# Storing geographic data in Copilot Studio

Microsoft Copilot Studio addresses geographic data storage needs by ensuring that data is stored and processed in compliance with regional regulations and organizational policies.

The concept of geographic data storage refers to the policies and practices governing where data is stored, processed, and managed geographically. This concept is crucial for organizations that need to comply with various legal requirements, ensure data sovereignty, and optimize data accessibility and performance.

Microsoft Copilot Studio addresses geographic data storage needs by ensuring that data is stored and processed in compliance with regional regulations and organizational policies.

This includes focusing on key aspects such as security, privacy, the General Data Protection Regulation (GDPR), data location, and compliance. By adhering to these principles, Copilot Studio helps organizations manage their data effectively across different domains, ensuring they meet legal requirements and maintain data sovereignty.

This approach not only optimizes data accessibility and performance but also provides a robust framework for managing data in a globally distributed environment. Copilot Studio can be configured to access Generative AI features in other domains, even when capacity is limited.

## Security

Security is paramount when handling geographicly stored data. Copilot Studio employs robust security measures to protect data during storage and transmission. Data is encrypted using industry-standard protocols, ensuring that unauthorized access is prevented. Furthermore, Microsoft continuously monitors and updates its security infrastructure to combat emerging threats.

## Privacy

Privacy is fundamental to data processing practices within Copilot Studio. The platform adheres to strict privacy policies to ensure user data is not only protected but also used responsibly. Microsoft Copilot Studio provides transparency regarding data collection, use, and storage, enabling users to make informed decisions about their data.

## General Data Protection Regulation (GDPR)

GDPR sets strict requirements for how personal data is handled. Microsoft Copilot Studio is designed to comply with GDPR by ensuring data is stored within designated geographic areas and that the rights of data subjects are respected. This includes the ability to process Data Subject Requests (DSRs) and conduct Data Protection Impact Assessments (DPIAs).

# Data storage location

Microsoft Copilot Studio allows organizations to choose where to store their data, providing the flexibility to meet regional data storage requirements. Data can be stored in multiple Azure data centers globally, ensuring it remains within a specified geographic area. This capability is crucial for organizations with specific data location needs.

# Comply with the EU Data Limits (EUDB).

Copilot Studio offers compliance with EU Data Limits.

For Copilot Studio, if a client provides a tenant with a billing address in the EU or EFTA, that tenant will fall under the EU Data Limit if the client also creates all of its environments within a geographic area that falls within the EU Data Limit.

# Follow

Compliance with regional and international regulations is a key focus of Copilot Studio. The platform supports compliance with various data protection laws, including GDPR, CCPA, and others. By providing tools and features to support compliance, Microsoft Copilot Studio helps organizations mitigate legal risks and maintain user trust.

# Data flow using connectors

Copilot Studio and Power Platform use connectors to facilitate seamless data flow between different systems and services. These connectors act as proxies or "wrappers" around APIs, enabling communication between Microsoft services (such as SharePoint, Dataverse, and Microsoft Graph) and external systems (such as Salesforce and other third-party APIs).

Data transmitted as part of a connector for a Microsoft service follows this process:

1. **Initialization** : A user action or an automated trigger initiates the data flow.
2. **Calling a connector** : The appropriate connector is called to handle the data transfer. For example, an agent might call a Power Automate flow to use the SharePoint connector to transfer data from a submitted form to a SharePoint list.
3. **Data transmission** : Data is transmitted securely between systems. Connectors ensure that data is encrypted during transmission and complies with the security protocols of both the source and destination systems.
4. **Processing and Storage** : Once data arrives at its destination in the Microsoft cloud, it is processed and stored according to predefined rules and configurations. For example, data sent to the Dataverse can be used to trigger subsequent workflows or analyses.
5. **Compliance and Monitoring** : Throughout the data flow, compliance with regional regulations and organizational policies is maintained. Microsoft provides tools to monitor and audit these data flows, ensuring transparency and accountability.

When using connectors to send and receive data from external systems (e.g., Salesforce), responsibility for maintaining the measures described in this article depends on whether the connection is to Microsoft services or

external services:

1. For connectors that send and receive data from external systems other than Microsoft (such as Salesforce), the responsibility lies with the agent creator.
2. For communication connectors within Microsoft's cloud, these responsibilities are handled by Microsoft.