23 April 2021

Comments by the Centre for Information Policy Leadership on the European Data Protection Board's Guidelines 02/2021 on Virtual Voice Assistants

On 9 March 2021, the European Data Protection Board (EDPB) issued its Draft Guidelines 02/2021 on Virtual Voice Assistants (Guidelines).[1] The EDPB invited public comments on this document by 23 April 2021. The Centre for Information Policy Leadership (CIPL)[2] appreciates the opportunity to submit the comments below as input for the final Guidelines.

CIPL welcomes the EDPB's initiative to provide Guidelines on the use of Virtual Voice Assistants (VVA or VVAs) to help organisations identify the risks associated with VVAs and implement the relevant mitigation measures. VVAs have become increasingly common in our daily lives due to the important benefits they can bring to individuals and society, from providing convenience to individuals in their daily life interactions and communications, to assisting people with disabilities or a dependency for whom the use of traditional interfaces is problematic. It is paramount that, in addition to ensuring consistency of approaches among Data Protection Authorities (DPA or DPAs), the Guidelines take a balanced approach that integrates the protection of personal data, the ability to provide a seamless user experience and the enablement of VVAs' functionalities. The Guidelines should also ensure they are aligned with existing guidelines of the EDPB (or endorsed by the EDPB) that are relevant for VVAs.

CIPL believes the Guidelines are sometimes not well aligned with current market practices and offerings and overlook the privacy-by-design controls implemented by some VVA providers. CIPL notes that there is a clear opportunity for the Guidelines to take strong leadership on a privacy-enhancing approach to VVAs which is also practical for organisations. In some instances, the Guidelines should be more nuanced and adaptable to account for the peculiarities of different VVAs and rapid technological developments. Without such flexibility, the Guidelines risk becoming quickly outdated. In this context, CIPL would like to point out the following areas of concerns and make several recommendations to help strengthen the Guidelines and ensure they can be duly implemented.

While CIPL hopes that the EDPB will consider these recommendations in finalising the Guidelines, CIPL would also respectfully request that, at a minimum, the EDPB (1) acknowledge that the implementation of the Guidelines may require significant work from VVA providers; and (2) recommend that DPAs focus primarily on proactive communication of the Guidelines to relevant stakeholders in the first six months after the publication of the final Guidelines, and refrain from proactive enforcement actions during this period in order to provide for a reasonable time for implementation.

---

[1] Guidelines 02/2021 on Virtual Voice Assistants—version for public consultation

[2] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 80 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

23 April 2021

1. **Need for a clear scope and definition of VVAs**

CIPL recommends the Guidelines refine the meaning of "Virtual Voice Assistant" so as to clarify the scope of this term. Paragraph 4 of the Guidelines introduces the concept of conversational agents. However, this description also encompasses audio input/output user interface that offer no assistant functionality. In other words, simple voice-based command interfaces or dictation functionality should not all be categorised as VVAs. Paragraph 8 considers that the capability for oral dialogue is the only criterion to determine if a software application is a VVA. However, not all software that have speech recognition and language understanding capabilities are VVAs. In the same vein, CIPL suggests that the example of callbots provided in Paragraph 5 of the Guidelines be updated, as callbots are not VVAs and, therefore, cannot serve as an example of the technology which the Guidelines seek to address. It is also important that VVAs are not defined as "terminal equipment" (see Paragraph 25 of the Guidelines) as further developed in Section 3 below. CIPL suggests the Guidelines define VVAs as conversational assistance software that has natural language understanding capabilities and which use AI to help the end-user perform certain tasks.

2. **Adequate distinction between the variety of VVA offerings**

CIPL welcomes the Guidelines' introductory remarks on the technology background of the VVAs to help readers better understand the functioning and ecosystem around VVAs. CIPL believes, however, that in the current terms, certain passages of the Guidelines could be read as generalising functionalities of VVAs and would thus benefit from adequately distinguishing between the varieties of VVA offerings available on the market. Examples of passages include:

- **"Due to their role, VVAs have access to a huge amount of personal data including all user's commands (e.g., browsing or search history) and answers (e.g., appointments in the agenda)"** (Executive summary–paragraph 2). **"[S]everal constants can be observed irrespective of the VVA type (i.e., type of device, functionalities, services or combination of them) that can be used by the data subject. Such constants relate to the plurality of personal data, data subjects and data processing at stake"** (Paragraph 33). **"[. . .] VVAs process personal data [. . .]"** and **"[c]urrently, all VVAs are connected to a user account and/or are set up by an application that requires one"** (Paragraphs 47 and 54). These statements seem to overlook the differing approaches to the collection of data by different VVA providers. For example, some VVAs do not require a registered user to be connected to a user account and do not process personal data within the meaning of the GDPR. In particular, privacy-preserving mechanisms such as the use of unique random identifiers associated with data collected enables some VVA providers to prevent voice utterances and other data from being tied back to the user including even where that identifier is shared with other applications. Some VVAs also allow for users to interact in privacy-enhanced modes like "incognito" or "guest" modes whereby less or no personal data is retained by the VVA provider. In these instances, data may, therefore, not be considered to be personal data under the GDPR. CIPL recommends these statements be rephrased to clarify that they relate only to VVAs where they process personal data within the meaning of the GDPR.

