Ensure compliance with Copilot Studio's regulations.

In today's digital landscape, regulatory compliance is more important than ever. Organizations must adhere to numerous regulations and standards to protect sensitive data, maintain customer trust, and avoid legal consequences.

In today's digital landscape, regulatory compliance is more important than ever. Organizations must adhere to numerous regulations and standards to protect sensitive data, maintain customer trust, and avoid legal consequences. A crucial aspect of compliance is ensuring data storage, including storing and processing data within specific geographic areas. Microsoft Copilot Studio provides powerful features to help organizations meet critical compliance requirements, particularly regarding geographic data storage.

Why is compliance with regulations important?

1. **Legal requirements** : Many countries have strict data protection laws that regulate where data can be stored and processed. Failure to comply can result in hefty fines and legal action.
2. **Customer trust** : Adherence to compliance standards demonstrates a commitment to data security, which can enhance customer trust and loyalty.
3. **Risk management** : Compliance helps identify and mitigate risks associated with data breaches and unauthorized access.
4. **Operational efficiency** : Adhering to guidelines can help simplify processes and improve overall operational efficiency.

Copilot Studio is designed with compliance at its core and is an online service as defined in the Online Terms of Service (OST). It complies with or is protected by:

1. Health Insurance Portability and Accountability Act (HIPAA)
2. Health Information Trust Alliance (HITRUST) Common Security Framework (CSF)
3. Federal Risk and Authorization Management Program (FedRAMP)
4. System and Organization Controls (SOC)
5. Various International Organization for Standardization (ISO) certifications
6. Payment Card Industry (PCI) Data Security Standard (DSS)
7. The Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)
8. United Kingdom Government Cloud (G-Cloud)
9. Outsourced Service Provider's Audit Report (OSPAR)
10. Korea-Information Security Management System (K-ISMS)
11. Singapore Multi-Tier Cloud Security (MTCS) Level 3
12. High-level security measures Spain Esquema Nacional de Seguridad (ENS)

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a U.S. law that governs the requirements for the use, disclosure, and protection of personally identifiable health information. This provision applies to regulated organizations—physician's offices, hospitals, health insurance companies, and other healthcare companies—that have access to patients' confidential health information (PHI), as well as business partners—such as cloud and IT service providers—that process PHI on their behalf.

Microsoft Copilot Studio falls under the Business Partnership Agreement (BAA) framework of the Health Insurance and Accountability Act (HIPAA).

You can create agents to handle confidential health information when your organization is bound by HIPAA, such as in the following cases, where the agent can:

1. Individuals are required to provide their health information (blood pressure, weight, etc.).
2. Collecting health information and personally identifiable information, such as customers' IP addresses or email addresses.

Note : Although Copilot Studio falls under the HIPAA regulations, it is not designed for use as a medical device. See the disclaimer regarding the intended use of Copilot Studio and medical devices.

Health Information Trust Alliance (HITRUST)

HITRUST is an organization run by representatives from the healthcare industry.

HITRUST created and maintains the Common Security Framework (CSF), a certified framework to help healthcare organizations and their providers consistently demonstrate security and compliance.

CSF is built upon HIPAA and the HITECH Act, which are U.S. healthcare laws that establish requirements for the use, disclosure, and protection of personally identifiable health information and penalize non-compliance.

HITRUST provides a standard—a framework for standardized compliance, assessment, and certification processes—that cloud service providers and insured healthcare organizations can use to measure compliance.

Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP was established to provide a standardized method for evaluating, monitoring, and authorizing cloud computing products and services under the Federal Information Security Management Act (FISMA) and to accelerate the adoption of secure cloud solutions by federal agencies.

Microsoft's cloud services for government meet the requirements of FedRAMP.

By deploying protected services, including Azure Government, Office 365 US Government, and Dynamics 365 Government, federal and defense agencies can utilize a range of standards-compliant services.

Comply with SOC

A Service Operations Center (SOC) is a method for ensuring control and regulation within a service. Microsoft Copilot Studio has been audited and complies with the SOC.

The SOC audit report is available on the Microsoft Service Trust Portal .

ISO compliance

Microsoft Copilot Studio complies with the ISO standards listed in the following table. Audit reports for each standard are available on the Microsoft Service Trust Portal .

