3 May 2020

JOINT SUBMISSION OF AFFILIATED COMPANIES

GILBARCO VEEDER-ROOT, TELETRAC NAVMAN, AND GLOBAL TRAFFIC TECHNOLOGIES

IN RESPONSE TO THE EU DATA PROTECTION BOARD'S INVITATION OF PUBLIC COMMENTS TO THE GUIDELINES ON PROCESSING PERSONAL DATA IN THE CONTEXT OF CONNECTED VEHICLES AND MOBILITY RELATED APPLICATIONS

Gilbarco Veeder-Root, Teletrac Navman, and Global Traffic Technologies (the "Affiliated Companies") welcome the publication of the European Data Protection Board ("EDPB")'s Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications ("Guidelines").

We also welcome the opportunity to provide this feedback and are grateful that the EDPB seeks the views of stakeholders within the connected vehicles sector. We consider this good practice and would encourage this also for future guidelines, as stakeholder input may add valuable market insight into the practical application of the Guidelines.

Given the clear growth opportunities of the connected vehicles sector, it is essential that the application of data protection and privacy rules is given careful consideration, such that Data Protection Authorities ("DPAs"), industry, and citizens may understand clearly what compliance means, how to achieve, and how to identify noncompliance.

Based on our collective experience within the automotive and smart city industries, the Affiliated Companies share below a collection of positions that we believe will help to enhance the Guidelines. You will find that our positions fall into three broad topics.

Topic I addresses the proposed scope of the Guidelines and identifies areas that we believe could benefit from additional clarification. We recommend that the Guidelines clarify existing language to leave no doubt that data processing in the employment context falls outside the scope of the Guidelines. We also put forward recommendations aimed at clarifying which apps fall within the scope of the Guidelines, namely those that are an integral part of the vehicle and are involved in a transfer of personal data between the app, the vehicle, and a third party.

In Topic II we consider the application of the ePrivacy Directive (hereinafter "ePD" or "ePrivacy Directive")[1] and the General Data Protection Regulation ("GDPR")[2] to connected vehicles. Based on the applicability of Article 5(3) of the ePrivacy Directive to the connected vehicle context, the importance of a case-by-case assessment of whether a connected vehicle and the devices connected to it qualify as terminal equipment, and the sources of available legal bases, we conclude that the Guidelines wrongly suggest that a legal basis is required under both the ePrivacy Directive and the GDPR. Our view is buttressed by the *lex specialis-lex generalis*

[1] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136/EC of 25 November 2009.

[2] Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

relationship between these laws, commanding that the ePrivacy Directive takes precedence over the GDPR in situations where both apply.

And in Topic III we detail two points of operational compliance. Privacy and the use of personal data by any third party deserve the very highest forms of protection, whether at law and in the actual carrying out processing activities. We believe these vital objectives will indeed be preserved, if not further promoted, by the EDPB building maneuverability into its interpretation in the Guidelines of, "strictly necessary in order to provide an information society service explicitly requested by the subscriber or user" in Article 5(3) of the ePD. Relatedly, the proposed approach to consent modalities and on/off functionality within the vehicle environment risk a practical effect of thwarting a user's expectations and intentions while significantly restraining innovation across the industry.

For each of the three Topics that follows, we (A) explain our position including by referring to specific paragraphs of the Guidelines; (B) whenever possible, offer real-life examples drawn from our expertise within the sector; and (C) close by proposing solutions and revised language for the Guidelines consistent with those positions.