- **"[C]urrent VVA designs do not offer by default authentication or access control mechanisms"** (Paragraph 6). This passage should take into account VVA offerings that need to be enabled by the user, and, thereafter, require authentication for various uses based on the sensitivity of the data (for

example, the user may need to unlock the device to read a message, but could get an update on the weather without authenticating). More generally, the Guidelines should clarify that a VVA is only a new audio interface complementing other touch-based interfaces. Depending on the device surface, audio input/output user interface (UI) may be the dominant way by which users interact with assistants, but it is not the only type of user's interface, and we suggest the Guidelines consider these peculiarities. CIPL recommends that a number of passages in the Guidelines be revisited to consider whether the recommendations would be the same for touch-based interfaces. Where that is not the case, CIPL would encourage the Guidelines to clarify the reason behind the differences in treatment of the different modes of UIs. For instance, where Paragraph 6 suggests that smartphones with integrated VVAs are switched on by default, it illustrates a different attitude towards audio UI as opposed to touch-based UI. It is unlikely that anyone would consider that a keyboard or a multi-touch interface is "switched on by default" on a smartphone. Additionally, pre-installation is not the same as activation: VVAs can be not activated by default, which means the user has to set up on a new device and activate before being used.

- **"Each VVA names the components differently but all involve the exchange of the users' personal data between the VVA designer and the app developer"** (Paragraph 13). **"[A]lthough most VVAs do not share the voice snippet with the app developers, these actors still process personal data"** (Paragraph 14). These statements appear to overlook that in many cases, the VVA only enables the user to send a command or intent to the third party app developer. In addition, they do not account for VVAs which by default associate data with random identifiers, and, therefore, do not collect personal data within the meaning of the GDPR and cannot share such data with third parties.

- The VVA **"is constantly listening"** and **"[t]he user says the wake-up expression and the VVA locally compares the audio with the wake up expression. If they match, the VVA opens a listening channel and the audio content is immediately transmitted"** (Paragraphs 16(1) and 16(2)). CIPL suggests that the Guidelines try to avoid imprecise language and what could be considered superficial descriptions. Such statements are not helpful in the regulatory context because they overly simplify the complexity of VVAs and could be taken to mean that all data is de facto being processed by the VVA provider before the VVA is activated. This also is inconsistent with the description in Paragraph 16(2) that the listening channel is opened after the utterance of the wake up expression. Most VVAs are by default in standby mode waiting to be activated, and while they are in standby mode, no data is retained—just like the keys on a keyboard are in constant receptive or standby mode, ready to be pressed, but while they are in standby mode, no data is logged. In those scenarios, the wakeword is somewhat analogous to the finger on a keyboard—albeit wakeword detection is probabilistic rather than deterministic.

- In addition, VVA providers have approached the wakeword detection differently: some allow for the audio-streams captured by the device's microphone to be transmitted to the VVA's server for further processing, while others have invested in privacy-enhancing federating learning solutions that allow for on-device wakeword recognition, and some may do both. CIPL also suggests that the Guidelines refer to one consistent term when referring to "wakeword" as, at the moment, they use several terms to refer to the same concept of "activation word," "wake-up word," "wake-up expression," "keyword," etc. Additionally, the ideal term should be inclusive of non-verbal activation methods as VVAs providers may offer additional methods beyond verbal activation.

- The Guidelines describe the ability of VVAs to change states from passive to active processing and note that there is a **"substantial asymmetry of information with the user, who is hardly aware if the device is listening, and even less on the status in which it lies"** (Paragraph 50). CIPL believes this statement does not reflect the actual practice as it overlooks the differences of the standby mode (default state and the device is almost always in that state) and the activated state. Many VVAs also incorporate physical indicators (e.g., lights turning on when it gets activated) that help users understand what status the VVA is in. These statements do not account for VVA providers who have designed their services to include, for example, visual or haptic feedback when the VVA is activated. Paragraph 63 provides that all use feedback should be at least available in visual and acoustic format. CIPL underlines that this may not be appropriate for all VVAs.

3. **VVAs are not "Terminal Equipment"**

CIPL believes that the Guidelines conflate VVAs with terminal equipment (Paragraph 25) and, therefore, should not consider that Article 5(3) of the e-Privacy Directive applies as this is only the case where information is in fact stored or accessed on the terminal equipment (Paragraph 71). This expansive interpretation of terminal equipment would cause any VVA functionality, as well as an extensive range of other software to fall under the scope of the e-Privacy Directive.

The Guidelines describe VVAs as **"a service that understands voice commands and executes them or mediates with other IT systems if needed"** (executive summary, page 2) and **"a software application that provides capabilities for oral dialogue with a user in natural language"** (see Paragraph 8) which is accurate from a technical perspective. CIPL welcomes that the Guidelines consistently recognise that VVAs rely on a layer of physical infrastructure that varies across offerings in order to operate. The Guidelines also correctly illustrate VVAs as follows: **"a VVA is not a smart speaker but a smart speaker can be equipped with a voice assistant."**[3] Despite these accurate statements, the Guidelines consider that VVAs are "terminal equipment" in the same way that IoT devices such as smartphones and smart TVs are. CIPL considers that this analogy is technically incorrect and contradicts the very concept of VVAs provided for in the Guidelines as described above. The VVA is in itself an application layer which, like any other application layer (i.e., software), relies on a physical layer (i.e., hardware, such as a computer, mobile phone or speaker) to function.[4] CIPL believes the Guidelines should distinguish between (1) the audio input/output UI, (2) the assistant as a service and (3) the device on which the UI and/or assistant may operate. CIPL highlights that the device on which the VVA is running may be such terminal equipment, but the VVA as such is not the equipment.

Further, the e-Privacy Directive does not define "terminal equipment." The term comes from Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, which defines it as an "equipment directly or indirectly connected to the interface of a public

[3] Paragraph 11 of the Guidelines goes on to state that "It is common to confuse both of them, however, the latter is only a material incarnation of the former." CIPL highlights, however, that the end of the sentence should be rephrased the other way round as follows "the smart speaker is only a material incarnation of the VVA."