Standard	Report and certificate names	Link to the standard (www.iso.org)
ISO 9001:2015	Microsoft Azure, Dynamics 365, and Other Online Service - ISO9001 Certificate and Assessment Report	ISO 9001:2015
ISO 20000-1:2011	Microsoft Azure, Dynamics 365, and Other Online Service - ISO20000-1 Certificate and Assessment Report	ISO/IEC 20000-1:2011
ISO 22301:2012	Microsoft Azure, Dynamics 365, and Other Online Service - ISO20000-1 Certificate and Assessment Report	ISO/IEC 22301:2012
ISO 27001:2013	Microsoft Azure, Dynamics 365, and Other Online Service - ISO27001 and 27701 Certificate and Microsoft Azure, Dynamics 365, and Other Online Service - ISO27001, 27018, 27017, 27701 Assessment Report	ISO/IEC 27001:2013
ISO 27017:2015	Microsoft Azure, Dynamics 365, and Other Online Service - ISO27017 Certificate and Microsoft Azure, Dynamics 365, and Other Online Service - ISO27001, 27018, 27017, 27701 Assessment Report	ISO/IEC 27017:2015
ISO 27018:2019	Microsoft Azure, Dynamics 365, and Other Online Service - ISO27018 Certificate and Microsoft Azure, Dynamics 365, and Other Online Service - ISO27001, 27018, 27017, 27701 Assessment Report	ISO/IEC 27018:2019
ISO 27701:2019	Microsoft Azure, Dynamics 365, and Other Online Service - ISO27701 Certificate and Microsoft Azure, Dynamics 365, and Other Online Service - ISO27001, 27018, 27017, 27701 Assessment Report	ISO/IEC 27701:2019

Payment Card Industry (PCI) Data Security Standard (DSS)

Payment Card Industry (PCI) Data Security Standards (DSS) are a global data security standard designed to prevent fraud by enhancing controls on credit card data.

Organizations of all sizes must comply with PCI DSS standards if they accept card payments from five major credit card brands:

1. Visa
2. MasterCard
3. American Express
4. Discover
5. Japan Credit Bureau (JCB)

Compliance with PCI DSS is mandatory for any organization that stores, processes, or transmits payment data and cardholder data.

Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR)

According to the CSA STAR website :

1. The Security Trust Assurance and Risk (STAR) program includes key principles of transparency, rigorous auditing, and harmonization of standards. Companies using STAR demonstrate best practices and validate the security posture of their cloud services.
2. The STAR registry documents record the security and privacy controls provided by popular cloud computing services. This publicly available registry allows cloud service customers to evaluate their security providers to make the best purchasing decisions.

Microsoft Copilot Studio has been tested and complies with CSA STAR standards.

United Kingdom Government Cloud (G-Cloud)

Government Cloud (G-Cloud) is a UK government initiative aimed at simplifying cloud service procurement for government departments and promoting cloud computing adoption across the government.

G-Cloud includes a range of framework agreements with cloud service providers (such as Microsoft), and lists their services in an online store, the Digital Marketplace. This allows public sector organizations to compare and purchase those services without having to conduct a full evaluation process themselves.

Being included in the Digital Marketplace requires self-certification of compliance, followed by a verification process conducted by the Government Digital Service (GDS) at their discretion.

Outsourced Service Provider's Audit Report (OSPAR)

The OSPAR framework was established by the Association of Banks in Singapore (ABS), which developed IT security guidelines for outsourcing service providers (OSPs) wishing to provide services to Singaporean financial institutions. The ABS guidelines aim to help financial institutions understand the due diligence, vendor management, and critical technical and organizational controls that need to be implemented in cloud outsourcing agreements, particularly for large workloads.

Microsoft Copilot Studio has been OSPAR certified.

Korea-Information Security Management System (K-ISMS)

K-ISMS is a country/region-specific ISMS framework that defines a rigorous set of control requirements designed to help ensure that organizations in South Korea consistently and securely protect their information assets.

Singapore Multi-Tier Cloud Security (MTCS) Level 3

Singapore's MTCS standard was developed under the direction of the Information Technology Standards Committee (ITSC) of the Singapore Infocomm Development Agency (IDA).

ITSC ??promotes and facilitates national programs aimed at standardizing ICT and communications, as well as Singapore's participation in international standardization activities.

High-level security measures Spain Esquema Nacional de Seguridad (ENS)

In 2007, the Spanish government enacted Law 11/2007, establishing a legal framework allowing citizens electronic access to government and public services. This law forms the basis of the Esquema Nacional de Seguridad (National Security Framework), which is governed by Royal Decree (RD) 3/2010.

The goal of this framework is to build trust in the provision of e-services and ensure access, integrity, availability, authenticity, security, traceability, and preservation of data, information, and services.