Addressing data residency needs with Microsoft 365

Some governments have started limiting where data can be stored. They may require data residency, which stipulates that data belonging to their citizens, or digital copies of that data, be stored in defined physical boundaries, for example, within a specific country or region. Like other large cloud service providers, Microsoft is educating government officials and supports laws that protect data without placing undue burdens on businesses or international commerce. We also offer ways to help organizations address data residency requirements today, including the Multi-Geo feature in Office 365.
Each and every day of 2017, our digital society produced data at the rate of 2.5 quintillion bytes—enough to fill over half a million DVDs.¹ This inundation of data into the digital universe reflects the breakneck pace of technology change.

Advances are happening so fast that governments struggle to evaluate their impact and design appropriate regulations. They know that digital data is extremely valuable to both private and public sectors but protecting the personal and economic interest of their citizens means legislating uncharted territory that’s constantly re-forming. While governments have been regulating the flow of physical commodities like precious metals across borders for thousands of years, regulating movement of data is a very recent undertaking.

Data is a different type of tradeable asset. Unlike physical commodities, data is an inexhaustible resource. Multiple entities can use the same piece of data many times without “using it up,” and copies of data can be sold an infinite number of times without ever relinquishing possession of the original. The more data you have, the more it can tell you, and the more diverse the data sources, the more insights, and therefore value, it provides. Data flowing across international borders—for example, data exchanged as part of e-commerce transactions—already contributes USD 2.8 trillion annually to global Gross Domestic Product.² Individual nations understandably want to capture their share of this value.

“Data can be seen as a commodity. Its ownership can be transferred; it can be marketed, re-used, aggregated, transformed, bought and sold.”

Andrus Ansip, European Commission Vice-President for the Digital Single Market, November 2015

¹ Source: World Economic Forum
² Source: World Economic Forum
³ Source: EMC Corporation
Data residency: a global trend

Some countries are limiting where data can be transferred, much like trade policies that control the import or export of raw materials or manufactured goods. They do this in an effort to ensure local economies benefit and the data of their citizens isn’t exploited. This trend is called data nationalism or data localization. Some countries require data residency, which stipulates that data belonging to their citizens, or digital copies of that data, be stored in-country.

“Data localization can be explicitly required by law or is the de facto result of a culmination of other restrictive policies that make it unfeasible to transfer data, such as requiring companies to store a copy of the data locally.”


Data residency laws have a direct impact on the use of cloud computing, which EMC estimates will touch 40 percent of data by 2020, because data stored “in the cloud” is really stored on physical servers connected to the Internet. The laws assume that the physical possession of servers, like the physical possession of tradable commodities, ensures control over who can access or use the data of local citizens, keeping it safe, and that hosting data locally will grow local economies.

This position, while well-intentioned, is based on misperceptions about cybersecurity and economics. The vast majority of cybercriminals access data through the network, not through the physical datacenter. The reality is that controlling physical storage alone doesn’t keep data secure. Sophisticated security software, hardware, and best practices are also necessary. Multinational cloud service providers who specialize in running data centers, like Microsoft, offer best in class security and can achieve the global economies of scale necessary to drive down costs for individual customers. Moreover, there are practical reasons, such as backup and disaster recovery, for storing data in multiple geographic locations.

“Practically no company would be able to do business, or take part in international trade, without the ability to transfer data across borders.”

Swedish National Board of Trade, January 2014

Since the international flow of data is a relatively new phenomenon in the history of global trade, it’ll take time for governments to understand the nature of data as a modern commodity and legislate accordingly. Technology companies, industry advocates, and trade officials are working to educate governments about the impact of data residency laws on economic growth. In the meantime, multinational organizations still have to comply with these restrictions.

“For companies in countries with data localization laws, the laws increase the price of computing by 30 to 60 percent.”

McKinsey Global Institute, April 2017
The General Data Protection Regulation (GDPR), enforced as of May 25, 2018, requires organizations doing business with the European Union to employ measures to protect personal data. It does not, however, require data residency. To learn more about rules that apply to the transfer of personal data outside of the EU, visit the European Commission’s official site. Always consult your legal department for the latest information on privacy compliance requirements. To learn how Microsoft helps organizations comply with GDPR, visit our Trust Center.

How Microsoft supports data residency

Like other large cloud service providers, Microsoft engages with government officials and supports laws that protect data without placing undue burdens on businesses or international commerce.

We also offer ways to help organizations address data residency requirements today. For example, when we sign a contract with a customer, we guarantee we’ll store certain Office 365 data at rest in a specific geography. This means we’ll honor requirements for data residency, compliance, and resilience within the physical boundaries of that geography.

Microsoft has datacenters in more than 50 regions and 140 countries. Office 365 supports more than a dozen geographies. By default, we store customer data in the datacenter geography associated with the customer’s billing address. To maintain reliability and high availability, we replicate core user data, such as mailboxes and OneDrive for Business documents, in at least two datacenter locations within the same geography. When we open a new datacenter, existing customers who have strict data residency requirements have the option of moving their core customer data to the new geography.

The Multi-Geo feature in Office 365

While organizations that operate within a single geography simply need to set up a cloud subscription within that geography, meeting data residency requirements is more challenging for multinational organizations. To ensure compliance, they can keep subsidiaries in some countries on-premises, while moving the rest to the cloud. This approach makes administration and user collaboration more difficult, however. If they keep data and apps on-premises, they lose the flexibility and productivity gains that cloud services provide. Users whose apps and data are still tied to on-premises servers don’t benefit from “work anywhere, anytime, from any device” convenience or continually updated services.