TOPIC I. SCOPE OF THE GUIDELINES

POSITION I(A): ***Paragraph 31 of the Guidelines presents an opportunity to clarify that processing in the employment context falls outside the scope of the Guidelines.***

Paragraph 31 of the Guidelines indicates that employers that provide company cars may engage in data processing to monitor their employees' actions for different purposes. The Guidelines refer to monitoring to ensure the safety of the employees, goods or vehicles, to allocate resources, to track and bill a service, or to check working time. The Guidelines acknowledge that this processing raises specific considerations to the employment context that are not addressed in the Guidelines. And employers are *not* mentioned in Paragraph 30 where categories of intended recipients of the Guidelines are listed.[3] The processing of personal data in the employment context does raise important issues specific to this context that have already been addressed by other sources, including the separate guidance issued by the Article 29 Working Party in its Opinion on data processing at work.[4]

This approach is entirely consistent with our own understanding and collective industry experience. We encourage the EDPB to maintain it in the final version of the Guidelines and believe Paragraph 31 should go further still. Because its current language allows for some doubt as to the true scope of the application of the Guidelines in this context, we call upon the EDPB to amend Paragraph 31 so that it states unequivocally that processing carried out directly by employers and by third party processors on their behalf is simply excluded from the scope these Guidelines.

EXAMPLES I(A): ***Several industry use cases illustrate where the Guidelines would be at odds with guidance around available legal bases and threaten to upset the balance between employer controllers and the data processors they need to engage.***

Employers that own or lease cars, vehicles, trucks, trailers, and other vehicles used by employees for different business objectives may use GPS tracking to manage their fleets and reduce operating costs. This often occurs through route optimization that helps to manage fuel costs and reduces employee driving time and therefore potential fatigue. Sometimes employers outsource the management of these functions to specialized fleet management companies acting as their data processors.

This type of processing raises important data protection issues, including ones related to the legal grounds available to employers. The Opinion on data processing at work stresses that for the majority of data processing at work, the legal basis should not be the consent of employees.[5] The same Opinion also validates the use of certain vehicle telematics as necessary to ensure compliance with the employee safety requirements, thus permitting employers to rely on the legal obligation legal basis.[6] Employers can also rely on its legitimate interests to know the

[3] Paragraph 30 lists non-exhaustively: "vehicle manufacturers, equipment manufacturers and automotive suppliers, car repairers, automobile dealerships, vehicle service providers, rental and car sharing companies, fleet managers, motor insurance companies, entertainment providers, telecommunication operators, road infrastructure managers and public authorities as well as drivers, owners, renters and passengers".

[4] Opinion 2/2017 on data processing at work, adopted on 8 June 2017, no. WP 249.

[5] *Id*. at 3, 4 and 23.

[6] *Id*. at 19.

location of its fleet vehicles.[7] And when addressing employer processing of information from vehicle tracking devices, the Article 29 Working Party Opinion on Geolocation services on smart mobile devices states that *rather* than seeking consent, employers are to consider whether they can rely on their legitimate interests under the Data Protection Directive.[8]

The reliance that the Guidelines place on Article 5(3) of the ePD—which, absent an exception, always requires the prior consent of the individuals where there is storage of information or the gaining of access to information that is already stored in the terminal equipment—is singularly at odds with the variety of legal grounds otherwise available to employers in guidance. Neither of the Opinions cited above nor the Article 29 Working Party Opinion on Legitimate Interests of the Data Controller under Article 7 of the Data Protection Directive[9] apply Article 5(3) of the ePD the way the Guidelines do, and for good reason.

These examples illustrate to us that the Guidelines create more confusion than they resolve for employers acting as data controllers and for the data processors the engage for fleet management support.

PROPOSED EDITS I(A): ***"Data processing by employers and their processors is outside the scope of these Guidelines."***

As the EDPB already recognizes, the Guidelines simply cannot address all potential issues and questions raised by connected vehicles. The concerns attendant to the employer-employee relationship are unique, peripheral to the main purpose of the Guidelines, and addressed in detail by other mandatory and persuasive regulatory sources. Because the current language of Paragraph 31 leaves some opening as to whether and how these Guidelines touch upon these ancillary issues, we suggest the following restatement:

> *Employers providing company cars to members of their staff (e.g. fleet managers providing vehicles to their employees) might want to monitor their employee's actions (e.g., in order to ensure the safety of the employee, goods or vehicles, to allocate resources, to track and bill a service or to check working time). Employers may also outsource such data processing or parts of it to data processors.*
>
> *Data processing by employers and their processors is outside the scope of these Guidelines. The EU Data Protection Board invites employers to consult the Article 29 Working Party's Opinion on data processing at work, which also addresses any processing involving vehicles used by employees. This Opinion was adopted prior to the GDPR, but by its own language it looked "toward the obligations under the GDPR" (pp. 4-5 of the Opinion). Data processing in the employment context may also be subject to national labour laws, which we invite employers to verify prior to data processing."*

[7] *Id*. at 19-20.

