23 April 2021

EBF_045080

EBF response to the European Data Protection Board's consultation on the Guidelines 02/2021 on Virtual Voice Assistants

EBF position:

The EBF welcomes the European Data Protection Board (hereafter 'EDPB') draft guidelines on the Virtual Voice Assistants (VVA). You will find below both general and detailed comments on the draft guidelines.

I. General comments

The EDPB rightly points out that the **processing of biometric data** is only allowed either by first obtaining explicit consent of the data subject or when another derogation from Art. 9 GDPR applies. However, in paragraph 31 the EDPB states that "*voice data is inherently biometric personal data*" while referring to Art. 4(14) GDPR. This definition refers to biometric data when it allows or confirms the "unique identification" of a natural person. We would like to point out that voice data **may not always be used to uniquely identify and individual, in which case if not used to do so, "voice data" does not qualify as "biometric data".** Using the word **"inherent"** is therefore **misleading** and we **suggest to include the following wording** in its place:

- "The EDPB ***recalls that voice data may qualify*** as biometric personal data when allowing or confirming the unique identification of an individual".

This suggested text is also **more in line with the definition of biometric data under the GDPR.**

Paragraph 125 rightly points out that VVA designers and developers must carefully identify "*in which cases the processing implies special categories of personal data (SCPD)*." This paragraph and the ones that follow provide a series of indications on the legal bases relating to the processing of biometric data, highlighting that if the use of the voice is aimed at identifying the data subject, their consent will be required pursuant to Art. 9 of

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

the GDPR (paragraph 128). The focus here seems to be vested on "explicit consent". There may be **other exceptions** which, if not available yet but in time, **may also constitute a base to use voice for uniquely identifying an individual other than consent.** For example, when it is necessary for reasons of substantial public interest (Art. 9(2)(g) GDPR).

We also recommend specifying that when the voice data is only used for interacting with the app, in its daily interaction, the consent pursuant to Art. 9 of GDPR is not needed unless other special categories of data are processed. In other words, the consent is only required when the voice is used for identification purposes (i.e. when the voice data qualifies as biometric data) or when other special categories of data are processed).

Finally, the examples concerning the banking sector may give rise to the misleading idea that it is common practice for more banks in Europe to offer to their customers an application that can be directly queried via a VVA. We would suggest to introduce a small disclaimer into the final Guidelines, indicating that that these are hypothetical examples to explain the possible roles of parties that could use VVA and that it should not be expected that that all financial institutions develop these applications.

II. Detailed comments

Overall, **almost all the aspects covered by the Guidelines will concern the provider of VVA services.** However, we would welcome more examples and further clarifications from the EDPB on how to manage issues such as the following:

- In Example 12 the draft Guidelines read "*If the user wishes to set up biometric authentication for access to certain protected data such as his/her bank account, the voice assistant could activate speaker verification, when he/she launches the application only, and verify his/her identity in this way*." In our view, it is important to underline that when accessing a bank account, also Art. 97 of EU Directive 2015/2366 (PSD2)[1] shall be taken into account whereby strong customer authentication is required, implying at least two factors for the identification.

  Indeed, there may be situations where biometrics (which may include voice, face recognition etc.) provide for a safer way to access services than the protection afforded by using a password. The potential positive aspects and possibilities of this do not seem to be sufficiently taken into account in the draft Guidance.

- As noted in Paragraph 125, the identification of a data subject through their voice implies biometric data processing, thus a processing of SCPD. In these cases the legal basis for the processing is consent (Article 9(2)(a) GDPR). If the data subject does not agree to give his/her consent, the data controller, should offer an alternative identification method to biometrics, with regard to the free nature of consent (see Paragraph 128). **Examples of alternatives identification methods to rely on**, **when the user does not give his/her consent for the processing of biometric data, would be welcome.**

- Paragraph 128 should also refer to other possible exceptions than consent. We therefore suggest to make an explicit reference should be made to Art. 9(2)(g) GDPR.

- With reference to Paragraphs 155 and 167 of the draft Guidelines, we would welcome further examples and clarification **with regards to fulfilling the data access and data portability rights requests**. This could be very complex when it comes to voice data, as well as the application of automated background-noise

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of on payment services in the internal market

filtering, as proscribed in Paragraph 139. They also raise concerns when it comes to the **technical implementation** (please see below).

- It would be helpful to provide further clarification on the **mechanisms regarding the execution of data subjects' right via VVA** in particular with regards to the following:
    i. When using a VVA tool, is the execution of data subjects' rights via "easy-to-follow voice commands" obligatory or just an additional option?
    ii. Is it sufficient that the request to exercise data subject rights can be made via VVA or shall also the information be provided via VVA?
    iii. Is it sufficient that the VVA refers to a form and where it is available?

We would also like to flag some aspects of the draft Guidance **that raise concerns on the feasibility of the technical implementation**, with particular regard to the:

i. Preparation of alternative voice recognition systems in the absence of the data subject's consent to the processing of biometric data.
ii. The application of filters aimed at eliminating any background items coming from third parties and in general from the external environment (see paragraph 139).
iii. The management of access rights and portability (see paragraphs 155 and 167).

It is important to note that in order to assess who is the data controller and who is the data processer, **a case-by-case assessment should be made per processing activity**. This approach is reflected in paragraph 15 and 42 of the draft Guidance and should be kept in mind.

III. Additional comments

We would also like to mention that, beyond the current Guidelines, it is helpful to consider other frameworks where the relationship between a bank, for example, and a VVA provider is present, such as the 2019 EBA Guidelines on outsourcing arrangements[2]. Under these guidelines, banks have an obligation to conclude a contract with any outsourcing services, this would include VVA service providers. The guidelines include a link between the obligations on the outsourcing service and data protection under the GDPR, notably under Art. 13(2) 13.2 Security of data and systems:

"…*Institutions and payment institutions should ensure that the outsourcing agreement* ***includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the institution or payment institution*** *(e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed.")*

However, including this obligation in contracts with the VVA service provider could be difficult, also due to a possible imbalance in bargaining power between the bank and the VVA service provider. As the executive summary of the draft Guidance states – "*The vast majority of VVA services have been designed by few VVA designers"*.

This could create difficulties when it comes to implementing obligations and **ensuring that personal data is protected by the VVA service provider,** who could process the

[2] European Banking Authority (2019) *EBA/GL/2019/02: EBA Guidelines on outsourcing arrangements*

personal data for other purposes. We recommend to reflect this potential imbalance and the risk it can create for the users in the final Guidelines.

ENDS

For more information:
Liga Semane
Policy Advisor – Data & Innovation
l.semane@ebf.eu

About the EBF

The European Banking Federation is the voice of the European banking sector, bringing together 32 national banking associations in Europe that together represent a significant majority of all banking assets in Europe, with 3,500 banks - large and small, wholesale and retail, local and international – while employing approximately two million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that reliably handle more than 400 million payment transactions per day. Launched in 1960, the EBF is committed to a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu