

ISO/IEC 27018:2019

ISO/IEC 27018 provides guidelines for protecting personally identifiable information processed in public cloud services.



What it is

ISO/IEC 27018 is an international privacy framework that helps organizations protect Personally Identifiable Information (PII) processed by public cloud service providers. It establishes guidelines and controls for securing PII in cloud environments, supporting organizations' data protection and privacy management objectives in line with global compliance requirements.

Developed and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), ISO/IEC 27018 is widely adopted by cloud service providers, regulators, and enterprises seeking to ensure robust privacy safeguards. The framework builds on ISO/IEC 27001, focusing on privacy governance, risk management, and specific security measures for handling customer data in the cloud.

At a glance

PUBLISHER International Organization for Standardization (ISO)	TYPE Standard	VERSION 2014
EFFECTIVE 2014	DOMAIN Privacy	FAMILY ISO 27000 Series
REGION International	INDUSTRY Cloud & Technology Providers	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.iso.org/standard/27018>

Why it matters

- Strengthen data privacy safeguards** Bolster privacy controls and processes to ensure the confidentiality and integrity of personally identifiable information in the cloud.
- Enhance regulatory alignment** Support compliance with global data protection requirements, reducing the risk of legal penalties or contractual breaches.
- Improve audit readiness** Enable independent assessments of privacy practices and streamline preparation for customer, partner, or regulatory audits.
- Support risk-based decision making** Facilitate thorough risk assessments for cloud-based services, allowing organizations to address threats and vulnerabilities effectively.

How SmartSuite supports ISO 27018

PII Processing Control Library

Structure privacy controls for PII processing in public cloud environments.

Data Handling and Retention Governance

Track purpose limitation, retention rules, deletion requests, and evidence of execution.

Vendor and Subprocessor Oversight

Manage subprocessors, contract requirements, reviews, and assurance artifacts.

Privacy Incident and Breach Workflow

Run privacy incident response with documented timelines, decisions, and actions.

Requests and Data Subject Support

Manage access/deletion workflows and track responses with a clear audit trail.

Privacy Reporting and Readiness

Provide reporting on control status, open issues, and privacy assurance posture.

Common framework mappings

- GDPR
- ISO 27001:2022
- ISO 27002:2022
- ISO 27017
- ISO 27701
- NIST Privacy Framework v1.0
- SOC 2

Official resources

ISO/IEC 27018 Standard

Defines guidelines for protecting PII in public clouds, building on ISO/IEC 27001.

iso.org/standard/61498.html

ISO/IEC 27018 Implementation Guidance

Provides practical guidance for implementing ISO/IEC 27018 controls in cloud environments.

iso.org/publication/PUB100405.html

Frequently asked questions

What is ISO/IEC 27018 used for?

ISO/IEC 27018 provides a framework for protecting Personally Identifiable Information (PII) processed by public cloud service providers. It establishes privacy-specific controls to safeguard customer data and align cloud operations with global data protection and privacy laws.

Is ISO/IEC 27018 certification mandatory for cloud providers?

ISO/IEC 27018 certification is not mandatory, but it is widely adopted as a best practice for demonstrating a commitment to privacy in cloud environments. Organizations may choose to seek independent certification for ISO/IEC 27018 to meet regulatory expectations or customer requirements.

To whom does ISO/IEC 27018 apply?

ISO/IEC 27018 primarily applies to public cloud service providers that act as PII processors, but it is also relevant for any organization responsible for managing or outsourcing the processing of personal data to the cloud. The framework's principles benefit both data controllers and processors when assessing cloud privacy risks.

What are the key controls and documentation required by ISO/IEC 27018?

Key controls include requirements for data subject consent, transparency, purpose limitation, deletion procedures, encryption, access management, and third-party oversight. Organizations must maintain policies, risk assessments, data handling procedures, and evidence of privacy controls' effectiveness.

How is ISO/IEC 27018 implemented in practice?

Organizations typically integrate ISO/IEC 27018 controls into their existing information security management systems (ISMS), conduct PII-focused risk assessments, and map privacy controls to cloud service offerings and contractual agreements. Ongoing monitoring, training, and incident response processes are also essential for implementation.

How does ISO/IEC 27018 relate to ISO/IEC 27001 and other standards?

ISO/IEC 27018 is an extension of the ISO/IEC 27001 framework, adding privacy-specific controls for public cloud PII protection. It complements ISO/IEC 27002's general security controls and helps align with global legal requirements such as GDPR, supporting broader compliance programs.

What are the ongoing compliance obligations under ISO/IEC 27018?

Organizations must continuously monitor the effectiveness of privacy controls, update risk assessments, manage third-party relationships, address incidents, and periodically review compliance with the standard. Auditable documentation and continual improvement of data protection practices are required for sustained compliance.

How would SmartSuite support ISO/IEC 27018?

SmartSuite enables organizations to operationalize ISO/IEC 27018 by facilitating risk tracking, centralized management of privacy controls, and automated evidence collection. The platform supports audit readiness, compliance tracking, remediation workflows, and generates comprehensive reporting to demonstrate ongoing conformity with ISO/IEC 27018 requirements.

Framework text is licensed by its publisher and is included only where stated above.

Full framework page and mappings: smartsuite.com/frameworks/iso-iec-27018-protection-of-personally-identifiable-information-pii-in-public-clouds