safous

CLOUD-ROUTED, NOT CLOUD-HOSTED

Meet ASEAN Compliance Requirements With Safous

Keep credentials and data within your trust boundary at all times.

Data protection laws across ASEAN jurisdictions, including Singapore's PDPA, Thailand's PDPA, Malaysia's PDPA, Indonesia's Personal Data Protection Law, Vietnam's Decree 13/2023, and the Philippines' Data Privacy Act, require organizations to implement cybersecurity measures that protect personal data from unauthorized access and misuse.

Safous helps you implement secure, governed access aligned with these laws with a platform that keeps your credentials and data within your trust boundary at all times.

Safous and ASEAN Data Protection Laws

Requirement	How Safous Helps
☐ **Access Controls**	Enforces least-privilege access and MFA to prevent unauthorized access or misuse of personal data.
☐ **Data Minimization**	Enables role-based and just-in-time (JIT) access, so employees and third-party vendors get only the access they need.
☐ **Auditability**	Captures detailed logs and optional recordings managed within your environment through the AppGateway. These must follow retention, access, and deletion policies.
☐ **Purpose Limitation**	Restricts remote access to specific systems or functions to ensure personal data is only used for intended, consented purposes.
☐ **Security Safeguards**	Enforces TLS encryption in transit for all remote connections, reducing interception and tampering risk.
☐ **No Standing Access**	Credentials are vaulted and injected dynamically, and users never see or store passwords. Safous has no standing or administrative access to customer data or the AppGateway.
☐ **Retention & Deletion**	Session recordings and logs can be retained or purged per data retention policies.
☐ **Vendor Oversight**	Third-party access is brokered via Safous without direct VPN or broad network reachability. The Safous cloud is stateless and hosts no customer data; all control remains in your AppGateway.
☐ **Secure Transfers**	Sessions are routed via a stateless Safous cloud plane (routing/orchestration only). Session data and access governance remain inside your environment via the AppGateway, but cross-border legal requirements may still apply.
☐ **Breach Prevention**	Eliminates the need for exposed public IPs, VPNs, or agents on endpoints.
☐ **Data Residency/ Governance**	All privileged sessions, credentials, and logs are controlled and audited within your environment; no customer data is hosted in the Safous cloud.

safous

How Safous Supports Compliance

Safous offers:

- Agentless zero-trust remote access that **eliminates VPN exposure**
- **Role-based access controls** and dynamic credential vaulting
- Full session recording and logs to **simplify compliance audits**
- Access and session governance remain **inside your environment** with the AppGateway
- No customer data is **hosted in the Safous cloud**
- **Fast, flexible deployment** to support global and local data protection obligations

Safous uses a vendor-managed cloud plane only for stateless routing and orchestration. No customer data is hosted in the Safous cloud, and all session activities, credentials, and logs are governed within your environment through the on-premises Safous AppGateway. Safous personnel have no access to that data.

Get Started With Safous

Safous supports compliance with global and local data protection laws with a fully integrated Zero Trust platform designed to embed security, transparency, and accountability into every remote access session.

Contact us today to learn how Safous can help you meet privacy requirements across multiple ASEAN jurisdictions – all while strengthening your cybersecurity posture.

EXPLORE SAFOUS

safous

Safous provides technical and governance controls – including on-prem AppGateway enforcement and a stateless vendor cloud used only for routing/orchestration – that support compliance efforts. This does not itself establish a lawful basis for processing, satisfy consent/notice, create cross-border transfer legality, or fulfill statutory breach-notification, record-keeping, or rights obligations. Customers remain responsible for compliance.