployment of technologies – and granting privacy at the same time. Such a model would therefore solve upcoming issues where otherwise privacy and technology may collide.

2. Rights of the data subject

If the concept of facilitating data subject's control over their data is understandable as such, the reality is the absence of solutions as we speak. This requirement is therefore very aspirational in our opinion. Also, HERE disagrees with the following statement: "To facilitate settings modifications, a profile management system should be implemented inside the vehicle". From a customer perspective, it should be the data subject's call to decide where they want to give the consent, and this should not be limited inside the car, it should also include other interfaces. No regulation today mentions that consent should be done inside the car exclusively. Also, such a scheme would make any third-parties like service providers largely dependent on the vehicle manufacturer's technology, which would contradict the guiding principles of the EU Data Strategy.

Should the driver/owner refuse to share data, it must be made clear that as a consequence they cannot benefit from cybersecurity protection and real-time services like maintenance warnings and all other services that an OEM or a service provider can propose. As such, the regulator needs to make the vehicle owner/ driver accountable in case a car has been hacked and data sharing is not allowed.

3. Personal Data

The guidelines mention that "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". In our opinion, this statement is too vague and fails to reflect the specificities of connected vehicles. Also, it introduces the risk that all data shall be considered PII Data.
Cars are very different from smartphones as they have multiple users. This should be well considered and can affect the degree to which type of data can be associated to the different data subjects.
Also, a large amount of the data emanating from connected vehicles are purely technical data (sensor data, oil temperature), which will still be highly needed for third parties to provide in novative services to the driver. However, they do not relate to any specific user.
The definition of personal data in art. 4(1) GDPR and specifically the notion of indirect identification should remain crucial to determine this. These guidelines should take the definition of personal data in art. 4(1) GDPR as a starting point.

4. Geolocation data

We are concerned that some elements of the proposed guidelines would have detrimental effects on the functioning of our location services and on the benefits of these services for our customers and end users. When it comes to geolocation data, we would like to highlight that:

- In order to ensure the continuity of notably safety-critical services, a large amount of location data needs to be collected and the option to deactivate geolocation at any time could therefore have severe consequences on the driver, who would not be informed of upcoming road hazard warnings for example. Also, we consider the notion of "absolutely necessary" being too subjective and restrictive in this regard, and we call EDPB to provide further precisions.
- The guidelines state that geolocation should be activated "only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started". This is unworkable in practice for key services like i.e parking or road hazard warnings. Too cumbersome requirements would make these services unattractive for customers, diminish their benefits and would negatively impact the development of data-based services and AI Technology in Europe.
- HERE practices data minimization and don't collect data we don't need. **We have taken a reductive approach to data collection, seeking to collect and maintain the minimum amount of data needed for a specified purpose.** E.g. For our HERE Positioning service, we only collect information we need for positioning which doesn't identify the end-user. And we promote pseudonymity for data subjects wherever a service does not require personal information to function.

So, in reality, **most services we provide are oriented to provide services in location context without identifying the end-user. Where personal data may be involved, we strive to apply pseudonymization techniques to reduce the direct identifiability of data related to individuals. Therefore, principles governing geolocation data should not be overly strict in order to ensure continuity of services to the driver.**

In general, more details in the guidelines on anonymisation/pseudonymisation would be helpful. For example, VIN numbers could be used for pseudonymisation purposes, if it is kept separate from personal identity.
The conditions under which datasets can be considered anonymous in specific contexts need to be in line with the GDPR. Clarity on anonymization techniques and a realistic assessment of what can be considered as anonymous data in practical scenarios is mission critical.

From a technical perspective, anonymization can only be done, when the purpose for which the data is been used, is known. Otherwise, there is a risk that:

- Anonymization can be "reversed" (de-anonymization) or
- Data becomes useless for the intended purpose, as the anonymization is taking away relevant information from this data

5. Future-proof purposes

As regards automated decision-making in the context of the provision of a service by a third-party, we believe the GDPR adequately covers data protection-related matters that arise with current and future technologies, and specifically with artificial intelligence (AI). However, it is particularly crucial to emphasise how unduly restrictive interpretations of the GDPR should be avoided to enable AI to flourish, for example through this guidance. This includes, notably, the interpretations of the right not to be subject to an automated decision, the purpose limitation and data minimisation principles as well as the purposes of processing and legal bases.

As well, although this guidance appears to consider future use cases, i.e. as regards limiting processing of sensitive data in vehicle "whenever possible", the guidance is not tech neutral with reference to latency for automated driving-assistance functions, and also prioritization of frequencies for security measures.

6. Data Controller

A clearer separation between data processor and data controller (service provider) should be introduced. The guidelines mention that data should be processed as much as possible inside the vehicle and highlights that if data has to leave the vehicle, consideration should be given to anonymize them before being transmitted.
This would have major consequences since it requires data leaving the vehicle to be disconnected from any vehicle identifier such as the VIN for example, which would make any commercial use of the data impossible.

7. Scope of mobile applications

The Guidelines state that mobile applications that contribute to the vehicle's connectivity capacities are included in the scope, even when these applications don't rely on the transmission of vehicle data.

Guidelines introduce a distinction between GPS navigation applications which are in the scope whether applications suggesting POIs (places of interest) to drivers should be outside of the scope.
We believe that the criteria invoked can lead to unclear implementation by causing unnecessary confusion. In reality, many mobile applications collect location data to suggest POIs while at the same time these applications also offer GPS navigation functionality to get there.

Guidelines should only **cover mobile applications which support vehicle functionality by exchanging data with or receiving data from a connected vehicle.** This means standalone GPS navigation using data from the mobile device, e.g. mobile phone GPS position, shall remain outside of the scope of these Guidelines.

8. Access to in-vehicle data and case-studies

We believe there is an urgent need to speed up the development of a data-driven economy in Europe. Today, there is a single model for accessing car data: The extended vehicle model. HERE is committed to make this work. HERE is indeed involved to find a compromise with suppliers and OEMs regarding the categories of data that need to be – and can be - made available to third parties in order to accelerate business opportunities and innovation.
As well, for certain use-cases, we do believe that the best way to facilitate data exchange is via a neutral server in order to enable safe, secure and privacy-compliant third-party access to car sensor data. This model opens up new monetization opportunities for car manufacturers, while fostering innovation among service providers to create new digital solutions that drivers will ultimately benefit from.

Nevertheless, this is not a one-size fits all picture, and we need to adopt a use-case based approach. HERE is dependent on the data that becomes available and remains agnostic when it comes to the way of harvesting this data. A hybrid approach, depending on the use-case, should be favored by the EU Commission when considering future regulation.

For any question, please contact marion.auzolle@here.com