



**GUIDELINES 2/2021 ON VIRTUAL VOICE
ASSISTANTS**
Reply to public consultation

23rd April, 2021

Regarding **Guidelines 2/2021 on Virtual Voice Assistants¹**, adopted on March 9, 2021 by the European Data Protection Board, **VERIDAS DIGITAL AUTHENTICATION SOLUTIONS, S.L.** (“VERIDAS”) appreciates this opportunity to submit certain comments to the public consultation.

VERIDAS is a Spain-based company specialized in biometry and digital ID verification. Considering VERIDAS’ knowledge of biometric technologies, its team believes their input on the topic could be interesting for the understanding and regulation of the processing of biometric data.

The company was founded in 2017 by das-Nano, S.L., a technology company specialized in High-Security Printing and supplier of 25 central banks worldwide, and BBVA, one of the 20 biggest commercial banks in the world.

In order to give context to our comments on the recommendations, we would like to provide the following information regarding the AI-based biometric technology.

How does AI-based biometric technology work?

Biometric engines models

Recently, biometric methods have been based on artificial intelligence (AI) and, more specifically, on computation with neural networks. Under this premise, the result of the processing is a numeric template (an irreversible mathematical descriptor as seen in Image 1 below) which depends on the artificial intelligence of the biometric engine (the system may also have other mathematical variants, but the AI algorithms are the main components of the model). This means that the same raw data (e.g. a voice segment), used as an input of two different engines (or even if it is the same engine but in a different version) will have, as an output, a different template. Moreover, with this model, it is not feasible to extract data from the template by an individual.

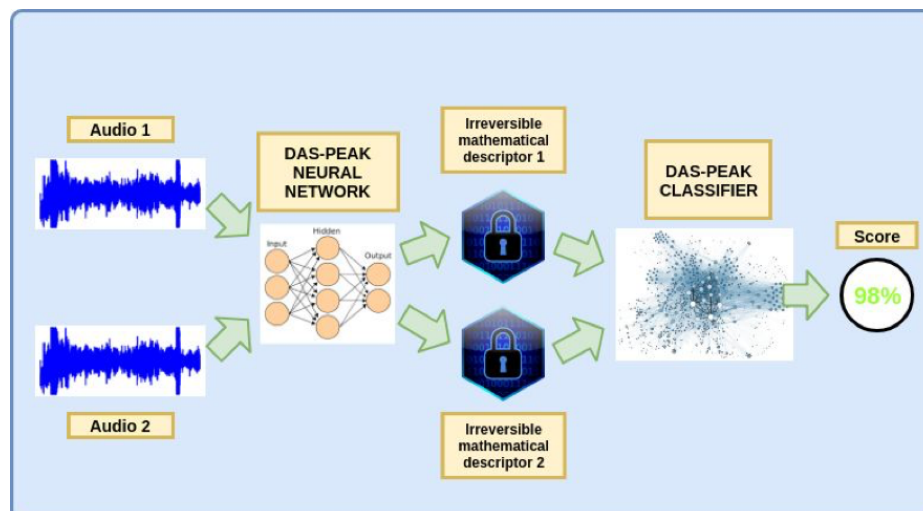


Image 1. Biometric engine based on neural networks

1

https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_022021_virtual_voice_assistants_adoped-public-consultation_en.pdf

Irreversibility

Given a template generated with a biometric engine that uses neural networks, it is not possible to obtain the raw data used to build such a template. This premise is still applicable even if the persons trying to obtain the raw data from the template are the scientists who designed the biometric system.

Biometric engine and specific versions of the biometric engine

With an AI-based model, a template generated with a biometric engine that uses artificial intelligence will only be understood by such a biometric engine and, more specifically, by the exact version of the biometric engine that was used to create it.

As previously explained, this is due to the artificial intelligence used in the generation of the template, which is unique per engine as it is affected by many factors.

If a template were to be disclosed to the public or among data controllers, its potential repercussions (even if no other security measures were taken, what should not occur) would be minimal.

Temporality

It is also important to understand that a template is only a representation of the subject's raw data at the moment of the capture, and that this data will only be used for comparison purposes and it does not provide any further information about the subject.