[4] The ISO's OSI reference model in this respect is a well-established technical description of the architecture of information technology systems and is instructive in demonstrating the clear differences between software interfaces (layer 7) from the physical transmission medium (layer 1) and all the other intermediary layers which separate those functionalities.

telecommunications network to send, process or receive information [. . .].” According to the Merriam-Webster online dictionary, an equipment refers to “the set of articles or physical resources serving to equip a person or thing.”[5] It is thus clear that the notion of “terminal equipment” refers to a physical device and does not cover services or the software underlying services. Construing the notion of “terminal equipment” as including services would make it impossible to delineate the exact scope of Article 5(3) of the e-Privacy Directive. A service is not something that one possesses as one would possess a physical device. Article 5(3) refers to “the terminal equipment of a subscriber or user,” which confirms that the terminal equipment is a physical device that does not include VVAs or other services as these cannot be possessed by an individual in the same manner as an individual would possess a physical device.

In addition, CIPL underlines that Article 5(3) of the e-Privacy Directive has to be read in conjunction with its Recital 24 which clarifies that Article 5(3) is intended to address situations where “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.” This is different from a VVA where a user’s device opens a stream to a cloud-based service that fulfils the user’s request, after being prompted by the user, and which does not implicate the use of spyware, web bugs, hidden identifiers, or other similar devices. When the user speaks to his/her device, the information is processed on the device or sent directly to the cloud for processing without the VVA service provider gaining access to the device itself, whether through spyware or other means.

CIPL believes that VVAs should not be considered as terminal equipment in and of themselves and that this characterisation is inappropriate and creates legal uncertainty with regard to the applicability of the e-Privacy Directive. CIPL recommends that the Guidelines in this respect be amended as it could have profound and unintended legal consequences for VVA providers. If not, this inadequate qualification would effectively bring software interfaces such as VVAs under the scope of the e-Privacy Directive and its national implementation laws with respect to all processing of personal data, and could lead to conflict with the well-established application of GDPR to such services. Taken to the extreme, this may be taken to mean that processing of personal data by software installed on hardware falling within the definition of terminal equipment would be under the scope of the e-Privacy Directive, which was certainly not the intention of EU lawmakers.

Furthermore, following the logic of the draft Guidelines, Article 5(3) would apply to any digital service that is accessed through a device. However, the European legal framework on data protection does not support this interpretation. First, Article 3 sets the scope of the ePrivacy Directive to comprise “the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.” In accordance with the CJEU, notably in *Google LLC v. Bundesrepublik Deutschland* (C-193/18), the definition of an “electronic communication service” mostly comprises the services provided by internet access providers and operators of the various networks of which the open internet is constituted (C-193/18, § 36). The e-Privacy Directive thus normally only applies to the services that are required to access the internet but not the digital services, such as a VVA service, that are provided *over* the internet. Second, applying Article 5(3) to any digital service that is accessed through a device would unduly limit the scope of the GDPR and extend the scope of the e-Privacy Directive.

[5] https://www.merriam-webster.com/dictionary/equipment.

The GDPR applies to the processing of personal data, including the processing of personal data in connection with digital services. The providers of such services notably need to choose one of the six available lawful bases provided for under Article 6 of the GDPR as appropriate for the processing at hand. If one would apply Article 5(3) of the ePrivacy Directive to all digital services simply because they are accessed through a device, this would limit the available lawful bases for a great proportion of processing activities in today's society as more and more services are in fact being digitalised. This cannot be the intention of the drafters of the EU lawmakers (see also section 5 below).

Article 5(3) of the e-Privacy Directive applies to "the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user." CIPL underlines most VVAs are used in tandem with terminal equipment and may also rely on cloud services: the voice recordings may be processed on device or streamed to the cloud when the user activates the VVA service. A cloud-based VVA does not generally require storing information or accessing information in the customer's device. By design, the streaming of the voice recordings to the cloud typically occurs when the voice command of the user activates the VVA service. When this happens, the VVA 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. The opposite happens: it is the user that initiates the streaming of the voice recordings to the servers of the VVA provider via the device rather than the VVA 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. It is like clicking on a hyperlink of a website, or entering text input into a search engine or other web application: the user makes a connection to the server to receive information without the server gaining any access to the user's device. It is also important that the EDPB align the Guidelines with its guidelines 3/2019 on processing of personal data through video devices that apply the GDPR (and not the e-Privacy Directive) to data processing linked to CCTVs and video devices, where data including images and voice are collected from such video devices.

More generally, CIPL understands that the relevant legal framework for VVAs is the GDPR as mentioned in Paragraphs 7 and 24 of the Guidelines. The core function of a VVA is to accurately recognise and respond to users' spoken requests. Users want VVA services to perform this function well for the entire duration 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 VVA services are diversified and complex, it is necessary to rely on different legal bases for the data processing, where a processing takes place. The GDPR indeed offers the necessary flexibility to tailor appropriate privacy-protective practices to the particular data processing at stake, as it articulates different and equally valid legal bases for the data processing.

4. **No hierarchy among legal bases for processing data by VVAs**

The Guidelines note that beyond the execution of the user request, consent may generally be the most adequate legal basis for subsequent processing of personal data, such as processing for improving a service or developing new functionalities within a service. As a result, other equally valid legal bases such as legitimate interests and contractual necessity, for instance, would be de facto unavailable for VVA related processing. By favouring consent over other legal bases, this position contradicts the fact that there is no hierarchy among legal bases under the GDPR. Further, this would also conflict with the EDPB's position that it is for the controller to ensure that the selected legal basis matches the objective and context of the

processing operation in question, consistent with the accountability principle.[6] Ruling certain lawful bases out from the outset eventually negates this principle.