[8] Opinion 13/2011 on Geolocation services on smart mobile devices, adopted on 16 May 2011, no. WP 185, at 14.

[9] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, no. WP 217. Example 14 provided in the Opinion examines the electronic monitoring of internet use (such as cookies generated) of employees. It shows that a controller should do a balancing test and possibly rely on its legitimate interest for such processing.

POSITION I(B): ***Paragraph 19 of the Guidelines is overbroad by including within their scope apps used merely "within" a connected vehicle.***

In specifying the scope of the Guidelines, Paragraph 19 indicates that they deal with the personal data processed, among others, inside the vehicle, or collected within the vehicle and exported to external entities. Such a statement could lead to a misguided conclusion: that mere use of any app from *inside* the vehicle or the mere collecting of any personal data while *physically within* a vehicle are processing activities within the scope of these Guidelines. Such a result would cause these Guidelines to apply, for example, to apps installed on a personal smartphone even when they bear no relation to driving whatsoever.

Paragraph 27 picks up where Paragraph 19 leaves off, saying that mobile applications are indeed within the scope of the Guidelines because they are related to the environment of driving. But this misses an important reality that we observe commonly and widely in our field of expertise: there are many popular GPS navigation applications used in smartphones yet not related to the environment of driving. Consider apps that assist people who walk or take public transport: such apps simply may not need or may not collect any information related to the vehicle, not even the most basic identifiers like license plate number or vehicle identification number ("VIN").

These non-driving navigation apps do not relate to connected vehicles in any way. They are merely used *within* vehicles, sometimes in a user's mobile phone and sometimes simply mirrored or projected through a vehicle's display or speakers. Covering these apps would be an inappropriate overreach beyond the intended jurisdiction of the Guidelines. Accordingly, we propose that the Guidelines clarify that such apps are outside of the scope of the document.

EXAMPLES I(B): ***The current version of the Guidelines will lead to unintended or ill-advised consequences because a variety of apps that are unrelated to the operation or monitoring of a vehicle would nevertheless be considered within their scope.***

Take as an example a smartphone app enabling the user to pay for fuel tanked at a petrol station, but not connected to, in any way related to the operation of, or involved in any monitoring of a vehicle. Paragraphs 19 and 27 depart significantly from established law and previously published guidance by using the temporary, physical location where an app is used as a sweeping method of bringing that app within the scope of the Guidelines.

Consider also a vehicle's control display, which enables the user to visualize information from and utilize some functions provided by the app. Route planning maps, voice calling, and the display of phone address books are ready examples of the vehicle and its display act as nothing more than a figurative mirror of the smartphone. Apps are more easily visible to the driver and, critically, permit safer use of their features. But in the current version of the Guidelines, mirroring alone would cause the Guidelines to apply to the app, and we believe that this is a result that lacks, in the privacy context, any meaningful and convincing connection between the user and the vehicle.

The next example concerns a passenger of a connected vehicle who, sitting in a vehicle, uses a smartphone to tether a laptop to the Internet and sends work-related emails or buys a book from an online shop. These are activities that involve personal data "processed inside the vehicle," which, by those very terms, would fall within the scope of the current Guidelines. But it is difficult to imagine why and for what purposes such a result could be intended by the EDPB.

