WHITE PAPER

ARMORVOX™ VOICE BIOMETRICS – SECURE BY DESIGN

How to Make ArmorVox the World's Most Secure Voice Biometric Solution

AURAYA

World Leaders in Voice Biometrics
info@aurayasystems.com
aurayasystems.com

Contents

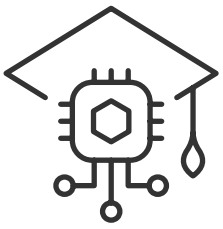
Abstract

When it comes to personal data, there is nothing more important and sensitive than our own individual biometric data. After all, it is this data that uniquely identifies us as individuals. Voice, like face and fingerprint, is a powerful biometric and Auraya takes data privacy and data security extremely seriously. We're so serious about it that the team at Auraya has designed ArmorVox to be 'secure by design'.

To practice what we preach, this whitepaper addresses the 14 steps that we have implemented to make ArmorVox the world's most secure voice biometric capability!

14 Steps to Security

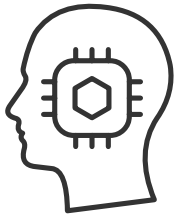
1. Retain Biometric Data Sovereignty with Embedded Machine Learning



Since the beginning, ArmorVox has implemented new machine learning technologies. These allow language independent operations and optimised accuracy. Most importantly, it ensures that end-users retain control and sovereignty over their customers' and citizens' Personally Identifiable Information (PII) voice data. Unlike other systems, which require end-users to record and transfer customers' and citizens' voice files to their centralised facilities for language and accent customisation and optimisation, ArmorVox's embedded machine learning technology

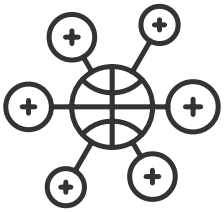
achieves language independence and optimises performance without any of the voiceprint data ever leaving the end user's secure infrastructure. This way, end-users retain complete control over their own customers' and citizens' voice biometric information.

2. Eliminate Single Point of Vulnerability with Individual Thresholds



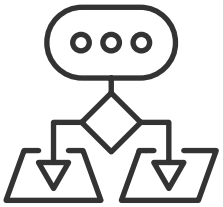
In a traditional system, a single global threshold is used for all enrolled voiceprints. This allows the security setting for the system to be secure whilst allowing some individual users to have very insecure voice prints. However, in ArmorVox, individual threshold settings can be computed using unique speaker adaptive algorithms. This optimises performance with increased accuracy and less vulnerability. It is critical to note that all voice prints can be made equally secure by having a computed threshold for each voice print that achieves the desired security point.

3. More Secure with Individual Speaker Specific Background Models



A background model controls the system's ability to discriminate between speakers. In traditional systems, a single Universal Background Model (UBM) is often used. In ArmorVox however, individual background models are created for each voiceprint. This patent protected innovation of Speaker Specific Background Models (SSBM) improves ArmorVox's ability to discriminate between voiceprints and remain language and accent agnostic.

4. Separate Personally Identifiable Information from Biometric Information



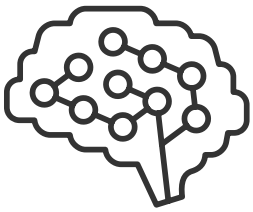
Business applications using ArmorVox utilise a client-server architecture. In this architecture, the business application containing customers' PII is implemented in the client; whilst ArmorVox, which stores the voice biometric information, is implemented separately as a 'server function'. In effect, the client-server architecture stores customers' PII and biometric information separately in different locations. This means that both types of information must be present to identify a customer's identity, keeping their identity safe from security threats.

Founded in 2009, Auraya is the world leader in voice biometric technology. Auraya focuses on empowering people and organisations to interact and engage with convenience and security.

5. Obfuscate Personally Identifiable Information in Voiceprint Index

To further enhance security, business applications using ArmorVox can implement an encrypted translation table that converts a speaker's personal identifier to a new identifier which is used to look up voice prints in the database. The allocation of this new identifier can be completely random. This way, the voiceprint identifier, which is internal to ArmorVox, cannot be used to infer the original identity of the voiceprint.

6. Operate ArmorVox As A ‘Stateless’ Machine

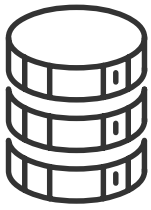


ArmorVox is a ‘stateless’ machine, making it highly scalable. More importantly for security, it has no notion of the 'state' or 'function' of the business application’s request for a voice enrolment or verification. As a 'stateless' machine, ArmorVox does not require session identifiers or the retention of any PII. Through this, ArmorVox complies with the GDPR requirements.

7. Immediately Destroy Voiceprint Data

ArmorVox performs an enrolment or verification process by comparing the acoustic analysis of a voice file submitted by a business application to the ArmorVox server. Upon receiving the voice file, the acoustic parameters are extracted and scrambled then the original voice file is immediately destroyed. Moving forward, the acoustic parameter can only be interpreted by ArmorVox. The acoustic parameter data can neither be played nor extracted for any PII. This allows ArmorVox to achieve compliance with the GDPR by ensuring that no PII is retained on the ArmorVox system.

