



22 april 2021

An insurance perspective on VVA guidelines

On behalf of Dutch life and non-life insurance companies, we would like to react on the EDPB consultation of its guidelines on virtual voice assistants. Our main issue with the current guidelines is that these make it harder for companies to develop VVA's in the EEA.

The guidelines state that the only legal basis for other goals than executing a contract is consent and explains how this consent is to be obtained. In the executive summary, the EDPB speaks of the possibility to develop voice based interfaces in receiving consent. We do not think these voice based interfaces for receiving consent will be listened to, just like online manuals and privacy policies aren't read. Will these voice based interfaces have to be translated into 27 languages? How does a developer know that the consumer has listened to the interface/message? And also: only some (large/highly skilled) companies are able to develop these formats, where the average European business will likely have a very hard time.

We also do not understand what the EDPB means in its executive summary when speaking of the requirement to have at least one registered user and that a registered user for each functionality should be considered. We wonder what the EDPB exactly means: we believe a VVA's services should be limited to use by its registered user, or else family members would be able to receive information from each other. Or does it mean that for each single person there should be a separate log in for each service? Will it be possible to make use of voice as a biometric identification (which would be a separate goal)?

Another way in which these guidelines make the development of VVA's harder is by stating that controllers should refrain from the bundling of services in user accounts. We believe VVA's are often used as personal assistants/butlers: it is just this bundling of services with e-mail/streaming services that users expect. We hope that the EDPB will develop guidelines or formats for how to inform customers in a well written privacy policy on the processing, in stead of asking for this unbundling.

In the last line of page 2 regarding consent the EDPB speaks of prior consent under 5.3 ePrivacy. If we assume this consent is similar to GDPR consent, then we don't see how a VVA controller would be able to meet the threshold of informed/specific/freely given/unambiguous. In order to be freely given the consent should not be conditional to the provision of the service. Does this mean the provider of the service also has to provide a valid alternative which does not require consent? In the case of VVA services we find this difficult to meet. With the exception of the case of biometric identification, we found little explanation in the guidelines on how this requirement should be met for other uses. This would mean that it wouldn't be possible to process data for other goals than executing the requested services, such as improving the VVA's machine learning model, biometric identification and profiling for personalized content or advertising. This takes away important aspects of the business case for the controller, making it very hard if not impossible to offer VVA services within the EEA. This would cause the EEA to lag further behind from jurisdictions where less strict rules apply.

Page 3 third paragraph speaks of accidental collection and urges to check for a valid legal basis. The terminology 'accidental' seems to imply that the collection wasn't foreseen/thought of beforehand, so how could this data ever be in compliance with GDPR? We believe the legal grounds mentioned here should be thought of before any data is collected and a course of action should be thought out for each category, of which deletion is a possibility.

In the paragraph starting with "VVA providers/designers should consider that" the EDPB states that it's the designer's responsibility to ensure it's recording only the users voice and not someone else's. Doesn't the user have any responsibility for preventing accidental collection? If she/he uses the device in the middle of a busy shopping street, wouldn't that make it very hard for the providers/designers to ensure they only record the users voice? In order to avoid



recording background voices and situational information, VVA service providers should apply automated background-noise filtering. This would not only provide a technical challenge but - what is worse - it would also not always guarantee that the voice of other users is recorded in the process.

In the last paragraphs of the executive summary, the EDPB states that VVA services very likely fall in the category requiring a DPIA. Could the EDPB explain why it thinks this is the case and also provide some guidance on what this DPIA should consist of? This would be helpful, seeing that European companies will have to get information from a few American companies delivering VVA devices: how likely is it that companies such as Google will provide the necessary information?

When the EDPB in this last sentence of the executive summary speaks of information to users by voice or by a written notification, we don't understand what the EDPB wants to achieve and which GDPR article this refers to?

In paragraph 51 the EDPB discusses the role of VVA designers. We think that there is no clear division here on the responsibilities of VVA designers and developers, with the result that it is the 'integrator', i.e. bank/insurer or any other arbitrary party that offers a VVA, that will have to solve the 'privacy risks'.

Little is said in the Guidelines about the interoperability. If the technology of 1 designer takes over in a home, this automatically means that it depends on all integrators. Dependency is undesirable. We believe the network should be able to function independently from the provider. What is the point of view here of the EDPB?