In the examples above, we describe an app stored on a smartphone and put to use within the vehicle or its proximity; a smartphone user interface that is mirrored on the vehicle's display without an exchange of information; and a portable computer and smartphone combination present within the closed doors or a vehicle but otherwise removed entirely from the driving environment. These scenarios, as applicable, fall fairly within the scope of the GDPR and the ePrivacy Directive by their own terms. The Guidelines attempt to bring each of these scenarios within their scope, but doing so could only be based on the illogical rationale of covering functions or systems that occur *within* a vehicle, but are unrelated to it. We believe Paragraphs 19 and 27 ought to be amended to correct their overreach.

PROPOSED EDITS I(B): ***The scope of the Guidelines is properly limited to personal data "exchanged between the vehicle and personal devices connected to it . . . or collected from the vehicle and exported to external entities".***

A key element to perfecting the scope of the Guidelines turns on whether information is exchanged between the vehicle and the device or app, and we suggest that the Guidelines clarify the scope accordingly. This could be achieved if Paragraph 19 is amended as follows:

> *(…) More specifically, it deals with the personal data in relation to the vehicle that is (i) ~~processed inside the vehicle, (ii)~~ exchanged between the vehicle and personal devices connected to it (e.g., the user's smartphone), or ~~(iii)~~ collected from the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.*

It would also require Paragraph 27 to be rephrased to make sure that smartphone mobile applications and GPS navigation devices are not *per se* always covered, but instead covered only when the app or device is an integral part of the vehicle and there is a transfer of personal data between them, which is then further transferred to a third party.

TOPIC II. APPLICABILITY OF ARTICLE 5(3) OF THE EPRIVACY DIRECTIVE

POSITION II(A): ***Whether a device connected to a vehicle qualifies as "terminal equipment" is a determination to be made on a case-by-case standard, not one that lends itself to application of a blanket rule.***

Paragraph 13 of the Guidelines makes a conclusory assertion that a connected vehicle and the devices connected to it are "terminal equipment"—"just like a computer, a smartphone or a smart TV"—that trigger the application of Article 5(3) of the ePD and, often, its prior consent framework. The Guidelines refer readers to Commission Directive 2008/63/EC[10], but they do not offer reasoning behind how, or why, the EDPB saw fit to adopt this crucial position. The idea that a device connected to a vehicle is *per se* terminal equipment does not take account of the multiplicity of componentry, configurations, interactivities, and purposes at play across industry today. For these reasons, we believe the question of whether something qualifies as terminal equipment is one answered best by application of a standard, not a rule.

Naturally, some devices connected to a vehicle will likely always satisfy the definition of terminal equipment[11]. What is less clear is whether the application of Article 5(3) of the ePD has a clear *raison d'être* in the connected vehicles context. By focusing on the involvement of terminal equipment, the effect of the Article is to protect the private sphere of individuals, where terminal equipment may contain information of a very private nature like evidence of communications, pictures, the location of individuals, contact lists, and other information already stored in the device. In this sense, terminal equipment is an extension of the individual's home.

Extending the private sphere to computers, phones, and laptops is understandable, indeed sensible. Reflexively placing connected vehicles into that same sphere may not be. In our experience, there are devices at work in a connected vehicle that do not interact with the type of information conventionally found in the private sphere of terminal equipment. Industry and users need to have a balanced, analytical framework to help them understand the legal nuance and relevant perspectives and would be well served if the Guidelines addressed this topic.

We draw support for our position from guidelines issued by national Data Protection Authorities, like the *Commission Nationale de l'Informatique et des Libertés*,[12] that discount the application of Article 5(3) of the ePD to the connected vehicle environment and apply only the GDPR instead, removing altogether the need to assess where a vehicle or a device connected to it constitutes terminal equipment.

PROPOSED EDITS II(A): ***The determination of whether a device constitutes "terminal equipment" is better suited to case-by-case analysis than the conclusory rule now present in Paragraph 13 of the Guidelines.***

[10] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment.

[11] "(a) equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network".

[12] See the connected vehicles compliance package for a responsible use of data, available at: https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.

