

## Comments on Guidelines 02/2021 on Virtual Voice Assistants

### EuroCommerce

EuroCommerce is the voice for over 5 million retail, wholesale, and other trading companies. Our members include national federations in 31 countries, Europe's 35 leading retail and wholesale companies, and federations representing specific retail and wholesale sectors.

### Introduction

EuroCommerce welcomes the opportunity to provide comments on the European Data Protection Board's ("EDPB") Guidelines 02/2021 on Virtual Voice Assistants (the "Guidelines"). EuroCommerce appreciates the EDPB's efforts to provide guidelines for Virtual Voice Assistants ("VVA") with the aim to guarantee adequate privacy protection for users as the service is available for a vast majority of people when using for example their smartphones. In light of the foregoing, EuroCommerce believes that it is important that such guidelines remain sufficiently open and flexible so that they can take into account the specific characteristics of the different voice service architectures and the rapid technological developments in the VVA sector. In this regard, the legal framework should allow for use of VVA solutions in a way that is not to the detriment of digital innovation as well as European businesses' competitiveness on the global market.

Below we summarise our key points and proposals and detailed comments which we hope will be helpful when finalising the Guidelines. We would be more than pleased to discuss these issues further with the EDPB should you have any questions regarding our comments.

### Our key points and asks

- We ask the EDPB to (i) re-consider its reference to the applicability of the ePrivacy Directive in the Guidelines, or (ii) as a minimum, to provide that the relevant VVA actor (i.e. the data controller) should assess whether the ePrivacy Directive is applicable for its service. However, it is essential that the ePrivacy Directive does not by default apply for use of VVAs if the requirements of Article 5(3) are not met (please see section 1.1).
- We ask that the EDPB includes further examples of situations involving joint controllership in the Guidelines (please see section 2.1-2.2).
- We ask that the EDPB (i) revises its statement concerning the necessity to seek consent from the user, as it relies on an incorrect assumption and other lawful legal bases such as the performance of a contract or the pursuance of a legitimate interest under Article 6(1)(f) GDPR may be valid for data processing by voice service providers; and (ii) removes its reference to profiling as a purpose for data processing in para. 29 of the draft Guidelines as profiling merely is a means to an end, e.g. personalisation or marketing purposes (please see section 2.3).
- We ask that the EDPB revises its conclusion regarding service improvement purposes and consider Article 6(1)(b) of GDPR as an appropriate lawful basis (please see section 3).
- We ask the EDPB to revise its statement on the obligation to provide information under Article 12 GDPR to accidental users as Article 12 of the GDPR only sets out an information requirement with regard to intended processing. Moreover, in the event Article 12 of the

GDPR should be considered applicable on accidental processing, we ask the EDPB to clarify the involved VVA actors' responsibilities to inform accidental users (please see section 4).

- Please also see section 4 for additional comments in relation to specific paragraphs of the draft Guidelines.

## 1. LEGAL FRAMEWORK

### 1.1. ePrivacy Directive

According to para. 24 and 28 of the draft Guidelines, the EDPB is of the opinion that the Article 5(3) of the ePrivacy Directive applies, meaning that the article would “[set] a specific standard for all actors who wish to store or access information stored in the terminal equipment of a subscriber or user in the EEA” as “current VVAs require access to the voice data stored by the VVA device”. EuroCommerce is of the opposite opinion for the reasons set out below.

- 1.1.1. Article 5(3) applies to (i) the storing of information, or the gaining of access to information already stored, in (ii) the terminal equipment (iii) of a subscriber or user. There are thus three requirements that must be satisfied for the ePrivacy Directive to become applicable.

#### ***(i) the storing of information, or the gaining access to information in a VVA***

- 1.1.2. It is important to note that a cloud-based voice service does not generally require storing information or accessing information in the customer's device. By design, the VVA allows for streaming of the voice recordings to the cloud typically when the voice command of the user activates the voice service. When this happens, the voice service provider does not “store” voice recordings in the device of the user nor “gains access” to voice recordings stored on the device of the user.

- 1.1.3. Contrary to this, it is the user that initiates the streaming of the voice recordings to the servers of the voice service provider via the device rather than the voice service provider retrieving that information from the device. In a way, the voice command of the user makes a connection to a server, but this does not mean that the server gains access to the user's equipment. An illustrative example on how this works is the use search fields of a search engine or other web application. In this case, the user makes a connection to the server to receive information without the server gaining any access to information of the user's device.

- 1.1.4. By reason of sections 1.1.3-1.1.4, we do not believe that Article 5(3) of the ePrivacy Directive should apply.

