European Automobile Manufacturers Association

EDPB GUIDELINES ON VIRTUAL VOICE ASSISTANTS – ACEA COMMENTS FINAL

The European Automobile Manufacturers' Association (ACEA) welcomes the publication of the draft guidelines on virtual voice assistants (VVA).

As this technology is used increasingly in motor vehicles, we would like to offer our views regarding specific issues around identification, transparency, and consent. Our comments below refer to the respective paragraph in the document:

25 - Is a VVA always to be considered as terminal equipment. We think not. If the processing of data is strictly limited to the device itself, without interacting with a remote server, then a VVA is no terminal equipment following the definition of the Privacy Directive. A very data protection friendly variant of a VVA provides an option, that "limited" command recognition and feature execution on the device (e.g. climate control in the vehicle) is done without interaction with a remote server. In consequence this feature requires no consent of the user at all as it would be in-vehicle processing only.

This is how we as European vehicle manufacturers have implemented voice recognition in our vehicles: a limited set of instructions is available offline and offline processing is also the default setting.

29 – This section would imply, that a user must be identified to collect proper consent (and to show accountability) following the ePrivacy Directive for accessing device information (e.g. GPS position for finding the nearest gas station). Identification typically requires processing of "biometric" data (voice print). This "forced" processing of sensitive data is in strict contrast to the privacy by design principle, which would recommend processing this data in an anonymised form only. Subsequently, Section 71 and Example 6 clarify that access to data stored on the terminal device may be exempted from the consent requirement. This issue appears hard to resolve: to get consent the user must be identified but at the same time anonymous processing is required.

At the same time, any "forced" identification also contradicts art. 11 GDPR, according to which "the controller shall not obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation". Therefore, and following the data protection by design principle, we would deem it more data protection friendly to de-personalise the data already in the vehicle.

31 – It should not be stipulated, that all voice data is in general to be seen as sensitive data. If – following privacy by design features - meta-information is not processed and the nature of the

system does not require sensitive content (e.g. control of vehicle features only), then voice data is non sensitive.

49 – Providing transparency to multiple users would imply, that different users will be identified/differentiated. A "forced" identification/differentiation of users would require some sort of profiling, which is contrast to privacy by design principles. See also our comments on paragraph 29: to identify or nor to identify.

58 – Providing transparency to multiple users: see comment on 49. Paragraph 59 already states, that this condition is difficult to fulfill.

90 – Following this requirement the use of a complex VVA ecosystem would require probably various consents for different purposes of different providers… This is neither transparent for the customer nor easy to choose following GDPR requirements. Only very limited standardized processing purposes would be understandable for the user. Again, identification of the user und documentation of the consent and of the transparency information provided is a rather big challenge. If all this is done in oral form, the user will completely lose track and will only be more confused.

109 – Understandable recommendation, but hard to fulfill in practice because at the time of detection the processing has already occurred. That would also imply that some form of monitoring occurs or else a recording based on a mistaken activation could never be identified.

141 – How can consent of multiple users of a system be proven without identifying them? Forced identification contradicts privacy by design principles. Same comments as above.

149 - To exercise data subject rights: if a data subject is not identified then it is impossible to determine which data "belongs" to whom and it could well be that when access to data is given, personal data associated with someone else will be provided as individuals are not identified.