The Guidelines would respond more accurately to the relationship between users and industry if the "terminal equipment" rule now set out in Paragraph 13 is converted into a standard capable of case-by-case application. The analysis should consider not only the technical elements of that term, but also functionally whether devices are used to process information that belongs within an individual's private sphere. Doing otherwise would risk placing the Guidelines into a less helpful theoretical realm that risks over classifying as terminal equipment devices that don't raise the concerns that Article 5(3) of the ePD is designed to address.

POSITION II(B): ***The current version of the Guidelines does not account for the* lex generalis-lex specialis *relationship between the GDPR and the ePD.***

Read together, Paragraphs 17 & 18 of the Guidelines mean that a data controller must rely on one of the legal bases of Article 6 GDPR for any processing of personal data that was obtained by accessing information in terminal equipment. This requirement rests on top, not in place of, the other requirement of having to rely on one of the legal bases under Article 5(3) of the ePD. The case studies laid down in the Guidelines further confirm that the EDPB considers as necessary the reliance on legal grounds from each of these two sources.[13]

This doubling-up of legal bases produces tension with the *lex specialis* nature of the ePD *vis-à-vis* the GDPR. Under the *lex generalis-lex specialis* relationship, a law governing a specific subject matter (the *lex specialis*) overrides a law that governs the general matter (the *lex generalis*). Extending the principle to the case at hand, it is Article 5(3) of the ePD, and that Article alone, that becomes directly applicable to the legal grounds, while the GDPR remains applicable except for its provisions, namely Article 6, that are specifically addressed by the ePD.

Our view is also the one espoused by Article 95 "Relationship with Directive 2002/58/EC" and Recital 173 GDPR. Article 95 GDPR provides in essence that the GDPR cannot add obligations in relation to matters for which such processing is subject to specific obligations with the same objective set out in the ePD. Whether or not personal data are accessed is irrelevant.[14] The conclusion that rightly follows is that Article 5(3) of the ePD alone suffices to provide legal bases for the access to information in terminal equipment and for the processing of personal data.

PROPOSED EDITS II(B): ***The Guidelines should recognize that processing activities involving terminal equipment present an important* lex generalis-lex specialis *superseding of the GDPR by the ePD.***

Access to and storage of information originating in terminal equipment is proper when based solely on a legal ground in Article 5(3) of the ePD, which is *lex specialis* on the matters it addresses in common with the *lex generalis* GDPR. A need to identify an Article 6 GDPR

[13] *E.g.*, legal basis for the 'Pay as you drive insurance', Paragraph 105; legal basis for renting and booking a parking space, Paragraph 119.

[14] As confirmed by the Court of Justice of the EU in Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH*. See paragraph 82, point 2 of the judgment: "Article 2(f) and Article 5(3) of Directive 2002/58, as amended by Directive 2009/136, read in conjunction with Article 2(h) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation 2016/679, are not to be interpreted differently according to whether or not the information stored or accessed on a website user's terminal equipment is personal data within the meaning of Directive 95/46 and Regulation 2016/679".

legal ground cannot be excluded in the connected vehicle context[15], but would arise only where the processing does *not* involve vehicles or devices that are determined to be terminal equipment. The Guidelines should be amended accordingly.

[15] *E.g.*, where the initial purpose of accessing or storing information on terminal equipment is followed by an unforeseen change or extension in purpose, such subsequent processing would need to rely on the legal grounds of Article 6 GDPR.

TOPIC III. MATTERS OF OPERATIONAL INTERPRETATION AND COMPLIANCE

POSITION III(A): ***The Guidelines do not eliminate doubt around what activities are "strictly necessary" and what types of providers qualify as "information society services".***

Article 5(3) of the ePD provides an exemption from its baseline consent requirement where storage or access to personal data on the terminal equipment is "strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service".

To establish whether this exemption applies, the provider needs to assess whether it is an information society service and, if it is, whether the access or storage is "strictly necessary" to providing the service. In current form, the Guidelines do little to assist service providers in making either of these assessments.

