

Defining the Microsoft Compliance Envelope Model



AI & Data Governance Series

Dr. Colin Beech, CEO

September 10, 2026

Table of Contents

Abstract	2
The Problem: Compliance Is a System Property	2
Defining the Microsoft Compliance Envelope.....	3
The Layers of the Envelope	4
Regulatory Layer	4
Contractual Layer	4
Service Layer	5
Identity Layer	5
Data Layer	5
Application and Integration Layer	5
AI Processing Layer.....	5
Audit Layer	5
Inside, Conditional, and Outside	6
The Compliance Envelope and Artificial Intelligence	6
The Envelope Is Traversed by Data, Not Products.....	7
Shared Responsibility	7
From Concept to Governance Artifact	8
A Better Question for Regulated AI.....	8
Conclusion.....	9
References.....	9

The Microsoft Compliance Envelope

A Control-Boundary Model for Regulated Data and Artificial Intelligence

Abstract

Organizations increasingly operate regulated workloads across interconnected Microsoft cloud services rather than within a single application, server, or security perimeter. Identity may reside in Microsoft Entra ID; operational data in Azure SQL or the Dataverse of the Microsoft Business backend; documents in SharePoint; classification and data-loss controls in Microsoft Purview; application logic in Power Platform or Azure; and artificial intelligence capabilities in Microsoft-hosted AI services such as CoPilot. Traditional descriptions of a “secure environment” are consequently inadequate. Compliance does not arise merely because each component carries a Microsoft brand, nor because an individual cloud service possesses a particular certification.

This white paper explores and refines the **Microsoft Compliance Envelope**¹ as an architectural model for defining the complete set of services, identities, configurations, contractual assurances, technical controls, data flows, and governance mechanisms within which regulated information may be processed. The model is particularly useful in the context of Large Language Model (LLM), or generative, artificial intelligence. Instead of asking whether an organization may broadly “use AI with regulated data,” the Compliance Envelope reframes the question:

Can a particular AI workload be constructed so that regulated information remains within an explicitly defined, controlled, auditable, and contractually appropriate processing boundary throughout its lifecycle?

The Problem: Compliance Is a System Property

Modern information systems are compositions. A single business process might involve a user authenticated through Entra ID, a Power Apps interface, records stored in Dataverse, documents retrieved from SharePoint, API calls executed through Azure services, monitoring through Azure Monitor, classification through Purview, and analysis by an artificial intelligence service. Assessing any one of these components in isolation provides an incomplete picture.

An organization may select services capable of supporting HIPAA, FedRAMP, IRS Publication 1075, or another regulatory framework while nevertheless constructing a workflow that moves regulated information into an inappropriate service, geography, identity context, external connector, unmanaged endpoint, or downstream system. This is almost always inadvertent, but nevertheless consequential.

¹ “Microsoft Compliance Envelope” is a conceptual framework proposed by Public Computing Consultants LLC in this paper and is not the name of a Microsoft product, certification, or formally defined Microsoft architecture. The framework synthesizes Microsoft's established concepts of compliance boundaries, data security boundaries, geographic boundaries, shared responsibility, information protection, identity and access control, and workload-specific governance into a unified architectural model for regulated data processing.

Compliance must therefore be understood in a holistic fashion as a property of the entire information-processing system and its data flows, rather than as an attribute inherited automatically from its technology vendors.

Microsoft's own documentation reflects this distinction. Microsoft describes both environment-guaranteed compliance boundaries and compliance boundaries that customers construct through architecture, policy, encryption, and configuration². Microsoft guidance for AI similarly emphasizes maintaining data security boundaries and preventing sensitive information from reaching unauthorized AI endpoints³. The question is therefore not simply:

Is this Microsoft service compliant?

The more useful question is:

Does this transaction remain inside the compliance boundary established for this workload?

Defining the Microsoft Compliance Envelope

For the purposes of this model, Public Computing Consultants proposes the following definition of the Microsoft Compliance Envelope:

The explicitly defined collection of Microsoft cloud services, organizational identities, data repositories, configurations, security controls, governance policies, contractual commitments, geographic constraints, audit mechanisms, and approved integrations within which a specified class of regulated information may be stored, transmitted, retrieved, transformed, or processed while maintaining the organization's required compliance posture.

The Compliance Envelope is therefore not synonymous exclusively with a Microsoft tenant. It is also not synonymous with Azure, Microsoft 365, Power Platform, or any particular licensing arrangement. Rather, the envelope is workload-specific and data-specific. An organization might maintain one envelope for ordinary internal business information and a substantially narrower envelope for protected health information, Federal Tax Information, criminal justice information, controlled unclassified information, or another regulated data class.

