This document briefly explains the CLOUD Act and clarifies what it does and does not allow regarding US law enforcement access to cross-border data.

The CLOUD Act: What It Is – And What It Isn't

What is the CLOUD Act?

The Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in 2018, clarifies legal obligations for technology providers, enables efficient, privacy-protective, law enforcement access to cross-border data, and includes safeguards that enhance security and digital sovereignty. The CLOUD Act contains two parts:

CLOUD Act Part 1: Clarifying authority to seek cross-border data

The CLOUD Act clarifies the circumstances under which US law enforcement may seek access to data, regardless of where it is stored. This part has been subject to significant misunderstandings about its scope and effect:

- **Fact: The CLOUD Act does NOT permit unfettered, bulk, or automatic government access to data**. US law enforcement must meet strict legal requirements and obtain a warrant or court order subject to judicial approval. The law does not allow indiscriminate or bulk access to domestic or foreign data. To obtain a warrant or court order under US law, the government must prove to independent courts that there is reason to believe that evidence of crimes will be present in specified account data.
- **Fact: The CLOUD Act does NOT ignore foreign law**. The law specifically recognizes a provider's right to bring a challenge based on conflicts with foreign law and the international principle of comity. The concept of comity, or deference to foreign law, is based on principles of courtesy, reciprocity, and mutual respect for the sovereignty of nations. Microsoft is committed to challenging any US requests that fail to respect digital sovereignty and conflict with foreign laws.
- **Fact: CLOUD Act requests for foreign enterprise data are NOT common—and indeed are exceptionally rare**. Microsoft's transparency reports[1] show that disclosures of foreign enterprise content data to US law enforcement constitute a mere 0.008% of the total number of demands that Microsoft has received each year since the CLOUD Act was enacted, representing fewer than one out of every 10,000 demands.
- **Fact: The CLOUD Act does NOT permit the US to conduct economic espionage or access trade secrets of foreign companies.** The US has a long-standing position of opposing any use of law enforcement or intelligence authorities to support the theft of intellectual property, including trade secrets or other confidential business information.

[1] Government Requests for Customer Data Report | Microsoft CSR

Under US law, theft of trade secrets is subject to criminal prosecution with penalties of up to ten years in prison.

- **Fact: The CLOUD Act does NOT override technical controls like end-to-end encryption that protect digital sovereignty**. Microsoft offers advanced encryption, data residency options, and customer-controlled encryption keys that provide customers with control of their data. Features like Azure Confidential Compute ensure that Microsoft is incapable of accessing data without customer assistance and consent. Microsoft does not provide any government with the ability to break our encryption.
- **Fact: Extraterritorial law enforcement access to data is NOT unique to the US**. Many countries have laws and precedents that authorize their access to data stored in other jurisdictions. The Budapest Convention on Cybercrime and the UN Convention Against Cybercrime require parties to adopt laws to compel access to electronic records without regard to their location. This principle is also reflected in the EU e-Evidence Regulation, the laws of numerous EU Member States, Canadian law, UK law, and elsewhere.
- **Fact: The reach of the CLOUD Act is NOT limited to US companies**. The law applies to any company that has "minimum" contacts with the US economy. Foreign cloud providers with any US presence, including those simply offering services over the internet in the US, may be subject to the CLOUD Act and required to turn over data to US authorities – regardless of where that data is stored. Eliminating exposure to US law would require relying on companies with no ties to the US economy, which would likely lack the global resources and expertise necessary to build and maintain world-class technology services.

CLOUD Act Part 2: Data access agreements with qualifying countries

The CLOUD Act also authorizes the US Department of Justice (DOJ) to enter into agreements with qualifying governments to allow direct requests for cross-border data without violating each other's domestic laws. DOJ finalized agreements with the United Kingdom in 2019 and Australia in 2022 and entered negotiations with the European Commission in 2019 and Canada in 2022. This part of the CLOUD Act is also subject to privacy and data sovereignty protections:

- **Parties must meet strict rule-of-law and due process safeguards** to ensure third-party oversight and the protection of civil liberties.
- **Investigations must relate to serious crimes** such as child exploitation, cybercrime, drug trafficking, and terrorism.
- **Critically, the parties cannot target each other's persons**. That is, the US cannot use its agreement with the UK to target UK persons or enterprises, and vice versa.
- **Data access agreements require additional conflict of law protections** to ensure that a provider does not have to violate the laws of either party to comply.

Why Microsoft supports additional CLOUD Act agreements

Microsoft strongly supports DOJ completing negotiations with the European Commission on an EU-US e-Evidence Sharing Agreement, as well as with the Government of Canada on a Canada-US Data Access Agreement. Such agreements:

- **Enhance security** by accelerating investigations into serious transnational crime, such as terrorism, child exploitation, cybercrime, and drug trafficking.
- **Enhance sovereignty** by creating conflict of law protections that ensure each party's laws and fundamental rights are respected and that each side has the tools necessary to investigate and prosecute threats to domestic public safety and security. For the EU and Canada, an agreement would empower their law enforcement agencies to seek data without relying on US authorities to approve and process time-consuming mutual legal assistance treaty requests.
- **Enhance trust and strengthen data flows** by directly addressing privacy concerns around cross-border data access and potential conflicts of law. These agreements would provide additional assurances that each side is a trusted partner and would afford providers another mechanism to contest demands that conflict with any local laws, which would further bolster the legal framework supporting the digital economy.

Microsoft's practices and principles responding to data requests

Microsoft has a strong track record of defending our customers' rights in response to government access requests. We rigorously scrutinize every legal request and regularly challenge those that conflict with our principles and any applicable laws—even taking cases to the U.S. Supreme Court. We maintain transparency by providing customers with notification of demands and through detailed public reporting. Our transparency report demonstrates how few cross-border requests Microsoft receives: Cross-border enterprise content disclosures represent just 0.008% of our global law enforcement demands, none of which involved public sector customers. We also offer strong contractual and technical safeguards to ensure we can meet our customers' needs and comply with local laws. Some core policies Microsoft adheres to across our services include:

- Microsoft does not provide any government with direct and unfettered access to our customers' data, and we do not provide any government with our encryption keys or the ability to break our encryption.
- If a government wants customer data, it must follow applicable legal process. It must serve us with a warrant or court order for content, or a subpoena for subscriber information or other noncontent data.
- All requests must target specific accounts and identifiers.
- Microsoft's legal compliance team reviews requests to ensure they are valid, rejects those that are not valid, and only provides the data specified.