Feedback on EDPB Guidelines 02/2021 on Virtual Voice Assistants

The H2020 COMPRISE project welcomes the opportunity to provide input to the European Data Protection Board's (EDPB) consultation on its draft guidelines on virtual assistants ("Guidelines 02/2021 on Virtual Voice Assistants") published on 9th of March 2021.

COMPRISE is an H2020 project financed by the European Commission that defines a fully private-by-design methodology and tools that reduce the cost and increase the inclusiveness of voice interaction technology through research advances on privacy-driven data transformations, personalised learning, automatic labelling, and integrated translation. This leads to a holistic easy-to-use software development kit interoperating with a cloud-based resource platform. The sustainability of this new ecosystem is demonstrated for three sectors with high commercial impact: smart consumer apps, e-commerce, and e-health.

Please, find in the table below our specific comments on the guidelines:

Section	Paragraph	Text	Comment
Executive summary		"Currently, all VVAs require at least one user to register in the service. Following the obligation of data protection by design and by default, VVA providers/designers and developers should consider the necessity of having a registered user for each of their functionalities."	Please, consider including an example of one or two functionalities for which it wouldn't be necessary for the user to register. This would help to make the paragraph clearer
Section 2.2	16	"Please note that while currently most voice-related processing is performed in remote servers, some VVA providers are developing systems that could perform part of this processing locally".	Please also consider including in the footnote examples of open source European initiatives such as COMPRISE, which also perform part of the processing locally (on device or on a personal server).
Section 2.5	21	"The over or under-representation of certain statistical characteristics can influence the development of machine learning-based tasks and subsequently reflect it in its calculations, and thus in its way of functioning, just as much as its quantity, the quality of the data plays a major role in the finesse and accuracy of the learning process"	The consequences of the under-representation of certain population segments in the training datasets can be illustrated with an example. One clear consequence that particularly affects voice assistant users is "the accent gap", i.e., the inability of voice-based technologies to understand speakers with non-native or regional accents with the same accuracy as most speakers. Also, consider analysing the bias issue in voice technologies and compliance with the "fairness principle". A subsection could be added to Section 3.
Section 3.1	30	"If data controllers become aware (e.g., through automated or human	Regarding this point, a recommendation should be included

		review) that the VVA service has accidentally processed personal data, they should verify that there is a valid legal basis for each purpose of processing of such data. Otherwise, the accidentally collected data should be deleted”	stating that data controllers should maintain a proactive attitude regarding the performance of reviews to identify possible accidental recordings of personal data.
Section 3.1	31	“Moreover, it should be noted that personal data processed by VVAs may be highly sensitive in nature. It may carry personal data both in its content (meaning of the spoken text) and meta-information (sex or age of the speaker etc.). The EDPB recalls that voice data is inherently biometric personal data. As a result, when such data is processed for the purpose of uniquely identifying a natural person or is inherently or determined to be special category personal data, the processing must have a valid legal basis in Article 6 and be accompanied by a derogation from Article 9 GDPR (see section 3.8 below).”	Please consider indicating that very sensitive information may be inferred through the user's voice. It could also be mentioned here, as it is done some pages after, the existence of patented technologies that aim to infer health status and emotional states from the user's voice.
Section 3.2	36	“The plurality of personal data processed when using a VVA also refers to a plurality of personal data categories for which attention should be paid (see below section 3.8). The EDPB recalls that, when special categories of data are processed, Article 9 GDPR requires the controller to identify a valid exemption from the prohibition to processing in Article 9(1) and a valid legal basis under Article 6(1), using an appropriate means identified under Article 9(2). Explicit consent may be one of the appropriate derogations where consent is the legal basis relied on under Article 6(1).“	There may be voice apps that do not directly request any sensitive data or for which, in principle, the purpose of the processing does not require the collection of sensitive data, but still sensitive information is collected or may be inferred (e.g. a cooking app through which the user asks for specific ingredients that may reveal their health condition, or an e-commerce voice app through which the user may acquire products that may reveal their health status, sexual orientation, or religious beliefs). Other voice apps may enable a very open interaction with the user, so the user may reveal sensitive information (e.g., a voice app for writing a diary, a voice app to write notes or input appointments in the calendar) For these cases, consider providing some guidelines on the best

