Overview

The Protection of Personal Information Act (PoPIA) regulates the collection, use and processing of personal information collected from an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person in South Africa. It sets conditions for lawful processing of personal information. The Information Regulator of South Africa monitors and enforces, among other tasks, compliance with PoPIA.

The **Yimilo Web Application** is built on and hosted by the AWS datacentre in Cape Town. All information is stored in encrypted format and hosted in a secure facility.

Cross Border Data Flow

Section 72 of PoPIA permits the transferring of personal information outside of South Africa subject to the following conditions:

- the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection (as described in PoPIA)
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
- the transfer is for the benefit of the data subject, as further stipulated in PoPIA.

AWS is vigilant about your privacy and data security. Security at AWS starts with our core infrastructure. Custom-built for the cloud and designed to meet the most stringent security requirements in the world, our infrastructure is monitored 24x7 to ensure the confidentiality, integrity, and availability of our customer's data. The same world-class security experts who monitor this infrastructure also build and maintain our broad selection of innovative security services, which can help you simplify meeting your own security and regulatory requirements. As an AWS customer, regardless of your size or location, you inherit all the benefits of our experience, tested against the strictest of third-party assurance frameworks.

AWS implements and maintains technical and organizational security measures applicable to AWS cloud infrastructure services under globally recognized security assurance frameworks and certifications, including ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1, and SOC 1, 2 and 3. These technical and organizational security measures are validated by independent third-party assessors, and are designed to prevent unauthorized access to or disclosure of customer content.

For example, ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to Personally Identifiable Information (PII) processed by public cloud service providers. This demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content.

These comprehensive AWS technical and organizational measures are consistent with the objective of PoPIA which is to protect personal information. AWS customers maintain control over their

content uploaded to AWS services and are responsible for implementing additional security measures based on their specific needs, including content classification, encryption, access management and security credentials.

AWS does not have visibility into or knowledge of what customers are uploading onto AWS services. AWS customers are ultimately responsible for their own compliance with PoPIA and related regulations. The content on this page supplements the existing Data Privacy resources to help you align your requirements with the AWS Shared Responsibility Model when you store and process personal data using AWS services.