OpenText™

OpenText Secure MFT:

Data Sovereignty in the European Union and Australia

Drive data sovereignty, privacy and compliance in the European Union (EU) and Australia with in-region processing and dedicated infrastructure

In the EU, there are a variety of regulations in place designed to promote privacy and the notion of data sovereignty. For example, the EU's Data Protection Directive of 1995 and the United Kingdom's (UK) Data Protection Act of 1998 are government mandates requiring all EU member states to protect citizens' fundamental rights around the processing of their sensitive information. A similar regulation has also been established in Australia to regulate the handling of personal information, namely the Privacy Act 1988.

These government directives also state that personal information should not be transferred between countries or territories outside of Europe or Australia, except those deemed capable of providing acceptable levels of data protection. As a result, many enterprises in EU and Australia are looking for cloud solutions that process data within their fixed geographical boundaries.

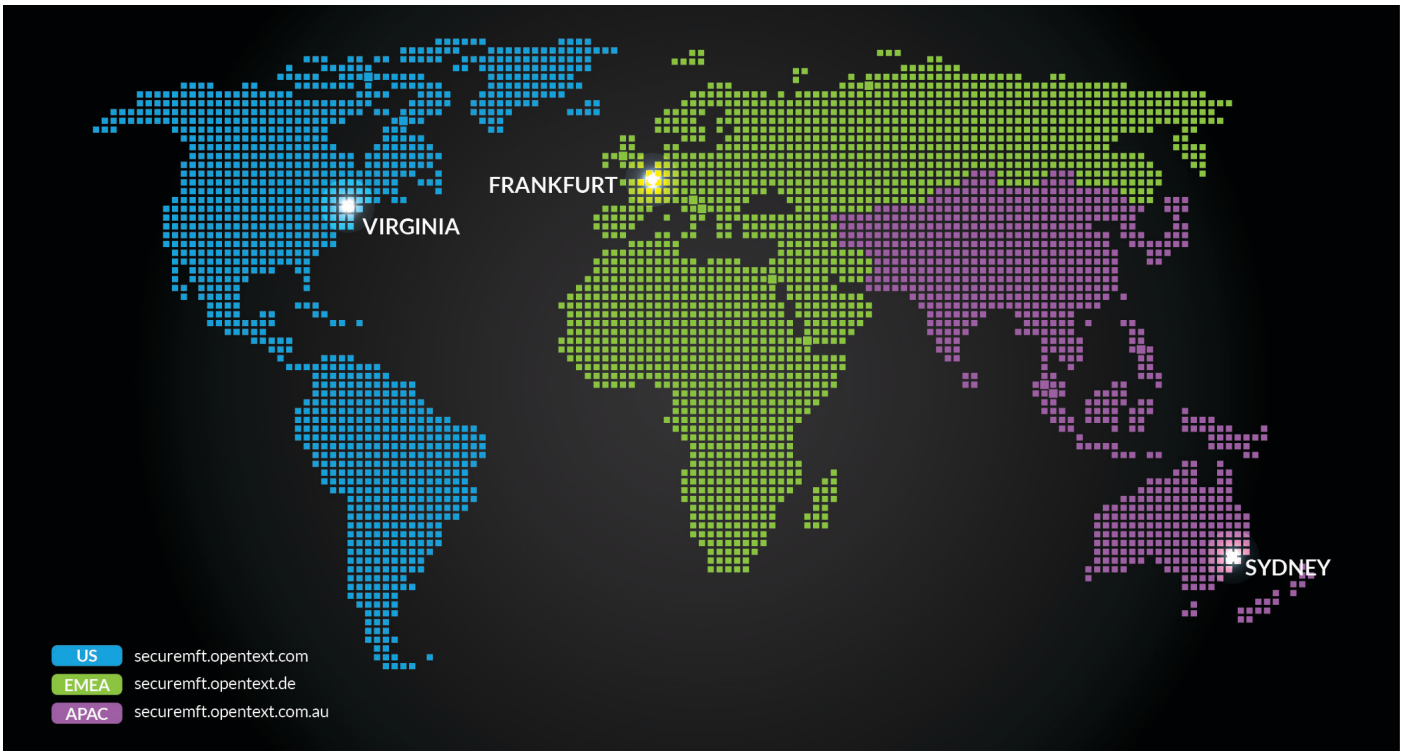
OpenText has the ability to store and process EU and Australian customer files sent via Secure MFT strictly within its data centers in Frankfurt, Germany and Sydney, Australia; this in-region processing capability was designed to help address privacy and data sovereignty concerns for customers who have requested in-region processing. Thus, all their files sent via Secure MFT will be stored exclusively at the data center in either Frankfurt or Sydney, and all metadata processing, user authentication and auditing information recording are handled independently at one of those fully secure data centers.

FEATURES:

- *Processes and stores EU customers' important assets strictly within the EU*
- *Processes and stores Australian customers' important assets strictly within Australia*
- *Accommodates all Secure MFT transfers*
- *Provides physical and environmental security mechanisms*

BENEFITS:

- *Supports customer data sovereignty requirements*
- *Safeguards the Secure MFT network from unauthorized access and security threats*
- *Personnel monitors customer inquiries, support issues and incidents on a real-time basis*



Physical Safeguards

Both the Frankfurt and Sydney data centers have exterior and interior barriers designed to physically protect various data center entry points and prevent unauthorized personnel from accessing the facility. The exterior barriers are made up of an outer wall that is steel clad and thermally insulated; all entry points are kept to a minimum with each exterior door being fully reinforced, alarmed, controlled, and monitored. Access control systems serve as interior barriers; they are in place throughout our data centers to restrict access to unauthorized personnel. Finally, customer infrastructure is compartmentalized, locked, protected, and monitored via video for added surveillance.

Environmental Safeguards

The Frankfurt and Sydney data centers also feature environmental safeguards to protect servers from adverse situations of fire and/or other overheating instances. Fire protection includes fire, smoke and heat detection and suppression that is monitored 24 hours a day, with sensors located throughout the data center providing alerts as necessary.

Both data centers are also equipped with dedicated HVAC units. Each data center has both audible and visual alarms to notify data center personnel of any temperature or humidity threshold issues. With regards to power management, the data center utilizes multiple inbound connections from electricity providers; power is provided by an Uninterrupted Power Supply (UPS) fed by back-up generators.

Data Center Personnel

OpenText commissions a team of dedicated support personnel that's available to customers 24 hours a day. The team follows defined procedures for identifying, facilitating, and escalating any unexpected events that might negatively impact the data center's overall functionality. They regularly monitor customer inquiries, support issues and other incidents on a real-time basis, documenting each one in a centralized ticketing system and tracking them to resolution.

Personnel staff escorts all data center visitors, including customers, through the facility and requires them to register prior to entry. The staff also performs daily inspections of all fire suppression, power generation, and distribution equipment as well as any climate controlling infrastructure. These daily inspections are validated at pre-determined intervals by third-party specialists. Finally, preventive maintenance agreements and scheduled maintenance procedures are in place for all key hardware components and environmental systems.