As the functionality of cloud information services increases, and the level of interest in gaining access to private data for private individuals and public figures, Verviam encrypts ALL data that can be considered as private, both personal and technical data, in transit,in process and at rest in accord with GDPR (the European Union General Data Protection Regulation), industry data privacy standards and best practice. Verviam NEVER accesses unencrypted data. The only time it is in clear text, is when it is input into a web browser. Verviam is an Identity Management Service provided by Trac-Car Proprietary Ltd, International House, 64 Nile Street, London, N17SR.

Verviam is an Identity Management Service provided by Trac-Car Proprietary Ltd, International House, 64 Nile Street, London, N17SR.

By accepting this policy you are giving consent to your personal and private data being encrypted in your browser, transported encrypted to Verviam servers, and stored encrypted in a high security encrypted database in the European Union, subject to and compliant with EU General Data Protection Regulation (GDPR) data privacy and security.

Data Privacy and Protection Policy

Verviam does not transport, store or access any private account holder data in an unencrypted form. This includes both personal and technical data and identifiers, and includes passwords,

PINs, and secrets, personal and demographic details. Encryption occurs at the time of account set up and configuration, in the account holder's browser, and data is only unencrypted on Verviam AWS perimeter protected servers to be immediately re-encrypted with stronger keys and algorithms, without exposure to any person, automated system or application.

The data is protected by the infrastructure security perimeter, and best practice security configuration on the AWS Cloud: See Verviam Security Measures and Controls

Access to account holder data is monitored by audit trails and logs. When an account is removed, Verviam removes all of the audit trails and logs about the account and account usage that it holds in digital storage. Verviam automatically generates a unique public private keypair that is used to encrypt account holders' JWT (JSON Web Tokens). These keys are stored using the AWS Key Management Service. The specifications for these keys are that they have a modulusLength: 4096, a Public Key Encoding of type: 'spki', a Private Key Encoding of type: 'pkcs8'. The key format is 'pem', a digital certificate encoded X509 file. The private key is used to encrypt the account holder's private data, including the scope of the JWT bearer tokens. The public key can only be used programmatically when an account holder presents a token prior to request forwarding to private account endpoints, to decrypt the scope of their JWT bearer tokens prior to forwarding to the account holders private applications and systems. The public private keypair is rotated every 90 days to ensure data security and token integrity. While Verviam stores the public key on behalf of the account holder and uses it to decrypt the JWT bearer token for validation of credentials, it is the responsibility of the account holder to ensure that the content of their endpoint requests is secure.

By continuing to set up an account, you acknowledge that Verviam does not hold or transport any unencrypted private account holder data. Verviam encrypts account holder data elements both at field level and at the TLS transport layer to ensure protection over the public internet, in storage and in use by the Verviam cloud infrastructure, platform and application services. Verviam personnel never access unencrypted account holder data, and do not have access to the account public/private keypair used to automatically encrypt and decrypt JWT tokens. These keys are protected by the AWS Key Management Service. Validation of tokens is performed on fields that are encrypted from the values set up by the account holder on registration. Only an account holder has access to unencrypted private data, at the point of entry in the account holder's browser.

By continuing, you also acknowledge that Verviam has no responsibility for the security of data on the account holder's device e.g. desktop, notebook or tablet computer, mobile phone or IOT device.