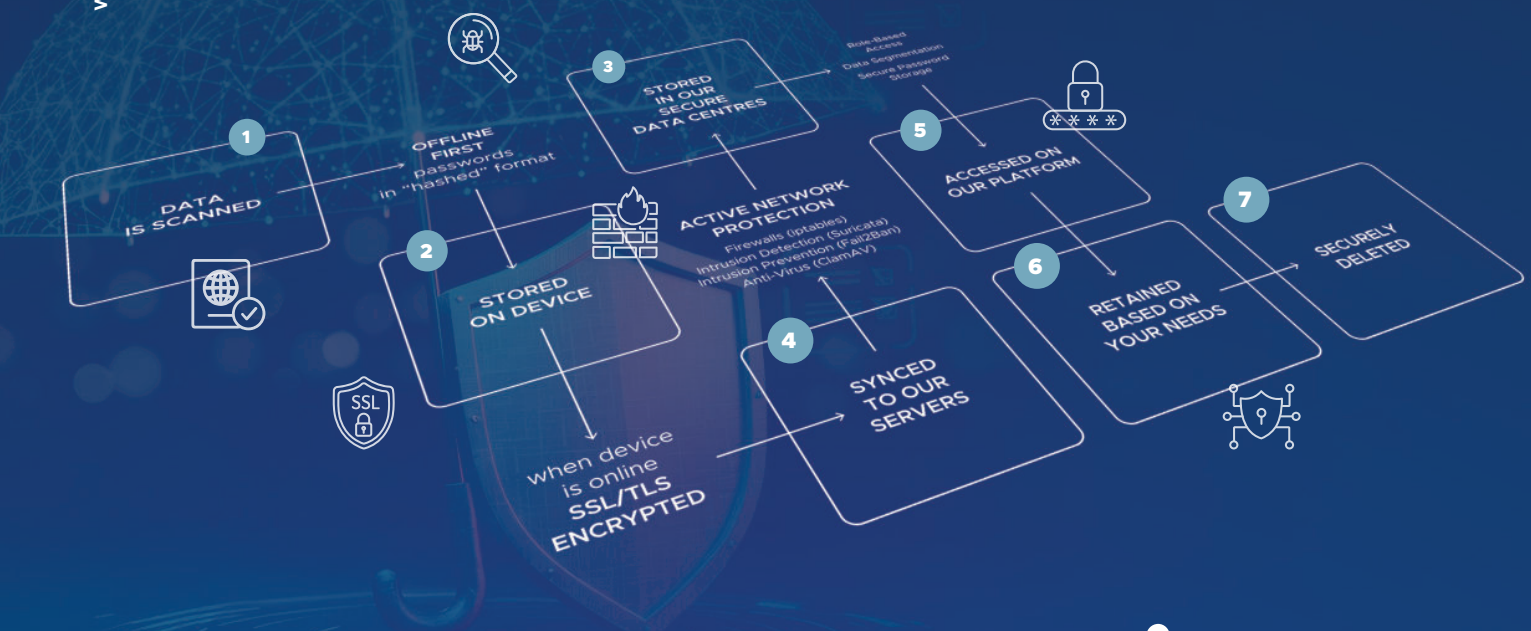
www.openitem.co.za

openitem



Data Protection

Keeping your information safe and secure

At Wyobi, we take your information—and your customers' privacy—seriously. Our systems and processes are built to comply with South Africa's Protection of Personal Information Act (POPIA). We want you to feel confident about how information is handled, so here's a quick tour of your data's journey with us: from the moment it's collected to when it's securely deleted.

Your data's journey follows seven key stages — it is **SCANNED**, **SECURELY STORED** on the device, **SYNCED** to our servers, **PROTECTED** within our secure data centres, accessed through **CONTROLLED PERMISSIONS**, **RETAINED** according to your requirements, and finally, **PERMANENTLY DELETED** when no longer needed.

TOP-LEVEL PRIVACY, SECURITY, AND COMPLIANCE

Openitem is fully compliant with POPIA, undergoes comprehensive penetration testing, and follows SOC standards with rigorous system controls to ensure data security.

YOUR DATA'S JOURNEY

DATA IS SCANNED

What happens: Users capture documents via mobile devices — including driver's licences, passports, vehicle discs, waybills, or other forms.

How it's protected: Data capture fields are predefined for your lawful purpose, ensuring only authorised information is collected.

DATA IS STORED SECURELY ON THE DEVICE

What happens: The platform works "offline-first," saving data securely on the device until connectivity returns.

How it's protected: Information is stored in a secure local database, with optional encryption. User passwords are hashed and never stored in plain text.

DATA IS SYNCED TO OUR SERVERS

What happens: Once online, data automatically syncs to our central platform.

How it's protected: All transfers use SSL/TLS encryption, preventing interception and ensuring end-to-end security.

DATA IS STORED IN SECURE DATA CENTRES

What happens: Data is hosted within the high-security OpenItem3 platform.

How it's protected: Data is stored in POPIA-compliant South African centres with 24/7 security, site replication, firewalls, and AES-256 encrypted, locked databases with secure backups (not accessible by the public).

DATA IS ACCESSED ON THE PLATFORM

What happens: Authorised users access data for reports or management tasks.

How it's protected: Access is controlled through role-based permissions, with data visibility limited by segmentation and all passwords securely salted, hashed, and stored.

DATA IS RETAINED BASED ON YOUR NEEDS

What happens: The default retention period is 2 years; however, this can be adjusted to align with your specific business requirements.

How it's protected: POPIA-compliant retention policies ensure no data is held longer than necessary.

DATA IS SECURELY DELETED

What happens: Data is stored for 2 years, after which the retention period ends or the user requests deletion. At that point, the data is permanently destroyed.

How it's protected: Secure deletion methods — including multi-pass overwriting or physical destruction — ensure complete, irreversible removal.

We trust this provides a clear and comprehensive overview of our unwavering commitment to safeguarding your data at every stage of its lifecycle.