8. No Logs or Audit Reports Retained in ArmorVox Servers



In addition to destroying voice files, ArmorVox's servers also do not retain any logs or audit reports which could potentially expose PII. Logs and audit reports that may be retained for business compliance purposes are saved by the client-side business application and separated from the voice biometric information saved on ArmorVox.

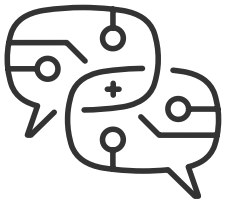
9. Secure Voiceprint Data with One-way Encryption

ArmorVox authenticates a speaker by comparing the acoustic parameter file against the voiceprint. Like the acoustic parameter file, the voiceprint is a blob of data representing the acoustic attributes of the speaker. Additionally, the voiceprint is a proprietary data set that can only be used by the ArmorVox voice biometric algorithm. There are no aspects of the voiceprint that are personally identifiable.

The voiceprint is not a .wav file and it cannot be played, or reverse engineered to expose the identity of the speaker or what they have said. The voiceprint is one-way encryption of the enrolment voice files that do not allow the reconstitution of the voice file. It cannot be used as an input to another voice biometric system to uncover the identity of the speaker. In short, the voiceprint that ArmorVox stores, on its own, is useless. As such, it does not constitute Personally Identifiable Information and complies with the GDPR requirements.

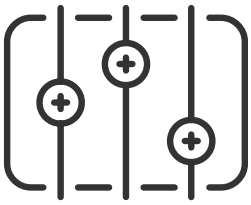
ArmorVox supports encryption of voiceprints providing additional protection and security of the voice biometric information.

10. Encrypt Client-Server Communications Protocols



Communications between the business application (client) and ArmorVox (server) is via published Application Programming Interfaces (APIs) using encrypted communications protocols (https). This ensures PII contained in the voice files in transit between the client application and the ArmorVox are secured and meet GDPR requirements to protect PII in transit.

11. Delete Voiceprint Data Securely on Command

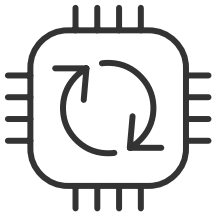


ArmorVox provides an API that allows business applications to command ArmorVox to destroy voiceprints and all associated acoustic parameter data. This ensures compliance with GDPR requirements and data privacy requirements.

"Auraya's deep experience in security and design of voice biometrics enables us to create technology to deliver your business requirements and allow you to achieve your goals."

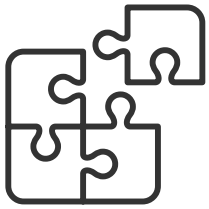
Paul Magee, CEO of Auraya

12. Superfluous Voiceprint Database Backups



As the voiceprints can be reconstituted from logged voice files, assuming the business application logs enrolment and verification voice files, which is typically the case for business compliance, then there is no need to back up the voiceprint database. As there is no need for backup, then there is no need to implement special data protection processes for backup copies of the voiceprint database. This makes complying with GDPR simpler and cheaper.

13. Stop Hackers with Tamperproof Voiceprints



To prevent insider attack, ArmorVox implements a voiceprint tamper detection mechanism which prevents a hacker from swapping speakers' voiceprints in the database. On enrolment, the index at which the voice print is stored is also embedded in the voice print data. On verification, ArmorVox extracts the embedded index to confirm that the voiceprint is at the correct location in the database. This way, if a hacker attempts to substitute one speaker's voice print for another, there is a mismatch in the indices resulting in ArmorVox returning an error condition.

14. Restrict Access to API Only Access

You can only access ArmorVox via APIs. As ArmorVox is a 'stateless' machine which does not retain any logs audit reports or customer information, then there is no need for the business applications operator to log into the system. All information is provided via the API requests and responses. This way, access to the ArmorVox server itself can be restricted ensuring a high level of security of the ArmorVox server and the voice biometric information saved on the server system.

Summary

The team at Auraya has developed ArmorVox as the next generation voice biometric capability to deliver a Biometric security capability that is easy for consumers to use, simple for IT teams to deploy and secure by design for security teams to rely on. The 14 steps outlined shows how we have taken the extra steps and further precautions necessary to provide a voice biometric capability that is ‘secure by design’. These steps were implemented to ensure compliance with laws and regulations globally such as the European Union’s General Data Protection Regulation.

The team at Auraya continues to improve ArmorVox and its machine learning abilities to provide better customer experiences and improve security in voice biometric implementations for all types of businesses.

For more information, please visit our website at aurayasystems.com and access our resources ranging from blog posts, case studies, press release and white papers.

AURAYA

World Leaders in Voice Biometrics

394 Lane Cove Road, Macquarie Park, NSW 2113, Australia

(02) 8999 4433 | info@aurayasystems.com | aurayasystems.com

Australia | United Kingdom and Europe | Americas | New Zealand | Asia