Although the Guidelines include five case studies, there is no analysis provided to help a reader determine whether an activity is "strictly necessary" or whether a provider is "an information society service". There is a need across the connected vehicle industry for enhanced guidance on these points, in part because these issues are determinative of whether consent has to be obtained.

We therefore encourage the EDPB to provide examples or categories of commonly used services related to connected vehicles that it believes would constitute an information society service. Indeed we would welcome the opportunity to assist the EDPB in identifying such a list. Doing so will also provide a source of persuasive authority and offer efficiencies to numerous DPAs that are responsible for the interpretation and enforcement of Article 5(3) of the ePD.

We likewise encourage the EDPB to explain how information society services should determine whether or not their intended access or storage is "strictly necessary" in the connected vehicle domain. It is worth mentioning that the Article 29 Working Party and national DPAs have provided detailed guidance on how Article 5(3) of the ePD affects the use of cookies, including particular guidance on types of cookies, which are necessary to provide an information society service and are thus exempted from the requirement of informed consent. And the Article 29 Working Party Opinion on Cookie Consent Exemption[16] provides detailed guidance about when a cookie is "strictly necessary".

We suggest that an approach similar to the one found in the Opinion on Cookie Consent Exemption should be taken in these Guidelines. This would see the EDPB identifying and providing explanations as to why certain use cases of access to and storage of information in connected vehicle environments may fall under the Article 5(3) exception.[17]

EXAMPLES I(C): ***Use cases common across industry highlight why it is important for these Guidelines to go further in explaining what renders an activity necessary to the provision of a service and what markers providers***

[16] Opinion 04/2012 on Cookie Consent Exemption, adopted on 7 June 2012, no. WP 194.

[17] This approach can also prove useful to the topic of obtaining consent, in the same way as the Article 29 Working Party and the opinions of national DPAs have explained in enormous detail how to obtain consent to cookies. We further address this point in [Position III(B)] below. Absent such legal and technical argumentation and examples, the Guidelines add little value on this point.

should look for to determine whether or not they are information society services.

Consider a smart navigation service that periodically validates the suggested routing to account for changed traffic conditions or to respond to missed turns. In order to provide this service, and assuming that Article 5(3) of the ePD applies to it, the provider needs to access the location of the vehicle in compliance with Article 5(3) of the ePD. Otherwise, the service cannot be provided.[18] Given that services like this one are likely one of the most common services in this environment, it would be useful if the final version of the Guidelines would confirm the application of the exception to consent in Article 5(3) in the same way that the Opinion on Cookie Consent Exemption confirmed that "user-input cookies" are necessary and thus exempt from consent. Similar services, such as those that direct a driver to the closest fuel station when fuel levels are appropriately low, invite a similar statement of confirmation from the EDPB.

The EDPB provides an example of stolen vehicle tracking as a feature that qualifies as an information society service and avoids the Article 5(3) consent requirement. Such services may be provided together with associated mobile app services enabling the vehicle owner to check where the vehicle is located for reassurance that the vehicle is in the location where the owner left it. This "peace of mind" service is also typical in relation to connected vehicles, and it is therefore welcome that the Guidelines present this example and confirm that this is indeed one provided by information society service. It would be useful if the EDPB further developed its guidance in this regard to clarify the type of data necessary for the provision of such services. The EDPB could consider establishing an indicative list of functions and services that would be considered an information society service.

Pay as you drive insurance is another topic addressed by the Guidelines, but where the EDPB takes the view that this service offering is one that is possible only based on an individual's consent. The Guidelines do not explain why the service, in EDPB's view, does not relate to an information society service, and we invite revisions that would help industry to understand this outcome.

The rationale underlying the necessity legal ground is to enable a service requested by the user. The logic is the same as the contract performance legal ground of Article 6 GDPR. In this way, Article 5(3) of the ePrivacy Directive adapts the GDPR's legal ground of performance of contract to the specificities of the electronic communications sector and terminal equipment. And the objectives of the two legal grounds remain the same at their core: the provision of a service and the performance of a contract.