A service may consequently be inside one Compliance Envelope while remaining outside another.

² Microsoft, "Risk Assessment Guide for Microsoft Cloud," *Microsoft Learn: Microsoft Service Assurance*, last updated May 17, 2024, <https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide>

³ Microsoft, "Govern Azure Platform Services (PaaS) for AI," *Microsoft Learn: Cloud Adoption Framework*, accessed September 10, 2026, <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ai/platform/governance>

The Microsoft Compliance Envelope Model

A visual model for keeping regulated data within defined, controlled, and auditable boundaries.

Compliant AI isn't just about which tools you use — it's about how the data flows.

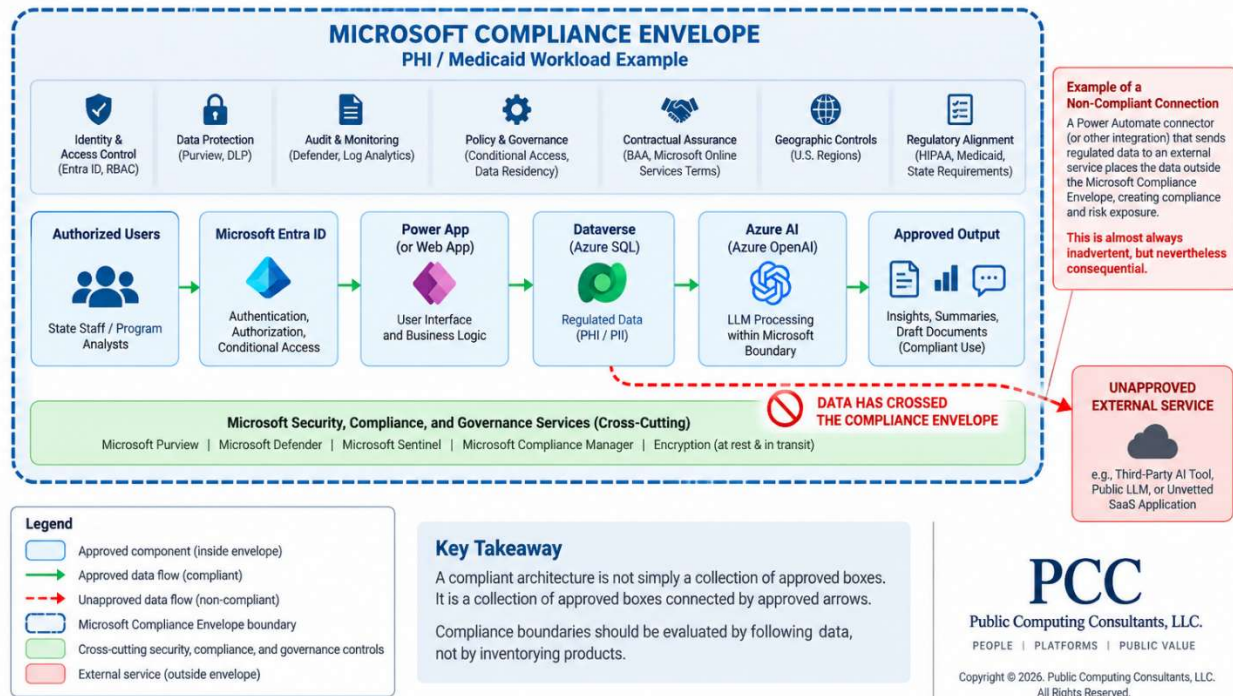


Figure 1: The Microsoft Compliance Envelope

The Layers of the Envelope

The Microsoft Compliance Envelope can be modeled through a series of intersecting control layers.

Regulatory Layer

The outermost requirement is established by law, regulation, contract, policy, or data-use agreement. This layer answers the fundamental question:

What obligations apply to this information?

Examples may include HIPAA, state privacy requirements, IRS Publication 1075, FedRAMP requirements, contractual confidentiality provisions, or organization-specific information handling policies.

Contractual Layer

A technically secure service is insufficient if the contractual relationship does not permit the intended processing. This layer includes applicable Microsoft contractual commitments, data protection terms, business associate arrangements (BAAs) where required, subcontractor or sub-processor provisions, and organization-specific agreements governing the information.