CIPL disagrees with the interpretation that consent should be favoured in the context of VVAs and believes that other legal bases, such as performance of a contract or legitimate interest, provide in most instances for a strong, protective and much more appropriate legal bases than consent. Performance of a contract under Article 6(1)(b) of the GDPR constitutes the appropriate legal basis, for instance, for service improvement purposes or for certain content customisation purposes, as these purposes participate in the fundamental objective of a voice service, which is to ensure that users can effectively and securely interact with the VVA (see section 6 below). Legitimate interest can also constitute a valid legal basis for the VVA provider to offer an attractive and useful product that continues to improve and add new features over time where the customers have a legitimate interest (as third parties) in receiving new desirable features. The reliance on legitimate interests as a privacy-preserving legal basis is further strengthened by the requirement that it be accompanied by the appropriate safeguards under the GDPR, such as an unconditional and easily accessible way to object to the processing as per Article 21(1) of the GDPR.

Finally, Paragraph 88 of the Guidelines appears to imply that consent is required for profiling. CIPL recommends the Guidelines clarify that consent for profiling under the GDPR is not automatically required.[7] For instance, Article 21(1) of the GDPR enables individuals to object to personal data processing based on legitimate interests or public interests which includes "profiling based on those provisions"—acknowledging that a certain category of activities which result in the creation of profiles can be conducted on the basis of legitimate interests.

CIPL recommends an adaptation of the Guidelines to rectify the perhaps unintended suggestion that there is a hierarchy between the different GDPR legal bases and to acknowledge that legal bases such as the performance of a contract or the pursuit of a legitimate interest may be equally valid grounds for data processing by VVAs.

5. **Unintended effect of the e-Privacy Directive on the GDPR**

The Guidelines propose an unprecedented understanding of the interplay between the e-Privacy Directive and the GDPR. In particular, they seem to require consent under Article 6(1)(a) of the GDPR based on the view that consent would be required under the e-Privacy Directive, and that relying on a different legal basis under the GDPR would be lowering the additional protections provided by the e-Privacy Directive. Even if VVAs did fall within the scope of the e-Privacy Directive (which CIPL believes is not the case, see

[6] The WP29 guidelines on DPIAs endorsed by the EDPB are very clear that "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." Equally, 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."

[7] As per article 22 GDPR, consent is required in case of solely automated processing, including profiling, which produces legal effects concerning the user or similarly significantly affects the user, or where the processing relies on special category data.

Section 2), the Guidelines seem to infer that consent under the e-Privacy Directive would automatically restrict the range of available legal bases under the GDPR. Consent would be the only possible legal basis to the exclusion of other legal bases under Article 6 of the GDPR, supposedly because they are less privacy preserving. This assertion finds support neither in the text of the GDPR nor in the e-Privacy Directive. In addition, this overlooks the fact that legal bases such as contractual necessity and legitimate interest call for continuous assessment and oversight from the data controller on its processing operations which make these legal bases more accountable than consent and better aligned with a seamless user experience.[8]

In addition, CIPL believes that by subjugating the availability of the GDPR legal bases to the e-Privacy Directive requirements, the EDPB could find itself exceeding its statutory advisory functions and entering the realm of normative decision-making that is reserved to EU lawmakers. CIPL underlines that the relationship between the e-Privacy Directive and the GDPR is based on the principle *lex specialis derogate legi generali.* The EDPB has confirmed that Article 5(3) of the ePrivacy Directive shall take precedence over Article 6 of the GDPR with regard to the activity of storing or gaining access to information stored in the terminal equipment of a user, but that "any processing of personal data which is not specifically governed by the e-Privacy Directive (or for which the e-Privacy Directive does not contain a "special rule"), remains subject to the provisions of the GDPR and "there shall only be a derogation from the general rule insofar as the law governing a specific subject matter contains a special rule."[9] In other words, any data processing activity of the VVA that does not consist in storing or accessing information stored in the terminal equipment of a subscriber or user is not subject to the specific obligations of the e-Privacy Directive. In such cases, the GDPR shall remain fully applicable. We would recommend that the Guidelines are clarified in this respect and that the EDPB re-considers more generally the references to the e-Privacy Directive.

Finally, the Guidelines should clarify that DPAs should apply the cooperation and consistency mechanism provided by Chapter VII of the GDPR to VVAs, including in cases where some of the processing of personal data may rely on access to information stored in the end-user's device.

6. **Service Improvement is a core functionality of VVAs**

CIPL believes the Guidelines adopt a very narrow interpretation with respect to service improvements of the VVA by considering that the processing cannot be based on the contractual necessity legal basis as per Article 6(1)(b) of the GDPR. Subsequent processing by VVA in order to ensure users receive a satisfactory experience is an absolute necessity for the VVA provider and an essential step for ensuring that user requests can continue to be executed. As service improvements are a core component of the VVA services, making a distinction between service necessary for the performance of a contract and service improvements would be difficult, if not impossible. CIPL believes that the legitimate interest legal basis should equally be relevant in relation to the processing of personal data for service improvement.

The Guidelines consider that performance of a contract cannot be the appropriate legal basis as VVAs are already functional when they come out of the box and can already perform as (strictly) necessary for the

[8] See for instance CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data and Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR.
[9] See paragraphs 38 and 41 of Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. See also Recital 173 of the GDPR and Recital 10 of the e-Privacy Directive.

performance of the contract. CIPL believes this approach is out of sync with customers' expectations and overlooks the similarities between maintaining and improving the performance of a voice service and traditional software debugging where either contract performance or legitimate interest can be an appropriate legal basis for the processing of data.

