SmartSuite

Framework / Privacy / ISO 27000 Series

ISO/IEC 27018:2025

ISO/IEC 27018:2025 gives guidelines for protecting PII in public clouds acting as PII processors, built on ISO/IEC 27002:2022 with an extended control set.



What it is

ISO/IEC 27018:2025 is the international standard of guidelines for protecting personally identifiable information (PII) in public clouds acting as PII processors, written for public cloud service providers and used by the customers that assess them. ISO and IEC published this third edition on August 26, 2025, prepared by ISO/IEC JTC 1/SC 27; it cancels and replaces ISO/IEC 27018:2019, which ISO withdrew the same day. It states guidelines, not conformity requirements, so organizations apply it rather than certify against it.

At a glance

PUBLISHER
International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

TYPE
Standard

VERSION
Third edition (ISO/IEC 27018:2025); replaces 2019 edition

EFFECTIVE
August 26, 2025

DOMAIN
Privacy

FAMILY
ISO 27000 Series

REGION
International

INDUSTRY
Cloud & Technology Providers

ADOPTION MODEL
Voluntary

IMPLEMENTATION COMPLEXITY
High

Source: iso.org/standard/88150.html

Why it matters

- **A common control set** ISO/IEC 27018 can serve as a common compliance framework for public cloud providers operating in a multinational market (Introduction 0.1).
- **Support for the contract** One stated objective is to assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement (Introduction 0.1).
- **Transparency for buyers** Another is to let the processor be transparent so customers can select well-governed cloud-based PII processing services (Introduction 0.1).
- **A route to audit and compliance rights** It gives customers a mechanism to exercise audit and compliance rights where auditing one customer's data in a multi-party, virtualized environment is technically impractical (Introduction 0.1).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ISO 27018

Selected Controls and Justifications

Record which ISO/IEC 27018 and 27002:2022 controls you select, the reason for any you leave out, and the owner of each (Introduction 0.4).

PII Requirements Register

Use Compliance Management to log the legal, contractual and policy requirements for PII that drive your choices (Introduction 0.3).

Processor and Controller Roles

Use Privacy Management to keep data inventories that show which processing you do as a PII processor and which as a PII controller (Introduction 0.1).

Sub-contractor and Supplier Oversight

Use Third Party Risk Management to assess and monitor the sub-contractors and suppliers named in your contracts (Introduction 0.4; Clauses 5.19 to 5.23).

Privacy Assessments and Risk

Run privacy assessments and track the risks and treatments they raise, with approvals and evidence attached (Introduction 0.3).

Audit Evidence and Reporting

Keep an audit trail of control status and open issues that you can share when a customer exercises audit and compliance rights (Introduction 0.1).

Common framework mappings

CSA CCM v4 · GDPR · ISO 27001:2022 · ISO 27002:2022 · ISO 27017 · ISO 27701 · NIST Privacy Framework v1.0 · SOC 2

Official resources

ISO/IEC 27018:2025 Standard

ISO/IEC 27018:2025, the third edition (August 2025), on the ISO catalog.

iso.org/standard/88150.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

Can an organization be certified to ISO/IEC 27018:2025?

ISO/IEC 27018 is a set of guidelines, not conformity requirements (Clause 1). It is meant to be used as a reference for selecting PII protection controls within an information security management system based on ISO/IEC 27001, or as guidance on its own (Introduction 0.2). Certification applies to the ISMS, not to ISO/IEC 27018 itself.

Who should use ISO/IEC 27018:2025?

Organizations of any type or size that provide information processing services as PII processors through public cloud computing under contract to other organizations (Clause 1). PII controllers can also find the guidelines relevant, although a controller usually carries additional obligations that the document does not specify (Introduction 0.2).

What changed from the 2019 edition?

The third edition cancels and replaces ISO/IEC 27018:2019. The Foreword lists two main changes: the text was aligned with ISO/IEC 27002:2022, and Annex B was added to show the correspondence with the 2019 edition. ISO withdrew the 2019 edition on August 26, 2025.

What is in Annex A and is it mandatory?

Annex A (informative) is the public cloud PII processor extended control set for PII protection, organized in line with the privacy principles of ISO/IEC 29100 (Introduction 0.2). Because it is informative and Clause 4.1 cross-refers to it, a provider applies the controls its requirements and risks call for and justifies any it leaves out (Introduction 0.4).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Does ISO/IEC 27018 cover a provider's own customer account data?

No. When a public cloud PII processor handles its customers' account data, it can be acting as a PII controller for that purpose, and the document does not cover that activity (Introduction 0.1, Note 1). The guidelines concern PII the provider processes for and according to the instructions of a cloud service customer.

License included / downloadable: No ISO/IEC 27018:2025 is a paid standard sold by ISO and national standards bodies, and the text is not included with the platform.

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

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.