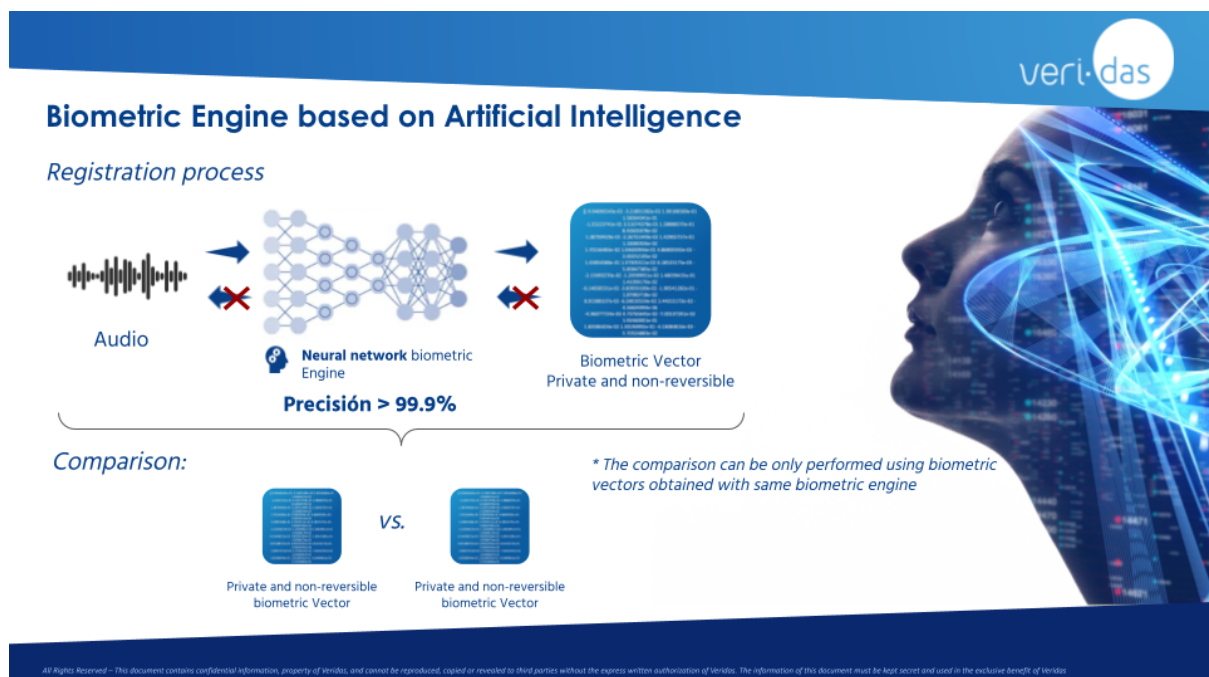


Image 2. How does AI-based biometric technology work?

Given the characteristics of these technologies, it might be advisable to undertake a thorough review of the current approach of biometric data. Active discussion between technologists, lawmakers, and policymakers is vital for all the parties to get a deep understanding.

The EDPB summarizes the measures to be analyzed by the data controllers so that the processing of biometric data can provide the maximum guarantees to the data subjects.

As a player on the identity verification and identification market, VERIDAS welcomes the EDPB initiative of regulating the processing of biometric data and establishing privacy standards so that biometric technologies, which have many benefits to offer, can be used safely. And, as developers of voice biometrics engines, VERIDAS considers that this regulation is also needed within this market.

In compliance with the legal requirements set by the General Data Protection Regulation [Regulation (EU) 2016/679] regarding, among others, the lawfulness of processing, information, and rights of the data subject, the work between lawmakers and technological experts would be, in VERIDAS' opinion, fundamental in order to continue determining the correct basis of the biometric technologies.

Comments on the recommendations

Recommendation paragraph 133: *"Voice templates should be generated, stored and matched exclusively on the local device, not in remote servers"*.

As players in the ID verification market, Veridas advocates secure systems for users. That is the reason why we are committed to the security offered by remote servers. We believe that to require companies to exclusively store and match the voice templates on the local device will prevent the users from the security offered by remote servers.

Furthermore, in order to be able to store and match the voice templates on the local device, the biometric engine must be installed on the local device. Given that the engine is where the Artificial Intelligence resides, it should be protected with maximum guarantees. In many scenarios it may be appealing to store the engine in remote servers as it allows for more comprehensive monitoring of safety measures and engine integrity. We believe that permitting the companies to select the better option in each case is the key to security.

It is also worth mentioning that restricting the storage of voiceprints to the device does not favor the usability of the solution (device-dependent) since it restricts its use to a specific brand and specific device. Ultimately this can make it difficult for other companies to enter the market, which may not favor market freedom within the EU.

In conclusion, we believe that having the opportunity to choose between a local device or a remote server, depending on the use case or situation, is the most advisable for the security of the users. Limiting an organization's options may eventually hurt the user's security.

Recommendation paragraph 135: *"If a VVA uses voice based biometric identification VVA providers should:*

- (...)

- *Ensure that the accuracy is similar for all user groups by checking that there is no substantial bias towards different demographic groups."*

We are committed to eliminate the bias that can be posed by biometric technology. The bias is not inherent to the technology, it is the result of inaccessibility of unbiased data bases on which the engines can be trained. We support the goal of erasing all bias from biometric technology at all cost, in fact we are of the opinion that this is essential in the time we live in. However, in order to achieve this goal we should correct the root cause. By making unbiased data bases more accessible, to solution providers we will be able to offer unbiased technology. Thus, it is important to bear in mind that this goal will always be dependable on the quality of data bases, which we encourage the EDPB to promote.