Contract performance, in particular, can justify the quality assurance and quality control activities necessary to ensure that services meet customer expectations. In practice, voice services are not always functional "out of the box" or always able to perform as needed or expected by customers. The purpose of the service contract between a VVA provider and its customers consists in ensuring that customers can effectively and securely interact with their VVA. To this end, the service must not only recognize specific speech patterns, vocabulary, dialects and grammatical structures (from standard speech to slang) in different acoustic environments but must also be able to adapt to the diverse and evolving nature of human voice (see for instance example 7 of the Guidelines where the user of the VVA has to issue the same voice command three times due to the voice service not understanding it). VVAs must constantly learn how to interpret new and varied pronunciations of words and phrases that emerge or evolve over time.[10] Service improvements targeted at specific dialects, colloquial uses of language, or accommodating users with language impairments further ensure that voice assistants work well for everyone. As a consequence, maintaining a voice service that is able to correctly understand and respond to customers' evolving requests is necessary to meet customers' contractual expectations of how a voice service should perform.

Service improvements are also crucial in ensuring the security of the service. For instance, accuracy improvements help reducing so-called false wakes, where the voice service starts listening upon erroneously detecting a certain word as a wakeword. Providing a secure product is clearly part of the fundamental objective of the contract between the customer and the VVA provider. Voice service providers must, therefore, be able to rely on the performance of the contract under Article 6(1)(b) of the GDPR to learn from so-called false wakes to improve activation accuracy of the voice service and reduce their occurrence.

The Guidelines also consider the case where the VVA 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 may in some cases be reviewed and corrected by humans.[11] The EDPB concludes

[10] For example, before 2019 Lil Nas X was not a popular musician and customers did not typically request VVAs to play songs by this artist. In 2019, Lil Nas X became one of the most requested musicians, and VVAs had to quickly learn all the varied ways customers pronounce his name and request to play his music. This example perfectly illustrate that an effective VVA service cannot stay frozen in time but has to evolve with the humans it interacts with. Similar considerations would apply for terms such as "coronavirus," "Covid-19," "practicing social distancing" or "immunity passports" that were not commonly in use before the Covid-19 pandemic.

[11] Paragraph 23 of the Guidelines refer to human intervention in the learning and training of AI system as "digital labour" and notes that this part of the work "raises questions about both working conditions and safety." As the EDPB does not specify what those questions are from a privacy perspective, there is a risk that the Guidelines provide guidance outside of its remit. In addition, while some providers may use external expertise, others can exclusively rely on full time employees for these quality review processes. This has created thousands of quality jobs in Europe as a primary location for language review due to its educated, multilingual population. CIPL suggests that this language is removed. This paragraph goes on to note that "news media have also reported data transfers between VVA designers and subcontractors allegedly without the necessary privacy protection guarantees." CIPL

that processing cannot be based on "performance of a contract" under Article 6(1)(b) of the GDPR and should be based on consent. CIPL highlights that the EDPB should recognise the availability of alternative legal bases for this processing to take place for the effective operation of the VVA as consent may not be workable in practice: refusal to consent or withdrawing of consent could affect the service level quality and security of the VVA, especially when VVA improvement relies on artificial intelligence (AI) and machine learning. In addition, it is crucial that the Guidelines clarify that they apply to VVA only and are not intended to serve as general guidelines to be used for training all machine learning models.

Paragraph 145 of the Guidelines advises VVA offerings to minimise the necessity of having a registered user for their functionalities. This is a welcome position by those in support of VVAs built with privacy by design principles in mind. However, the Guidelines go on to note that services which do not require an identified user should not associate any of the VVA identifiers used to the commands and suggests that a privacy and data protection friendly default VVA would only process users' data for executing users' requests and would store neither voice data nor a register of executed commands. This approach appears to ignore that maintenance and improvement of a VVA in order to ensure users receive a satisfactory experience is an absolute legitimate interest of the VVA provider (see above). CIPL also points out that this mechanism is necessary for the proper execution of the user request, especially in relation to maintenance and improvements that ensure functionality. If a VVA is not providing results that meet user requests, the VVA will not be used and the service will suffer. CIPL would welcome recognition of this fundamental principle coupled with recommendations for how such service improvement can be achieved with minimal data. VVAs built with privacy by design and which do not require user registration for use of functionalities do offer additional mechanisms to ensure protection of user privacy in such circumstances. Examples include state of the art measures specially developed to ensure that only the required data is collected, and to implement privacy friendly features, such as randomised IDs, to prevent any identification of the user by anyone, including the VVA provider, attempting to tie together requests.[12]

7. **<u>VVA provider classification and controllership to be assessed on a case-by-case basis</u>**

CIPL welcomes the Guidelines' flexibility on the qualification of the different stakeholders involved in VVA services' processing activities and the acknowledgement that the qualifications have to be established on a case-by-case basis. In particular, it welcomes example 3 in Paragraph 43, as it recognises that the processing operations can be split up among independent controllers.

Paragraph 42 of the Guidelines,[13] however, appear to imply that an application developer is de facto a controller under the GDPR without clarifying that this is the case only where it determines the purpose and means of the processing. CIPL suggests that this sentence be reworked in accordance with Article 4(7) of the GDPR and the EDPB's Guidelines 07/2020 on the concepts of controller and processor. Further, example 2 in the same paragraph describes a bank application that the customers can query directly via the VVA. In

cautions that that unreferenced media reports may not be sufficient justification for a statement in Guidelines with important implications for organisations.

[12] Paragraph 145 suggests various data protection by default/design considerations, such as allowing to make a phone call or an Internet search without being required to be a registered user. The example of a phone call is misleading since, in practice, a phone call has to come from someone's phone number.