Fortunately, there’s another option. Multinational organizations can use an out-of-the-box feature called Multi-Geo to expand their Office 365 tenant across multiple geographies. In a Multi-Geo configuration, an Office 365 tenant consists of a central location (also known as the default location) and one or more satellite geographies where data will be stored. Microsoft still serves the applications and collaboration experiences globally, but customers control where Exchange Online, OneDrive for Business, and SharePoint Online store content at rest within their tenant, so they can address their global data residency requirements.

Learn more about moving core data to new Office 365 datacenter geographies here.
IT administrators can assign each user’s data to a specific geography. Microsoft won’t store the user’s content in these services in a different geography without permission. Administrators can easily move this content between geographies if a user relocates to a different subsidiary. They can even designate where certain customer will not be stored or copied. Individual users interact with data in the geography where it’s stored at rest, whether it’s their own data in their own geography, or someone else’s data stored in a different geography.

**Microsoft’s global network of highly secure datacenters**

Because Microsoft understands concerns about security and privacy, we have strong policies and practices in place to protect customer data stored in our datacenters. For example, we encrypt all Office 365 customer data at rest and in transit.

Each year, we invest billions of dollars each year to maintain our [global network of datacenters](https://www.microsoft.com/en-us/), one of the world’s largest, and expand into new regions. Thousands of miles of privately-owned fiber and multi-terabit network connections keep network congestion minimal. More than 100 public Internet peering interconnection locations help ensure a consistent experience for users connecting into the network, no matter where they are or where their data is stored.
We not only have a presence in more regions than any other cloud provider, we also have the most comprehensive set of compliance offerings. Our defense-in-depth approach to cyber security protects our datacenters at both the physical and logical layers.

To prevent physical access to our datacenters, we employ perimeter fencing, video cameras, security personnel, secure entrances with multi-factor biometric and token scanners, as well as sophisticated communications networks.

We’ve fine-tuned technical defense measures through decades of experience building enterprise software using secure development practices. Our operational measures go beyond certification requirements and include dedicated cybersecurity teams, as well as a Cyber Defense Operations Center that uses artificial intelligence to visualize, identify and track global cyberthreats as they develop. We also work with partners, such as government agencies, industry allies, law enforcement, researchers, customers, investigators, and forensic analysts around the globe to fight against cybercrime.

---

**Microsoft’s layered approach to securing data in the cloud**

<table>
<thead>
<tr>
<th>Customer Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
</tr>
<tr>
<td>• Azure Active Directory / multifactor authentication</td>
</tr>
<tr>
<td>• Threat Management</td>
</tr>
<tr>
<td>• Mobile Device Management</td>
</tr>
<tr>
<td>• Message Encryption and Risk Management</td>
</tr>
<tr>
<td>• Data Loss Prevention</td>
</tr>
<tr>
<td>• Customer Lockbox</td>
</tr>
<tr>
<td>• Management activity API</td>
</tr>
<tr>
<td><strong>Logical</strong></td>
</tr>
<tr>
<td>• Secure Development Lifecycle</td>
</tr>
<tr>
<td>• DDoS protection</td>
</tr>
<tr>
<td>• Multi-tenancy</td>
</tr>
<tr>
<td>• Incident response/Cyber Defense Operations Center</td>
</tr>
<tr>
<td><strong>Physical</strong></td>
</tr>
<tr>
<td>• Access approval</td>
</tr>
<tr>
<td>• Perimeter</td>
</tr>
<tr>
<td>• Building</td>
</tr>
<tr>
<td>• Server environment</td>
</tr>
<tr>
<td>• Data-bearing device controls</td>
</tr>
</tbody>
</table>

### ADDRESSING DATA RESIDENCY NEEDS WITH MICROSOFT 365

- **Configuration**
  - Azure Active Directory / multifactor authentication
  - Threat Management
  - Mobile Device Management
  - Message Encryption and Risk Management
  - Data Loss Prevention
  - Customer Lockbox
  - Management activity API

- **Logical**
  - Secure Development Lifecycle
  - DDoS protection
  - Multi-tenancy
  - Incident response/Cyber Defense Operations Center

- **Physical**
  - Access approval
  - Perimeter
  - Building
  - Server environment
  - Data-bearing device controls
In addition to the measures we take to protect the services and infrastructure we manage, we offer software solutions and best practices that customers can employ to help secure their networks, devices, applications, and documents to keep customer data safe.

Visit our Trust Center to learn more about how Microsoft keeps data secure:
- Compliance offerings
- Secure development practices
- Operational security measures
- Use of artificial intelligence
- Cyber Defense Operations Center
- Partnerships
- Software solutions and best practices

Staying informed about data residency laws

Microsoft recommends implementing Multi-geography only when data residency is legally required. Dozens of countries are enacting or considering data residency laws. Unfortunately, these laws are not consistent from country to country, and their specific requirements are not always clear. Ensuring compliance will require close collaboration with legal experts. To stay informed, we suggest following organizations that issue reports about policy developments. These include industry advocates, such as the Information Technology Industry Council or the Business and Industry Advisory Committee to the OECD (BIAC), and organizations that determine national trade policy in each country, such as the Office of the US Trade Representative in the United States.

For more information on Multi-Geo in Office 365, visit aka.ms/multi-geo.
Addressing data residency needs with Microsoft 365

Some governments have started limiting where data can be stored. They may require data residency, which stipulates that data belonging to their citizens, or digital copies of that data, be stored in defined physical boundaries, for example, within a specific country or region. Like other large cloud service providers, Microsoft is educating government officials and supports laws that protect data without placing undue burdens on businesses or international commerce. We also offer ways to help organizations address data residency requirements today, including the Multi-Geo feature in Office 365.