#### ***(ii) VVAs as terminal equipment***

- 1.1.5. According to the draft Guidelines, “VVAs should be considered as “terminal equipment” and the provisions of Article 5(3) ePrivacy Directive apply whenever information in the VVA is stored or accessed” (para. 25 of the draft Guidelines). As stated in sections 1.1.1-1.1.4, no information is generally stored or accessed in the VVA. In addition, the EDPB does not provide any explanation to why a VVA constitutes “terminal equipment”.

- 1.1.6. Moreover, in the technical definition of VVA in the Executive Summary, the VVA is “a service that understands voice commands and executes them or mediates with other IT systems if needed” (para. 2, emphasis added) or in para. 8 of the same draft Guidelines as “software application that provides capabilities for oral dialogue with a user in natural language”, which clearly refer to a VVA as a service, not an equipment.

- 1.1.7. The ePrivacy Directive does not define “terminal equipment”. The term is defined in the Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment as “equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information [...]”. According to the Merriam-Webster online dictionary, equipment refers to “the set of articles

*or physical resources serving to equip a person or thing [...].*<sup>1</sup> It is thus clear that the notion of “terminal equipment” necessarily refers to a physical device and does not cover services.

1.1.8. By reason of sections 1.1.5-1.1.7, VVAs do not constitute terminal equipment and the article should thus not apply in our view.

***(iii) the terminal equipment must belong to the user***

1.1.9. Moreover, Article 5(3) of the ePrivacy Directive refers to “*the terminal equipment of a subscriber or user*”. This indicates that the terminal equipment belongs to the subscriber or user and that it regards a physical device – not a service.

1.1.10. We also believe that the notion “terminal equipment” should not include voice services as the wording does not allow for such interpretation given the fact that the VVA service could be offered by several actors as set out in para 15. However, the user, as defined by the EDPB, is not one of them.

1.1.11. By reason of sections 1.1.9-1.1.10, VVAs could not belong to a user and the article should therefore not apply.

***Summary***

1.1.12. In our view, VVAs do not meet the necessary requirements that would make the ePrivacy Directive apply. Moreover, we believe that it is important to remember that Article 5(3) aims to address “so-called spyware, web bugs, hidden identifiers and other similar devices can enter the user’s terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user” (recital 24). When using VVAs, the user has an intention to use the VVA which means that the VVA is not processing information without the user’s knowledge. Furthermore, this activity does not generally implicate the use of spyware, web bugs, hidden identifiers, or other similar devices. Indeed, as the customer speaks to his or her device, this information is directly sent to the cloud for processing without the voice service provider gaining access to the device, whether through spyware or other means.

In our opinion, the ePrivacy Directive should not apply for the use of VVAs. However, it is essential that the ePrivacy Directive does not by default apply for use of VVAs if the requirements of Article 5(3) are not met.

We thus ask the EDPB to:

- (i) re-consider its reference to the applicability of the ePrivacy Directive in the Guidelines, or
- (ii) as a minimum, to provide that it is the relevant VVA actor (i.e. the data controller) who needs to assess whether the ePrivacy Directive is applicable for its service.

*Related paragraphs in the Guidelines: 2, 8, 15, 24, 25, 28*

***1.2. GDPR***

1.2.1. Even though we believe that the ePrivacy Directive should not be applicable, the rights of the registered would still be protected by the GDPR as it applies for all processing of personal data related to the use of VVAs.

1.2.2. The core function of a voice service is to accurately recognise and respond to customers’ spoken requests. Users want voice services to perform this function well over the lifetime of their engagement with the service, and for the services to improve over time, including by adding new and desirable features. Since the activities involved in voice services are diversified and complex, it is necessary to rely on different legal bases for the data processing.

<sup>1</sup> <https://www.merriam-webster.com/dictionary/equipment>.

- 1.2.3. We agree with the EDPB that the relevant legal framework for voice services is the GDPR (see para. 7 and 24 of the draft Guidelines). The GDPR indeed offers the necessary flexibility to tailor appropriate privacy-protective practices to the particular data processing at stake, as it articulates several legal bases for the data processing – including contract performance and legitimate interest.

## 2. CONTROLLERSHIP AND LEGAL BASES

### 2.1. *Actors in the VVA ecosystem*

- 2.1.1. In para. 15 there is an enumeration of different actors that voice assistants may involve. Retailers will often act as VVA application developer since they create applications extending the voice assistants default functionalities. In some cases, they would also act as owners by making available voice assistants in their stores. For example, today retailers often place computers in the store which allows the customer to search for information about a product, see if the product is in stock and, if so, where to find it. These computers may instead be replaced with VVA. In addition, retailers could also benefit from VVAs in stores when developing robots with the aim to enhance customer experience, e.g., to help a customer finding a product to its liking or assist in packing groceries.
- 2.1.2. The examples above illustrate how VVAs also could be used in brick-and-mortar stores to enhance and optimise customer experience. It is of great importance that the legal framework allows for use of existing digital services and does not hinder or affect companies' willingness to invest in digital innovation.

