Add value.
Inspire trust.

ISO/IEC 27018

Enhance cloud security for personally identifiable information

Your challenges

As a growing number of organisations move to the cloud, the data entrusted to public cloud service providers (CSPs) often includes personally identifiable information (PII), such as bank records, credit card details and passport information. Consequently, a security breach can severely impact large data volumes, with the hacking of sensitive information resulting in identity theft and financial loss. A PII security incident also attracts regulatory fines and reputational damage for both data owners and CSPs.

It is therefore vital that CSPs' customers can be assured that all the necessary cybersecurity checks and safeguards have been implemented. An effective information security management system (ISMS), which is specifically customised for security and privacy of PII protection in public clouds, reduces the risk of data breaches.

What is ISO/IEC 27018?

ISO/IEC 27018 (Information technology – Security techniques – Code of practice for protection of PII in public clouds acting as PII processors) serves as a guideline or code of practice for selecting PII protection controls within the process of implementing an ISO/IEC 27001-based ISMS in a cloud environment.

While ISO/IEC 27001 (Information technology – Security techniques – Information security management systems – Requirements) safeguards an organisation's information assets, ISO/IEC 27018 helps CSPs to protect the highly sensitive or critical PII entrusted to them by their customers. It also includes provisions for confidentiality agreements with CSP staff for PII processing and training.

Why is ISO/IEC 27018 important for your business?

The exponential increase in security incidents over the last few years has seen the safeguarding of cloud-hosted PII data become a priority. Data owners expect enhanced IT security in the presence of dynamic attack vectors and an ever-altering cyber threat landscape.

ISO/IEC 27018 guidelines are widely recognised as an independent measure for the evaluation and comparison of privacy controls, helping to mitigate the risk of data compromise. As compliance with the standard ensures that a CSP has appropriate procedures in place for handling PII, this can increase marketplace appeal and deliver you a competitive advantage.

How can we help you?

TÜV SÜD has the proven expertise and experience required to assess your organisation's cloud security safeguards, as per the guidelines of ISO/IEC 27018.

STEPS TO CERTIFICATION

Receive a customised quote from TÜV SÜD – including detailed costs and timescales

TÜV SÜD conducts an in-depth assessment

Our assessment report is released to you

Prepare your prioritised action plan, based on our assessment report

TÜV SÜD issues your ISO/IEC 27018 certificate

Your business benefits

- **Mitigate risk –** Safeguard the access, storage, transmission and processing of PII data by following ISO/IEC 27018 guidelines.
- **Gain a competitive edge –** Customers and data owners are assured that you implement appropriate security measures against PII data breaches.
- **Win customer trust –** A third-party certification by TÜV SÜD demonstrates your commitment to information security.

Why choose TÜV SÜD?

The experts across our global network have the proven knowledge required to provide complete ISMS and cloud PII security assessments, based on ISO/IEC 27001 and ISO/IEC 27018 guidelines. As TÜV SÜD is vendor agnostic, our assessments are both impartial and independent. Our auditors are accredited for the assessment and certification of a wide range of management system standards, so you also have the option to combine audits for multiple management systems, saving your business time and money.

Add value. Inspire trust.

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. It specialises in testing, certification and auditing services. Since 1866, the company has remained committed to its purpose of enabling progress by protecting people, the environment and assets from technology related risks. Through more than 24,000 employees across over 1,000 locations, it adds value to customers and partners by enabling market access and managing risks. By anticipating technological developments and facilitating change, TÜV SÜD inspires trust in a physical and digital world to create a safer and more sustainable future.

Related services

TÜV SÜD provides the following related management system services:

- ISO/IEC 27001 – Information security
- ISO/IEC 27017 – Cloud security
- ISO/IEC 20000-1 – IT service
- ISO 22301 – Business continuity
- ISO 31000 – Risk management

TÜV SÜD AG Westendstr. 199, 80686 Munich, Germany
+49 89 5791-0 systemcertification@tuvsud.com www.tuvsud.com/system-certification