# ISO/IEC 27018 Code of Practice for Protecting Personal Data in the Cloud

Third-party independent auditors validate that Microsoft in-scope cloud and professional services have incorporated ISO/IEC 27018 controls for the protection of personal data.

## Microsoft and ISO/IEC 27018

At least once a year, Microsoft business cloud services are audited for compliance with ISO/IEC 27001 and ISO/IEC 27018 by an accredited third-party certification body, providing independent validation that applicable security controls are in place and operating effectively. As part of this compliance verification process, the auditors validate in their statement of applicability that Microsoft in-scope cloud services and professional services have incorporated ISO/IEC 27018 controls for the protection of personally identifiable information (PII). To remain compliant, Microsoft cloud services must be subject to annual third-party reviews.

By following the standards of ISO/IEC 27001 and the code of practice embodied in ISO/IEC 27018, Microsoft—the first major cloud provider to incorporate this code of practice—demonstrates that its privacy policies and procedures are robust and in line with its high standards.

- **Customers of Microsoft cloud services know where their data is stored.** Because ISO/IEC 27018 requires certified cloud service providers (CSPs) to inform customers of the countries in which their data may be stored, Microsoft cloud service customers have the visibility they need to comply with any applicable information security rules.
- **Customer data won't be used for marketing or advertising without explicit consent.** Some CSPs use customer data for their own commercial ends, including for targeted advertising. Because Microsoft has adopted ISO/IEC 27018 for its in-scope enterprise cloud services, customers can rest assured that their data will never be used for such purposes without explicit consent, and that consent cannot be a condition for use of the cloud service.
- **Microsoft customers know what's happening with their PII.** ISO/IEC 27018 requires a policy that allows for the return, transfer, and secure disposal of personal information within a reasonable period of time. If Microsoft works with other companies that need access to your customer data, Microsoft proactively discloses the identities of those sub-processors.
- **Microsoft will comply only with legally binding requests for disclosure of customer data.** If Microsoft must comply with such a request—as in the case of a criminal investigation—it will always notify the customer unless it is prohibited by law from doing so.

## Microsoft in-scope cloud services

- Azure, Azure Government, and Cloud App Security
  Learn more
- Azure DevOps Services
- Dynamics 365 and Dynamics 365 U.S. Government
  Learn more
- Flow cloud service either as a standalone service or as included in an Office 365 or Dynamics 365 branded plan or suite
- Genomics
- Graph
- Microsoft Professional Services: Premier and On Premises for Azure, Dynamics 365, Intune, and for medium business and enterprise customers of Office 365
- Health Bot
- Intune
- Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense:
  Learn more
- OMS Service Map
- PowerApps cloud service either as a standalone service or in an Office 365 or Dynamics 365 plan or suite
- Power BI cloud service either as a standalone service or in an Office 365 plan or suite
- Stream
- Windows Defender ATP: Endpoint Detection & Response, Automatic Investigation & Remediation, Secure Score

## Audits, reports, and certificates

Microsoft cloud and professional services are audited once a year for the ISO/IEC 27018 code of practice as part of the certification process for ISO/IEC 27001.

**Azure, Cloud App Security, Flow, Genomics, Graph, Health Bot, Intune, OMS Service Map, PowerApps, Power BI, Stream, and Microsoft Datacenter**

- ISO 27018 Certificate
- ISO 27001 and 27018 Audit Assessment Report
- ISO 27001 and 27018 Statement of Applicability (SOA)

**Azure DevOps**

- ISO 27018 Certificate PII 665918

**Office 365**

- ISO 27001, ISO 27018, and ISO 27017 Audit Assessment Report
- Office 365 ISO/IEC 27001 Certificate IS 552878
- Yammer - ISO 27018 Audit Assessment Report

**Dynamics 365**

- Dynamics 365 - ISO 27018 Audit Assessment Report
- Dynamics 365 for Marketing - ISO 27018 Audit Assessment Report
- Dynamics 365 Parature - ISO 27018 Audit Assessment Report
- Dynamics 365 ISO 27001 Certificate IS 580851

**Microsoft Professional Services**

- ISO 27018 Certificate PII 642270

**Windows Defender ATP - Endpoint Detection & Response, Automatic Investigation & Remediation, Secure Score**

- ISO 27018 certificate
- ISO 27001 and 27018 Audit Assessment Report

## About ISO/IEC 27018

The International Organization for Standardization (ISO) is an independent nongovernmental organization and the world's largest developer of voluntary international standards. The ISO/IEC 27000 family of standards helps organizations of every type and size keep information assets secure.

In 2014, as an addendum to ISO/IEC 27001, the ISO adopted ISO/IEC 27018:2014 code of practice for protecting personal data in the cloud, the first global code of practice for cloud privacy. Based on EU data-protection laws, it gives guidance to CSPs acting as processors of PII on assessing risks and implementing controls for protecting PII.

## Frequently asked questions

**To whom does ISO/IEC 27018 apply?**

This code of practice applies to CSPs that process PII under contract for other organizations. At Microsoft, it also applies to the support of those CSPs.

**What is the difference between *personal information controllers* and *personal information processors*?**

In the context of ISO/IEC 27018: *Controllers* control the collection, holding, processing, or use of personal information; they include those who control it on another company's behalf; *Processors* process information on behalf of controllers—they do not make decisions as to how to use the information or the purposes of the processing. In providing its enterprise cloud services, Microsoft—as a vendor to you—is an information processor.

**Where can I see information about Microsoft compliance with ISO/IEC 27001?**

Review all the ISO/IEC 27001 compliance certificates, assessments, and reports for in-scope Microsoft cloud services on ISO/IEC 27001:2013 Information Security Management Standards.

**Can I use Microsoft compliance in my organization's certification process?**

Yes, you can use Microsoft attestation of compliance with ISO/IEC 27018 in conjunction with Microsoft certification for ISO/IEC 27001 in your compliance assessment. However, you are responsible for engaging an assessor to evaluate your implementation for compliance, as well as for the controls and processes within your own organization.

## Additional resources

- Data access policies for Microsoft enterprise cloud and professional services
- Azure data privacy and protection
- Microsoft Online Services Terms
- Microsoft Government Cloud