There may be uncertainty as to whether a given service qualifies as an information society service, and we suggest that this is one area where interpretation should remain flexible, if for no other reason than to accommodate the need to access and store information without which a service cannot be provided. Using this standard, and because the service is explicitly requested by the user, privacy protections will remain intact.

We recall that DPAs have displayed a similar approach in the context of first party analytical cookies. For such type of cookies, the Article 29 Working Party Opinion on Cookie Consent Exemption reached the conclusion that such cookies "are not strictly necessary to provide a

[18] Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services defines at Article 1(1)(b) the 'information society service' as a service normally provided for remuneration, at a distance, by electronic means, and at the individual request of the recipient of services. Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') applies to information society services.

functionality explicitly requested by the user (or subscriber). In fact, the user can access all the functionalities provided by the website when such cookies are disabled. As a consequence, these cookies do not fall under the exemption. [. . .]". However, the Article 29 Working Party considered that first party analytics cookies are not likely to create a privacy risk when they are strictly limited to first party aggregated statistical purposes. "[. . .] In this regard, should article 5.3 of the Directive 2002/58/EC be re-visited in the future, the European legislator might appropriately add a third exemption criterion to consent for [these] cookies." As a result, some national DPAs such as the French[19] and the German[20] national DPAs have exempted such type of cookies from the need to obtain consent where certain conditions are satisfied. We commend this approach and strongly suggest following it when access or storage is necessary to provide the service in the context of connected vehicles. This result is all the more appealing if one takes into account the proposal for the Regulation on Privacy and Electronic Communications issued by the Croatian Presidency of the Council.[21] Article 8(1)(c) therein would allow the use of processing and storage capabilities of terminal equipment and the collection of information from terminal equipment if it is necessary merely for providing a service requested by the end user.

PROPOSED EDITS III(A): ***The legal ground of strictly necessary for the provision of an information society service could apply, by sound and logical extension, to some connected vehicle services that are requested by the driver.***

We ask the EDPB to consider adopting the following new language at or near Paragraph 105:

> *Certain services in the connected driving environment for which access to the vehicle is needed for the provision of the service may not satisfy all the conditions of an information society service (i.e., be provided for a remuneration, at a distance, by electronic means, and at an individual request of a recipient of services). However, it is nonetheless the vehicle owner or the driver who has requested such a service, for which the access to the vehicle's information is needed. It would be redundant that the service provider asks the recipient of the service for consent, as it is the service that the recipient of the service requested in the first place. Therefore, taking into account the willingness to receive the service, and minimal privacy risks, the EDPB considers that the legal ground of strictly necessary for the provision of an information society service could apply to such services by sound and logical extension. In addition, the EDPB calls on the European legislator to consider examining the scope of the exemption and broadening it in the context of the ongoing legislative process on the Proposal for a Regulation on Privacy and Electronic Communications.*

POSITION III(B): ***Modalities of consent and on/off functionality to be required for selected functional***

---

[19] See Article 5 of the CNIL's Guidelines of 19 July 2019, available at: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038783337

[20] See the German [Federal] Data Protection Conference's paper published in March 2019, available at: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

[21] Document no. 6543/20 of 6 March 2020, available at: https://data.consilium.europa.eu/doc/document/ST-6543-2020-INIT/en/pdf.

Paragraph 46 of the Guidelines recalls the conditions for obtaining legally valid consent under the GDPR. It also indicates that "data controllers need to pay careful attention to the modalities of obtaining it from different participants, such as car owners or car users". In paragraph 49, the EDPB acknowledges that "classic mechanisms used to obtain individuals' consent may be difficult to apply in the context of connected vehicles, resulting in a "low-quality" consent based on a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals". We similarly recognize the practical difficulties raised by the EDPB and would welcome its further views on how providers might overcome the challenges of obtaining consent, a task that features heavily throughout the Guidelines as a cumbersome inhibitor not only to innovation and the *status quo* alike.