			way to proceed for the data controller (e.g., inform the user about the possibility of collecting these kinds of sensitive data and asking for explicit consent, dataset anonymisation, etc.)
Section 3.3.	48	"Failure to provide necessary information is a breach of obligations that may affect the legitimacy of the data processing. Complying with the transparency requirement is an imperative since it serves as a control mechanism over the data processing and allows users to exercise their rights. Informing users properly on how their personal data is being used makes it more difficult for data controllers to misuse the VVA for purposes that go far beyond user expectations. For example, patented technologies aim to infer health status and emotional states from a user's voice and adapt the services provided accordingly."	The need for transparency when labelling is carried out by humans could be included as an example in this Section. There is a general perception that voice technology companies have failed to inform their clients adequately on the processing of their personal data. Several media published in 2019 hinted that different voice technology companies failed in informing their clients that they were hiring humans to review clips of conversations between devices and their users.
Section 3.2.2	58	"VVA designers must consider how to properly inform non-registered and accidental users when their personal data is processed. When consent is the legal basis for processing users' data, users must be properly informed for the consent to be valid. In order to comply with the GDPR, data controllers should find a way to inform not only registered users, but also non-registered users and accidental VVA users. These users should be informed at the earliest time possible and at the latest, at the time of the processing. This condition could be especially difficult to fulfil in practice".	Is there any good practice or mechanism for informing non-registered users and accidental VVA users of personal data processing by a VVAA that could be provided as an example?
Section 3.6	96	"The data minimization principle is closely related to the data storage limitation principle. Not only do data controllers need to limit the data storage period, but also the type and quantity of data"	Please, consider including some guidelines to determine the criteria that should be followed by the data controller to decide the timing of the personal data storage when this data is processed through voice technologies.
Section 3.6	105	"Anonymizing voice recordings is especially challenging, as it is possible to identify user through the content	The two articles cited in the footnote are irrelevant. The paper by

		of the message itself and the characteristics of voice itself. Nevertheless, some research is being conducted on techniques that could allow to remove situational information like background noises and anonymize the voice”.	Cohen-Hadria et al. does not “remove situational information like background noises”. On the contrary, it aims to preserve background noise and obfuscate any overlapping speech. The method by Qian et al. provides almost no protection, as we showed recently.[1] Please consider citing the voice anonymization baseline for the 1st VoicePrivacy Challenge[2] or the open-source voice[3] and text[4] anonymization tools developed by COMPRISE as example tools which provide much more effective anonymization.
Section 3.6	107	“Before considering anonymization as means for fulfilling the data storage limitation principle, VVA providers and developers should check the anonymization process renders the voice unidentifiable.”	Please consider citing COMPRISE’s rigorous evaluation protocol[5] (based on formal informed attacker models combined with state-of-the-art voice biometrics) as an example solution to check whether the voice is unidentifiable. Also clarify that effective anonymization decreases the utility of the data (i.e., its suitability for training ASR or NLU models), although this impact is limited for some anonymization techniques.
Section 3.9	140	“VVA designers should consider technologies deleting the background noise and conversations ensuring that only the user voice is recorded.”	The article cited in the footnote is irrelevant. It does not delete the background noise nor background conversations. On top of that, it provides almost no protection against re-identification, as explained above. Deleting the background noise or background conversations requires using speech enhancement technology with a special attention to privacy, which has not been done so far to the best of our knowledge.

[1] Brij Mohan Lal Srivastava, Nathalie Vauquier, Md Sahidullah, Aurélien Bellet, Marc Tommasi, and Emmanuel Vincent, “Evaluating voice conversion-based privacy protection against informed attackers”, in 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2802-2806, 2020.

[2] 1st VoicePrivacy Challenge: https://www.voiceprivacychallenge.org/

[3] COMPRISE Voice Transformer: https://gitlab.inria.fr/comprise/voice_transformation

[4] COMPRISE Text Transformer: https://gitlab.inria.fr/comprise/text_transformer

[5] COMPRISE Deliverable D2.3 “Final transformation library and privacy guarantees”: https://www.compriseh2020.eu/files/2021/02/D2.3.pdf

Foot-notes	• Footnote 5 • Footnote 34 • Footnote 47		Links to URL is broken (due to line break). URL address in link after line break are missing