[13] Example 2 of Paragraph 42 and example 3 of Paragraph 43 also refer to the concept of a "designer." CIPL recommends referring to "provider of the VVA" for accuracy purposes.

this case, the Guidelines classify the VVA provider as the bank's processor without considering that a VVA provider may often be an independent controller, defining its own independent purposes and means of processing. This includes cases where that VVA provider makes third-party applications available via its voice service. For example, when processing the customer's voice input and other associated data and transmitting the content of the customer's request to the third-party application, a VVA provider may independently determine both the purpose of the processing (i.e., providing a voice service that interprets and responds to the customer's spoken requests) and the means of the processing (i.e., determining (1) which data are collected such as the customer's voice input and other relevant data, (2) which data is transferred, such as the relevant content of the customer's request as interpreted by the VVA service provider, and (3) to whom such data is transferred, such as the appropriate third-party application developer). Finally, the VVA 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). The Guidelines should be revised to reflect these various possible roles for the VVA provider, which must be assessed on a case by case basis.

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 travel on request from its individual customers. Within this service, it sends the customers' personal data to airlines, hotels and organisers of excursions in order for them to carry out their respective services. Pursuant to these guidelines, the travel agency, the hotels, airlines and excursion providers are each separate controllers for the processing that they carry out as part of their respective services and are not in a controller to processor relationship. As with the travel agency ExploreMore, the VVA provider arranges voice experiences on request from its customers. Within this service, the VVA provider may sometimes send the customers' data to third-party applications in order for the developer of these third-party applications to provide their respective services. Accordingly, each of the VVA providers and the developers of the third-party applications qualify as individual controllers in that situation. The Guidelines should, therefore, take into account in its banking application example that a VVA provider may also qualify as an independent controller when implementing a third-party application, with the classification of the different stakeholders ultimately depending on a case-by-case analysis.

8. **Reconsider the need for user level consent and provide for flexible methods of authentication**

The Guidelines provide that consent under Article 5(3) of the e-Privacy Directive needs to be connected to an individual user, as opposed to relating to a specific terminal equipment (see Paragraph 29). Subject to CIPL's strong recommendation in section 3 above, in case the final Guidelines confirm that Article 5(3) of the e-Privacy Directive is applicable, CIPL recommends that this paragraph be amended to provide that consent obtained at the device level is valid and sufficient for the purposes of the e-Privacy Directive and that individual consents "per user" may be recommended but are not required. The requirement under Article 5(3) that refers to the "terminal equipment of a subscriber or user" has been interpreted to mean that a consent provided by a user of a device is sufficient for a certain period, without the need to obtain a new consent or re-authenticate each time the website or app is visited from the same device. This means that different members of the same household may use a device and access the same website, or app without collection of consent or attempt to identify the relevant user upon each visit (unless of course certain important actions are being performed). Indeed, the Guidelines recognise that VVAs are multi-user (Paragraph 111) and that log-in mechanisms may not be required for all VVA functionalities (Paragraphs

111, 145 and 146). This is especially the case for VVA offerings that do not require an identified user for the provision of the service.

Having a different approach would mean that every time a user uses the VVA, he/she should be re-authenticated to verify that it is the same user that previously consented. Such a requirement may materially impair the VVA user experience and using the internet or other accessible resources. Further, this may result in a situation where VVA providers will have to require biometric identification each time a voice command is issued which would essentially mean processing special category data for each and every instruction issued by a user, which is not aligned with the principles of privacy by design and also not necessary for non-personal requests.

Finally, in Paragraph 112, the Guidelines suggest some authentication methods, such as a password, smart card or voice identification. CIPL underlines that users generally issue voice commands to VVAs as a convenience to avoid needing to use a keyboard or touchscreen. As a consequence, methods of authentication involving passwords or PIN codes would be wholly inconsistent with how users interact with VVAs, not to mention also that many VVAs do not incorporate or include a keyboard or a smart card reader. By contrast, a device-level consent on a VVA would enable the owner of the device to grant or decline consent in accordance with the e-Privacy Directive on unboxing and setting up the device. In addition, CIPL recommends that the Guidelines clarify that VVAs should promote user choice on authentication features, including allowing the user to decide on whether and how to enable authentication features within the options offered by the VVA provider.

9. **Transparency and exercise of data subject rights to be adapted to VVA specificity**

Paragraph 49 of the Guidelines provide that in accordance with their transparency obligations, controllers should inform all users, including registered, non-registered and accidental users. The Guidelines acknowledge however at Paragraph 58 that this may be difficult to achieve in practice. It is, therefore, not clear how the EDPB expects controllers to operationalise this provision in particular as far as accidental users are concerned. They may not be customers of the VVA provider and may not have access to the provider's privacy notices and be familiar with them.

The Guidelines state in Paragraph 56 that VVA providers should develop voice-based interfaces. If a privacy notice should be provided orally, CIPL underlines that this may be problematic for the controller to evidence that the notice was effectively listened to by such accidental user. This would be even more so if the VVA relies on random identifiers with no effective means to link back to any specific recording, or where users are in a privacy-sensitive guest or incognito mode. Further, such an oral notice is only possible where there is use of voice data for user identification (biometric data processing). Where biometric processing for the purpose of uniquely identifying a person is not carried out, the VVA may be unable to provide individualised "just in time" notices. Providing otherwise would appear to require all VVAs to actually process biometric data to single out individuals solely for the purpose of providing notice of the VVA operation. CIPL suggests the Guidelines remove these comments or provide further guidance on how they might be operationalised in practice in line with the GDPR's risk-based approach. The Guidelines should also clarify that it does not intend verbal interfaces to replace textual ones in relation to the provision of information for users. It should be entirely a matter for a VVA provider as to which is the most appropriate means to provide notice.

Paragraph 55 of the Guidelines implies that bundling notice across a variety of services is inherently noncompliant with the GDPR's transparency requirements. CIPL underlines, however, that although an overly lengthy notice may be insufficiently transparent, bundling services into one notice may in fact provide better transparency and readability and should be considered on a case-by-case basis.