In Paragraph 74 of the Guidelines, the EDPB recommends that "data subjects should have the possibility to activate or deactivate the data processing for each other purpose and controller/processor and have the possibility to delete the data concerned". For example, Paragraph 61 of the Guidelines provides that geolocation shall 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". It is unclear to us whether the EDPB considers that such functionalities need to be available *during* driving and whether these functionalities ought to be considered as a heightened form of withdrawing consent or requesting erasure unique somehow to the connected vehicle domain. We are also left with doubt as to why a data subject should have an ability to activate and deactivate processing for each *processor*, as under the GDPR it is the controller that serves as the established point of reference for a data subject.

EXAMPLES III(B): ***In today's connected vehicle market, certain standard services are provided with the nonnegotiable expectation that they never be deactivated.***

A vehicle may be equipped with a system that tracks its location in case it has been stolen, allowing the service provider to cooperate with police in the recover. In some Member States, it is a common practice that insurance companies will only agree to cover a vehicle if the vehicle owner has beforehand installed this type of a system. By the very nature of such a system, it cannot be activated or deactivated by an individual because doing so would frustrate the very purpose for having such a system in the first place. One can also envisage other functionalities serving other important interests of the vehicle owner that cannot be turned on and off from within the vehicle or perhaps even at all. For this reason, we suggest that the EDPB allows for the possibility in these Guidelines that some functionalities may not be equipped with an option to activate or deactivate data processing on a purpose-by-purpose or controller-by-controller basis.

PROPOSED EDITS III(B): ***Suggested change***

We suggest that the EDPB amends the recommendation in Paragraph 74 as follows:

> *". . . the EDPB recommends that only data strictly necessary for the vehicle functioning, for the functioning of the devices installed on the vehicle, or for the services related to the vehicle or its devices are processed by default. Provided doing so does not frustrate the purpose of a service or feature, data subjects should have the possibility to activate or deactivate the data processing for each other purpose and controller ~~/ processor~~ and have the possibility to delete the data concerned. For instance, there may be devices and services, e.g. stolen vehicle tracking, whose purpose may be at odds with the possibility to deactivate it from within the vehicle or at all. In addition, it*

should be possible for the vehicle owner or driver to decide that a device or service is on at each ignition of the vehicle”.

About the Affiliated Companies

GILBARCO VEEDER-ROOT

Gilbarco Veeder-Root ("GVR") is technology with a human touch. When you fill up a tank or swipe a credit card, you're likely to touch the technology of GVR. From reliable fuel dispensers to intuitive point of sale, its integrated solutions power convenience stores and gas stations worldwide.

GVR is the global leader of integrated technology solutions in the retail petroleum and commercial fueling industries, with proven expertise that its customers around the world depend on. The company's systems and solutions are designed and tested to work together seamlessly to deliver the lowest cost of ownership and best integration possible.

For more than 150 years, Gilbarco has earned the trust of its customers by providing long-term partnership, uncompromising support and proven reliability, and will continue innovating to improve energy efficiency, safety and security for all of us.

TELETRAC NAVMAN

Teletrac Navman is a leading software-as-a-service (SaaS) provider leveraging location-based technology and services for managing mobile assets. With specialized solutions that deliver greater visibility into real-time insights and analytics, Teletrac Navman helps companies make better business decisions that enhance productivity and profitability. Its fleet and asset management technology uncovers information that would otherwise go unseen, helping customers reduce risk and confidently move their business forward with certainty. It tracks and manages more than 500,000 vehicles and assets for more than 40,000 companies around the world.

GLOBAL TRAFFIC TECHNOLOGIES

Global Traffic Technologies ("GTT") is the market leader in smart mobility solutions. GTT is the owner and manufacturer of the Opticom™ traffic signal priority control system and Canoga™ traffic-sensing system. These systems have provided safe and reliable traffic solutions to communities for more than 50 years.