### 2.2. *Defining the roles of the VVA actors according to the GDPR*

- 2.2.1. The draft Guidelines provide that “[f]rom a high-level perspective, the designer may act as a data controller when determining the purposes and means of a processing but may intervene as a processor when processing personal data on behalf of other parties, such as an application developer” (para. 42 of the draft Guidelines). We welcome that the EDPB does not adopt a rigid position on how to define the roles of the VVA actors involved in the provision of a voice service. As the EDPB rightfully states, “the applicable qualifications have to be established on a case-by-case analysis” (id.).

In addition, when defining the roles of the VVA actors under the GDPR, we believe that there are similarities to Case C-40/17 (FashionID) where the CJEU found that joint controllership existed between the service provider (Facebook) and the website owner (FashionID) for the collection and transmission of personal data from FashionID to Facebook. In the case, the CJEU considered the fact that the website owner “exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without [embedding that social plugin on its website]”.

- 2.2.2. We would like to point out that the transfer of voice recognition data from the VVAs to the service provided by the VVA application developer works in a similar way. In this case, the VVA provider offers its service to a VVA application developer allowing it to connect its services to the VVA resulting in that the VVA provider and the VVA application developer would enter into joint controllership for the collection and transmission of personal data. Moreover, given the complexity of VVAs, a VVA provider could often also qualify as an independent controller when making the VVA application developer’s service available to users via its VVA. For instance, Example 2 in the draft Guidelines sets out that the bank is the data controller and the VVA provider the data processor without consideration of other potential qualifications of the roles.
- 2.2.3. In Example 2, when processing the customer’s voice input and other associated personal data and transmitting the content of the customer's request to the third-party application concerned, a voice service provider could very well independently determine both the purpose and the means of the processing. The purpose consists in performing the voice

service provider's contract with the customer, that is to say providing a voice service that interprets and responds to the customer's spoken requests. Regarding the means of processing, the voice service provider may also determine which data are collected (i.e., the customer's voice input and other relevant personal data), which data will be transferred (i.e., the relevant content of the customer's request as interpreted by the voice service provider), and to whom (i.e., the appropriate third-party application developer). Finally, the voice service provider may also independently be responsible for complying with its obligations to customers in respect of these processing activities (e.g., informing customers of the processing activities or responding to data subject requests).

- 2.2.4. This situation can be compared to the example of the travel agency ExploreMore in the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR. ExploreMore arranges travels on request from its individual customers. Within this service, they send the customers' personal data to airlines, hotels and organisations of excursions in order for them to carry out their respective services. Pursuant to the EDPB, "ExploreMore, the hotels, airlines and excursion providers are each to be seen as controllers for the processing that they carry out within their respective services. There is no controller-processor relation" (para. 29).
- 2.2.5. As with the travel agency ExploreMore, the voice service provider arranges voice experiences on request from its individual customers. Within this service, the voice service provider may sometimes send the customers' personal data to third-party applications in order for the developer of these third-party applications to carry out their respective services. Accordingly, each of the voice service provider and the developers of the third-party applications qualify as individual controllers in that situation. Careful considerations should be taken when assessing involved parties' controllership as it in fact could be a joint controllership.

We ask that the EDPB includes further examples of situations involving joint controllership in the Guidelines.

*Related paragraphs in the Guidelines: 42 and Example 2*

### 2.3. Purpose limitation and legal basis

- 2.3.1. In section 3.4 of the draft Guidelines, the EDPB identifies common purposes for the processing of personal data by VVAs and discusses the appropriate legal basis in relation to such purposes. For example, in para. 87 of the Guidelines, the EDPB states that "[i]f processing is not strictly 'necessary for the performance of a contract' within the meaning of Article 6(1)(b) GDPR, the VVA provider must, in principle, seek the consent of the data subject." As we understand it, the EDPB is worried that "reliance on legitimate interest could, in certain cases, risk undermining the additional level of protection provided by Article 5(3) of the e-Privacy directive" (para. 87 of the draft Guidelines).
- 2.3.2. Moreover, in para. 27 of the Guidelines, the EDPB states that the controller, when seeking consent according to Article 5(3) of the ePrivacy Directive, also must inform data subjects about all subsequent processing. According to the EDPB, consent under Article 6 of the GDPR will generally be the most adequate legal basis for all subsequent processing. However, no justification is presented as to why this is the case. In addition, Article 5(3) only applies to "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user." As set out in section 1.1 above, a VVA does not generally require storing or accessing information in the device of the user which would mean that the ePrivacy Directive in fact is not applicable. Regardless of whether the ePrivacy Directive would be applicable to VVAs, we do not agree that consent should be the most appropriate legal basis for the processing of personal data.
- 2.3.3. For example, we believe that "performance of a contract" under Article 6(1)(b) GDPR would be the most appropriate legal basis, for instance, for service improvement purposes or for certain content personalisation purposes, as the EDPB states (para. 85 of the draft Guidelines), because those purposes participate in the fundamental objective of a voice service, namely ensuring that customers can effectively and securely interact with the voice service. Additionally, depending on the role you have, e.g., a VVA application designer, the VVA