Paragraph 152 of the Guidelines require that VVAs enable users, registered or not, to exercise data subject rights through easy to follow voice commands. For VVAs that do not engage in processing of biometric data to identify VVA users or do not require user registration for the provision of the service, the VVA device may be an inappropriate means to exercise data protection rights by the holder via voice commands, especially for right of access and deletion of data. Finally, there is substantial concern regarding how complex requests such as portability requests, can be processed by the controller via voice commands. CIPL would recommend the Guidelines be more nuanced and enable the exercise of data subject rights in the most efficient manner.

In addition, this overlooks VVAs that are built with a privacy preserving approach and have privacy built in by design, and do not process any personal data associated with the user. In some cases, the VVA provider is unable to search any data collected from the use of the service to identify the individual making the request, due to the manner in which the VVA has been engineered in order to protect user privacy. The exercise of data subject rights could inadvertently result in requiring collection of additional data and creation of detailed profiles of users, thereby undermining privacy for individuals. This cannot be the intention of the Guidelines. CIPL suggests the Guidelines recognise that the exercise of data subject rights cannot impose an obligation to re-identify individuals in accordance with Article 11 of the GDPR. This point is even more relevant for non-registered users, whose data subject rights may legitimately be limited on the basis of Articles 11(2) and 12(2) of the GDPR, i.e., where the requestor cannot be reliably identified as the individual.

Further, Paragraph 147 of the Guidelines seems to conflate interoperability and data portability. CIPL supports the suggestion that VVA providers should develop industry standards enabling data portability in accordance with Article 20 of the GDPR. However, CIPL notes that VVA is still a nascent service and the competition between different providers is strong, with differing models, technology and privacy preserving techniques. There are legitimate privacy concerns with regards to interoperability or concurrency of devices. CIPL suggests the Guidelines clarify what type of data is being considered to be in scope of the right to data portability in a VVA system. Data "provided by the data subject" through the VVA is likely to be rare, since most of the data specifically collected through VVAs will be commands that are not within the scope of Article 20 of the GDPR. The Guidelines should underline the inherent difficulty for effective exercise of portability rights.

Paragraph 161 states that the right to erasure could be hardly accommodated by anonymising personal datasets. However, the Guidelines should acknowledge that once data is made anonymous it is outside the scope of the GDPR. The Guidelines should refer to the WP29 guidelines 05/2014 on anonymization techniques to clarify that this is a statement about the inherent difficulty of successful anonymisation not a statement about the insufficiency of successful anonymisation.

10. **Rectify characterisation of biometric data**

The Guidelines provide that VVA providers could process special categories of personal data depending on the type of service requested by the user. Paragraph 14 of the Guidelines notes that the app developer receives intentions and slots that could include sensitive data. CIPL points out that "intentions" and "slots" are overly vague terms which do not necessarily qualify as personal data under the GDPR and therefore suggests that this wording be updated to clarify the EDPB's position here.

Paragraph 31 stresses that voice data is inherently biometric personal data. This statement is overly broad and inaccurate. While the data that results after some type of specific technical processing to extract unique characteristics of a natural person that allow or confirm identification of that person might be considered biometric data, mere recordings of voices are not biometric data, e.g., a voicemail is not biometric data in the way that a photograph is not biometric data. The EDPB's 3/2019 guidelines on video devices provide that "[t]o qualify as biometric data as defined in the GDPR, processing of raw data, such as the physical, physiological or behavioural characteristics of a natural person, must imply a measurement of these characteristics. Since biometric data is the result of such measurements, the GDPR states in its Article 4.14 that it is resulting from specific technical processing relating to the physical, physiological or behavioural characteristics." The video footage of an individual cannot however in itself be considered as biometric data under Article 9, if it has not been specifically technically processed in order to contribute to the identification of an individual. CIPL would suggest that, for the sake of consistency and legal certainty, that the EDPB apply the same reasoning to voice recording.

11. **Responsibility to protect children's data not shifted entirely on VVA providers**

Paragraph 91 of the Guidelines provides that "**data controllers should invest in developing means for parents or guardians to control children's use of VVAs**." Whilst CIPL supports the ongoing investment by VVA providers in means to ensure that parents and guardians remain fully informed of the use of VVAs by children, this statement appears to cast controllers as gatekeepers and to shift a portion of the responsibility for overseeing children's use of VVAs to them. CIPL assumes the Guidelines intend to indicate that controllers should seek to facilitate the exercise of this responsibility by parents and guardians in some way. CIPL suggests the Guidelines indicate ways in which this may be effectively operationalised.

Paragraph 93 of the Guidelines provides that when the legal basis for the processing is consent, processing of children's data is only lawful where the child is at least 16 years old or where consent has been given by the holder of parental responsibility over the child. CIPL highlights that this statement overlooks the fact that valid consent could be given in certain countries at ages 13, 14 or 15 years as per Article 8(1) of the GDPR. Therefore, CIPL suggests the Guidelines acknowledge the full provisions under Article 8(1) and the fact that there are Member States that have indeed provided for a lower age of consent than 16.[14]

[14] The EDPB may wish to consider guidance issued at Member State level, including by the Data Protection Commission of Ireland and the Autoriteit Consument & Markt in the Netherlands in relation to the processing of children's data to ensure a consistent approach to processing of children's data, including via VVAs in the EU.