Service Layer

Only explicitly evaluated services should be considered inside the envelope. The inclusion of one Microsoft service does not imply inclusion of every Microsoft service. Azure SQL, Dataverse, SharePoint, Power BI, Azure AI services, Fabric, Power Platform connectors, and third-party integrations must each be evaluated in the context of the workload.

Identity Layer

Microsoft Entra ID and associated identity controls establish who or what may cross the envelope. Controls may include role-based access control, conditional access, managed identities, privileged identity management, multifactor authentication, service principals, application permissions, and least-privilege authorization.

Data Layer

The data layer determines where regulated information may reside and how it must be protected. Controls may include encryption, Microsoft Purview sensitivity labels, data-loss prevention policies, retention policies, geographic residency requirements, customer-managed keys, database security, and document-level permissions⁴.

Application and Integration Layer

Applications define how information moves. Power Apps, Power Automate, Azure Functions, APIs, Logic Apps, custom applications, connectors, and integration services therefore represent potential crossings of the envelope. An approved data repository connected to an unapproved endpoint can create a noncompliant workflow even when the original repository remains properly secured.

AI Processing Layer

Artificial intelligence introduces a particularly important processing boundary. The organization must establish which model endpoints may receive regulated information, what information may be retained, whether prompts or responses are used for model training, where processing occurs, what sub-processors are involved, and which identity and authorization controls survive the transition between source data and model processing.

Audit Layer

An envelope that cannot be observed cannot be reliably governed. The architecture should therefore provide sufficient logging to reconstruct significant access, transformation, movement, administrative activity, and AI processing involving regulated information. Auditability is not merely an operational convenience. It is a defining property of the Compliance Envelope.

⁴ Microsoft, "Secure AI: Guidance to Set Up Your Organization's AI Security Process," *Microsoft Learn: Cloud Adoption Framework*, accessed September 10, 2026, <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ai/secure>; Microsoft, "Secure Azure Platform Services (PaaS) for AI," *Microsoft Learn: Cloud Adoption Framework*, last updated June 25, 2026, <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ai/platform/security>

Inside, Conditional, and Outside

The Compliance Envelope model provides a simple classification scheme for architectural components.

INSIDE THE ENVELOPE

The component has been evaluated for the relevant data classification and may process that information under established controls.

CONDITIONAL

The component may participate only when specified technical, contractual, geographic, identity, or governance controls are satisfied.

OUTSIDE THE ENVELOPE

The component is not authorized to receive the regulated information.

This classification should apply not only to services but also to connections between services. A compliant architecture is therefore not simply a collection of *approved* boxes. It is a collection of *approved* boxes connected by *approved* arrows. That distinction becomes critical in distributed cloud and AI systems.

The Compliance Envelope and Artificial Intelligence

AI governance discussions frequently begin with an overly broad question:

Can AI access this data?

The Compliance Envelope produces a more precise question:

Can this particular AI capability process this particular class of information without causing the information, its derivatives, its retrieved context, its prompts, or its outputs to cross the defined Compliance Envelope?

Consider a hypothetical healthcare workflow: A user authenticates through Entra ID. The user's role permits access to a subset of records stored in an approved Microsoft data service. An AI application retrieves only records authorized for that identity. The information is transmitted to an approved Microsoft-hosted model endpoint under appropriate contractual/BAA and geographic conditions. Responses are returned to the authorized application. Prompts, responses, access decisions, and relevant administrative actions are appropriately logged.

Under the Compliance Envelope model, the organization evaluates the complete transaction. This is materially different from approving "AI" as a category. Indeed, Microsoft AI guidance recognizes this boundary problem. Microsoft recommends maintaining data security boundaries across AI systems and warns that indexing and AI ingestion can remove or bypass security controls associated with source

data⁵. Microsoft documentation for Azure AI Search likewise places responsibility on customers to ensure that information does not flow outside organizational compliance or geographic boundaries⁶.

Consequently, an AI system should not be considered inside the envelope merely because its model endpoint is approved. Retrieval, identity, authorization, processing, storage, output, logging, and downstream use must all remain inside the envelope.

The Envelope Is Traversed by Data, Not Products

This distinction produces perhaps the most important principle of the model:

Compliance boundaries should be evaluated by following data, not by inventorying products.

Imagine an architecture consisting entirely of approved Microsoft services. A Power Automate workflow retrieves regulated information from Dataverse and passes it through a connector whose downstream service has not been approved for that data. Every major application visible to the user might appear to belong to the organization's Microsoft environment. Nevertheless, the transaction has crossed the Compliance Envelope.

Conversely, a carefully engineered distributed system may remain within the envelope across several services because identity, authorization, encryption, residency, contractual protection, and auditing persist throughout the transaction.