application designer may provide a service where the VVA designer has undertaken, as part of the agreement with the user, to personalise the content to facilitate user choices. For instance, assisting the user in finding a personalised selection of recipes according to the shopping lists created through the VVA. In these cases, consent would not constitute the most appropriate legal basis and does not offer any higher level of data protection than what “performance of a contract would”, namely because the data subject is both aware of the personalisation taking place by reason of the user agreement.

- 2.3.4. The pursuance of a legitimate interest can also constitute a valid lawful basis for data processing that is done by voice service providers. The voice service provider, for instance, has a legitimate interest in offering an attractive product that continues to improve and add new features over time, just as the customers have a legitimate interest in receiving new desirable features. With appropriate safeguards in place, such as an unconditional and easily accessible way to opt-out from the processing, Article 6(1)(f) GDPR can indeed be an appropriate lawful basis.
- 2.3.5. Retailers today face tough competition and must constantly develop their offer to the customers in order to stay relevant and competitive. Therefore, the legal framework must allow retailers to develop and package their services in a way that meets user demand and should not be restricted to one legal basis when benefitting from VVAs. In our opinion, it is unreasonable that consent would be the only available legal basis, and this cannot be the intended effect of Article 5(3) of the ePrivacy Directive. Other legal bases, such as “performance of a contract” or “legitimate interest”, provide in most instances for a strong, protective and much more appropriate lawful basis, which is ultimately up to the data controller to determine after a careful analysis of the processing at hand.
- 2.3.6. Indeed, the obligation for the data controller to decide the appropriate legal basis is made really clear in the Article 29 Data Protection Working Party (WP29) guidelines on DPIAs endorsed by the EDPB: *“it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR”*<sup>2</sup>. Moreover, the WP29 guidelines on legitimate interest provide that: *“In the first place, before a processing operation on the basis of Article 7(f) is to take place, the controller has the responsibility to evaluate whether it has a legitimate interest; whether the processing is necessary for that legitimate interest and whether the interest is overridden by the interests and rights of the data subjects in the specific case.”* If consent from the data subject is the only lawful basis it would counteract the whole purpose of the principles.
- 2.3.7. Lastly, the EDPB states that consent is required “for the storing or gaining of access to information for any purpose other than executing users’ request (e.g. user profiling)” (para. 29 of the draft Guidelines). We wish to bring to the EDPB’s attention that profiling is not a purpose in its own right but rather a means to an end to achieve the defined purpose. Common purposes where profiling is used is to provide the user with a personalised experience or to provide the user with relevant marketing. We therefore ask the EDPB to remove its reference to profiling in para. 29 of the draft Guidelines.

In light of the above, we ask that the EDPB:

- (i) **revises its statement concerning the necessity to seek consent from the user**, as it relies on an incorrect assumption *and* other lawful legal bases such as the performance of a contract or the pursuance of a legitimate interest under Article 6(1)(f) GDPR may be valid for data processing by voice service providers; and
- (ii) **removes its reference to profiling as a purpose for data processing in para. 29 of the draft Guidelines** as profiling merely is a means to an end, e.g. personalisation or marketing purposes.

*Related paragraphs in the Guidelines: 23, 27, 28, 29 and 85*

---

<sup>2</sup> wp248rev.01.