12. **Relevance of availability of voice templates and voice recognition**

The Guidelines provide that voice recognition may only be activated "**at each use at the user's initiative, and not by a permanent analysis of the voices heard by the assistant**." The Guidelines explain that, when the voice service is set to permanently listen for the voice of a registered user, "**the voice of non-registered and accidental users will also be processed for the purpose of uniquely identifying them**" (Paragraph 132). CIPL highlights that this is necessarily factually inaccurate as users who wish to be recognized when using a VVA generally must train the voice service to recognize the user's voice. Depending on the type of VVA, they may do so by creating a "voice profile" to enable the VVA to recognize their voice. This may not, however, enable the VVA to recognize the voices of other users who have not created a voice profile. When the VVA analyses an unknown voice making a request (including, possibly, a voice from a non-registered user or an accidental wake), it does so to determine whether the voice matches a stored profile of a registered user who gave his/her consent to use the voice recognition feature. The voice service simply rules these users out as not the registered user without the possibility to identify him/her. Paragraph 130 of the Guidelines stating that "**the voice of non-registered and accidental users will also be processed for the purpose of uniquely identifying them**" is therefore inaccurate as the systems are not capable of uniquely identifying non-registered or accidental users.

The Guidelines provide for voice templates to be generated, stored and matched exclusively on the local device, and not in remote servers (Paragraph 133). CIPL underlines that this requirement is not consistent with the WP29 2003 working document on biometrics that recognises that the biometric template of a customer can be stored in several ways, including in a central database or on distinct databases.[15] Therefore, CIPL recommends the Guidelines be more nuanced and enable for several storage options as long as they enable compliance with the GDPR.

13. **Reasonable reliance on background noise filtering**

The Guidelines recommend in Paragraphs 139-140 that background noise filtering should be applied. CIPL highlights however that there is currently no known reliable mechanism to perform background noise filtering in the context of VVAs. Applying this in the absence of effective technology could result in a drop in quality, which could impair the accuracy of the VVA provider's processing of the user's instructions. This may lead to processing incorrect data, contrary to GDPR's Article 5(1)(d) data accuracy requirements. CIPL notes that the paper cited in footnote 50 of the Guidelines cites a 19% drop in automatic speech recognition accuracy, which is very significant.

In addition, noise suppression technology typically covers stationary noise, such as a computer fan or air conditioner running in the background and would not usually have any impact on voices in the background. It is technically challenging to isolate the sound of human voices because other noises also happen at the same frequencies. On a spectrogram of speech signal, unwanted noise appears in the gaps between speech and overlapping with the speech. This is why it is so difficult to filter out the noise—if a person's speech

[15] Some VVAs enable the processing operations to be performed locally in the customer's device, while others rely on the processing capabilities of the cloud. Cloud storage may enable users to interact with multiple voice service endpoints linked to their account, application of security updates from the cloud and recovery of data in case where the device is stolen.

and noise overlap, it is very difficult to distinguish the two. Instead, it would be necessary to rely on AI technology and train a neural network beforehand to distinguish between the sound of noise and the sound of speech.

More generally, the Guidelines attempt to apply to accidental data which cannot be considered personal data, such as pet noises, background music, and general sounds which are simply normal occurrences of everyday life. While CIPL understands the Guidelines' apprehension that background noise may be intentionally used to draw additional inferences about the individual without his/her awareness, it would be important for the Guidelines not to overly focus on secondary aspects which are naturally present in voice utterances, even where state of the art filtering techniques are deployed. According to CIPL, the focus in such instances should instead be that such inadvertent data collection is not used to draw such inferences.

CIPL is grateful for the opportunity to provide recommendations on the EDPB's Guidelines on Virtual Voice Assistants. If you would like to discuss these recommendations or require additional information, contact Bojana Bellamy, bbellamy@HuntonAK.com, Markus Heyder, mheyder@HuntonAK.com, or Nathalie Laneret, nlaneret@HuntonAK.com.

23 April 2021

Summary of CIPL Recommendations

1. Define VVAs as conversational assistance software that has natural language understanding capabilities and uses AI to help the end-user perform certain tasks;
2. Avoid over-generalisation and better account for the variety of VVAs offerings on the market and in particular VVAs that do not rely on the processing of personal data;
3. Clarify that a VVA is only a new audio interface complementing other touch-based interfaces;
4. Avoid oversimplification of the complexity of VVAs to suggest that data is processed by the VVA provider before the VVA is activated;
5. Clarify that a VVA is not in and of itself a terminal equipment and that the e-Privacy Directive only applies where information is stored or accessed on the terminal equipment;
6. Confirm that the GDPR is the relevant legal framework for VVAs;
7. Confirm that beyond the execution of the user request, absent a hierarchy between the different legal bases, processing can be based on any relevant legal basis of the GDPR;
8. Confirm the narrow application of the e-Privacy Directive does not restrict the full range of available legal bases under the GDPR;
9. Confirm the application of the GDPR cooperation and consistency mechanisms to VVAs;
10. Confirm that service improvement based on voice data and commands is a core functionality of VVAs enabling reliance on the contractual necessity or legitimate interest legal bases;
11. Confirm that VVA provider classification and controllership should be assessed on a case-by-case basis;
12. Remove the obligation for individual consents per user;
13. Clarify that VVAs should promote user choice on authentication features within the options offered by the VVA provider;
14. Adapt transparency and exercise of data subject rights to the particulars of the VVA at issue;
15. Do not require VVAs to process personal data to single out individuals solely for the purpose of providing notice of the VVA operation.
16. Recognise that the exercise of data subject rights cannot impose an obligation to re-identify individuals in accordance with Article 11 of the GDPR;
17. Indicate ways to effectively operationalise the exercise of rights by parents and guardians of children using VVAs;
18. Provide that the voice of non-registered and accidental users should not be processed for the purpose of uniquely identifying them;
19. Enable several data storage options as long as they enable compliance with the GDPR; and
20. Avoid focus on secondary aspects, such suppressing as background noise, as state of the art filtering techniques are nascent and may affect user experience.