The appropriate unit of compliance analysis is therefore the data journey.

Shared Responsibility

The Compliance Envelope should not be interpreted as transferring compliance responsibility to Microsoft. Cloud compliance remains a shared responsibility⁷. Microsoft may provide infrastructure, contractual commitments, certifications, encryption capabilities, identity services, policy enforcement, and audit mechanisms. The customer remains responsible for selecting appropriate services, configuring them correctly, controlling access, establishing permissible data flows, governing integrations, monitoring the environment, and validating that the resulting architecture satisfies its obligations.

The Compliance Envelope makes that division of responsibility visible. Microsoft supplies many of the materials from which the envelope can be constructed. The organization defines and governs the envelope.

⁵ Microsoft, "Govern Azure Platform Services (PaaS) for AI."

⁶ Microsoft, "Azure AI Search Preview Terms," *Microsoft Learn*, last updated August 12, 2026, <https://learn.microsoft.com/en-us/azure/search/search-preview-terms>

⁷ Microsoft, "Risk Assessment Guide for Microsoft Cloud."

From Concept to Governance Artifact

Organizations can operationalize the Microsoft Compliance Envelope by maintaining an Envelope Register for regulated workloads. For each workload, the register should identify:

- Applicable regulatory and contractual requirements;
- Permitted data classifications;
- Approved Microsoft services;
- Permitted geographic processing locations;
- Approved identity mechanisms;
- Required encryption and key-management controls;
- Approved applications and connectors;
- Approved AI endpoints;
- Prohibited destinations;
- Logging and retention requirements;
- Responsible system and data owners;
- Required security or privacy reviews;
- Documented exceptions; and
- Procedures for periodically validating the boundary.

Architectural diagrams should visually distinguish components that are inside, conditional, or outside the envelope and identify every interface through which regulated data could cross it. The resulting artifact becomes useful simultaneously to architects, security teams, compliance officers, auditors, privacy professionals, application developers, and executive decision-makers.

A Better Question for Regulated AI

Organizations adopting artificial intelligence face a genuine governance problem. A blanket prohibition against using regulated information with AI may unnecessarily prevent valuable applications. Blanket approval, on the other hand, ignores substantial differences between model providers, service configurations, data flows, identities, integrations, and contractual protections.

The Microsoft Compliance Envelope offers a third approach. It treats AI as another controlled data processing capability within an explicitly governed information architecture. The resulting governance question is no longer:

Do we allow AI?

It becomes:

Under what conditions can this AI transaction remain inside the approved Compliance Envelope?

That is a question security architects can answer, compliance professionals can evaluate, engineers can implement, and auditors can test.

Conclusion

Modern compliance boundaries are no longer walls surrounding individual applications. They are dynamic boundaries constructed from identity, infrastructure, contracts, configuration, policy, encryption, geography, data classification, authorization, integrations, and auditability.

The Microsoft Compliance Envelope provides a conceptual model for understanding those elements as a coherent whole. Its central proposition is simple:

Regulated information may be processed only when its complete data journey remains within an explicitly approved and verifiable combination of services, identities, controls, contractual protections, and governance mechanisms.

For artificial intelligence, this principle provides a practical path between prohibition and uncontrolled adoption. The objective is not merely to deploy AI securely; the objective is to make the boundary around regulated AI definable, enforceable, observable, and auditable.

References

Microsoft. "Data, Privacy, and Built-in Protections in Azure AI Search." Microsoft Learn. Accessed September 10, 2026. <https://learn.microsoft.com/en-us/azure/search/search-security-overview>.

Microsoft. "Govern Azure Platform Services (PaaS) for AI." Microsoft Learn: Cloud Adoption Framework. Accessed September 10, 2026. <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ai/platform/governance>.

Microsoft. "Guidance to Set Up Your Organization's AI Security Process." Microsoft Learn: Cloud Adoption Framework. Accessed September 10, 2026. <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ai/secure>.

Microsoft. "Risk Assessment Guide for Microsoft Cloud." Microsoft Learn: Microsoft Service Assurance. Last updated May 17, 2024. <https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide>.

Microsoft. "Secure Azure Platform Services (PaaS) for AI." Microsoft Learn: Cloud Adoption Framework. Last updated June 25, 2026. <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ai/platform/security>.

Microsoft. "Azure AI Search Preview Terms." Microsoft Learn. Last updated August 12, 2026. <https://learn.microsoft.com/en-us/azure/search/search-preview-terms>