### 3. SERVICE IMPROVEMENT

- 3.1. In section 3.4.2 of the Guidelines, the EDPB analyses the appropriate lawful basis when processing personal data to improve the voice service's performance or to develop new functions within the voice service. More specifically, the EDPB considers the case where the voice service provider transcribes the customer's voice input and feeds it into the voice service's training dataset for machine learning purposes. The transcriptions of the customer's voice input are reviewed and corrected by humans. The EDPB concludes that such processing cannot be based on "performance of a contract" under Article 6(1)(b) of GDPR. According to the EDPB, "[t]he main reason being that VVAs are already functional when they come out of the box and can already perform as (strictly) necessary for the performance of the contract."
- 3.2. We believe this approach overlooks the similarities between maintaining and improving the performance of a voice service and traditional software debugging. Rather, the various types of data processing required to provide, maintain, or improve a voice service should each be independently analysed under Article 6(1)(b) of GDPR. Taking that approach, either contract performance or legitimate interest can be appropriate justification for the processing of customer data.
- 3.3. "Performance of a contract", in particular, can justify the quality assurance and quality control activities voice service providers engage in to ensure that services meet customer expectations. Contrary to the draft Guidelines, voice services are not always functional "out of the box" or always able to perform as needed or expected by customers. This is precisely illustrated in the example provided in the draft Guidelines where the customer of the voice service has to issue three times the same voice command due to the voice service not understanding it. The substance and fundamental objective of the contract between a voice service provider and its customers consists in ensuring that customers can effectively and securely interact with their voice assistant. To this end, the service must not only recognise specific speech patterns, vocabulary, dialects and grammatical structures (from proper to slang) in different acoustic environments but also adapt to the diverse and evolving nature of human voice. Moreover, it is not only the voice service providers that needs to improve and develop. The application developer also needs to use personal data to improve and optimise the service to function correctly and meet users' requests.

In light of the above, we ask that the EDPB revises its conclusion regarding service improvement purposes and consider Article 6(1)(b) of GDPR as an appropriate lawful basis.

*Related section in the Guidelines: section 3.4.2*

### 4. TRANSPARENCY

- 4.1.1. The draft Guidelines state that "data controllers should find a way to inform not only registered users, but also non-registered users and accidental VVA users" (para. 59).
- 4.1.2. Article 12 of the GDPR sets out a requirement on the controller to inform the data subject about the intended processing (e.g., purposes of processing, legal basis and retention periods). Because there is no purpose for the data controller to process personal data regarding accidental users in the first place, accidental processing should not be considered as intended processing. Therefore, it is unlikely that Article 12 of the GDPR is applicable on the processing of accidental users' personal data.
- 4.1.3. If accidental processing would be interpreted as intended processing, the data controller would be obliged to cater for all types of unintended processing outside the data controller's control (within and outside the VVA context), which would be an unreasonable and disproportionate obligation on the data controller.

- 4.1.4. In the event that Article 12 of the GDPR should be considered applicable on accidental processing, the involved VVA actors may have different obligations related to the provision of information. For example, the VVA provider may have the best opportunity to identify an accidental user and ensure that the information is delivered, whereas the VVA application designer should be responsible for what information to provide to the accidental user, and in some cases, the most appropriate person to inform accidental user may be the registered end-user of the VVA service.

In light of the above, we ask the EDPB to revise its statement on the obligation to provide information under Article 12 GDPR to accidental users as Article 12 of the GDPR only sets out an information requirement with regard to intended processing.

Moreover, in the event Article 12 of the GDPR should be considered applicable on accidental processing, we ask the EDPB to clarify the involved VVA actors' responsibilities to inform accidental users.

*Related section in the Guidelines: section 3.3*

## 5. ADDITIONAL COMMENTS ON SPECIFIC PROVISIONS

### 5.1. HIGHLY SENSITIVE DATA

- **On paragraph 31:** Sex or age is offered as an example of “personal data (...) highly sensitive in nature”. Even though both sex and age could indeed be processed in a way that can result in a risk to the rights and freedoms of data subjects (depending on the nature of processing, purpose and intended use of the outcomes of processing), sex and age as data categories by themselves are not considered as highly sensitive under the GDPR (e.g., they are not included in the list of special categories of data under Article 9 of the GDPR). Thus, EuroCommerce suggest removing references to “sex or age” from this paragraph.

### 5.2. DATA RETENTION

- **On paragraph 105, 107 and 140:** Since there is currently no tangible and concrete ways to anonymise voice recordings it would be helpful to have further guidance on how to sufficiently achieve this or, if deemed impossible/disproportionate, clarify that a margin of tolerance applies in relation to this issue.

### 5.3. DATA MINIMISATION

- **On paragraph 137:** The EDPB suggests rolling out settings by default that limit any data collecting and/or processing to a minimum required amount needed to provide the service. It is important to keep in mind that VVA is not a standard service but rather a personalised service. Hence the need to know more data, as needed to perform such personalisation.

Contact:  
Ilya Bruggeman - +32 2 738 06 41 - [bruggeman@eurocommerce.eu](mailto:bruggeman@eurocommerce.eu)

Transparency Register ID: 84973761187-60