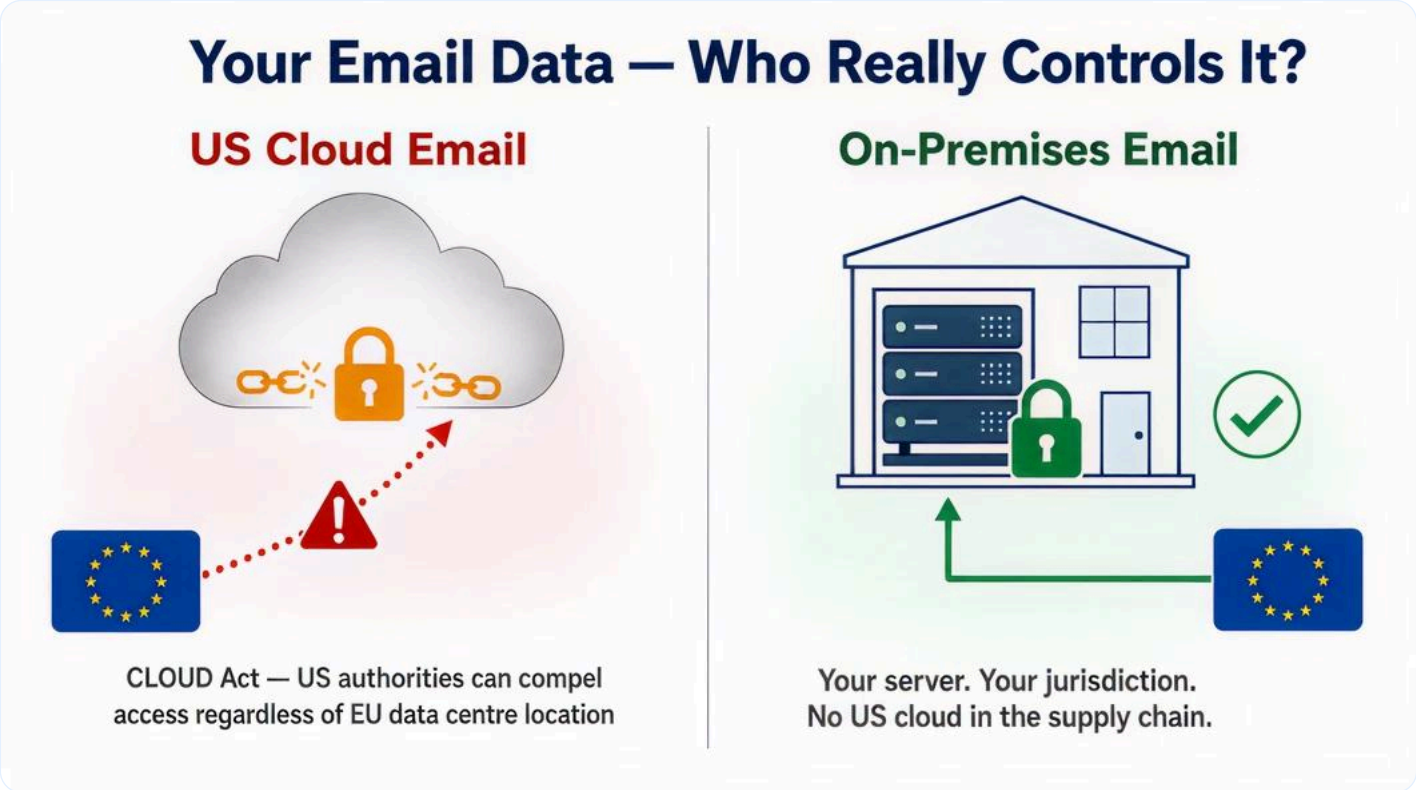
KerioConnect®

USE CASE

Your email is on a server you don’t own, and someone else has the keys

Data sovereignty and GDPR compliance for EU SMBs



The problem no contract can fix

When your organization uses Microsoft 365 or Google Workspace, personal data about your employees and clients is processed by a US company on infrastructure subject to the **US CLOUD Act**, a law that allows US authorities to compel access to that data regardless of which country's data center it sits in, without notifying you.

This conflicts directly with GDPR. The EU-US Data Privacy Framework (DPF) is the current transfer mechanism, but it is the third framework designed to solve this problem, after Safe Harbor was invalidated in 2015 and Privacy Shield in 2020. Legal challenges are already in progress. In June 2025, Microsoft's own Chief Legal Officer in France confirmed it plainly: if compelled by a US court, Microsoft must hand over the data.

No Data Processing Agreement resolves this. The conflict is structural. **The only resolution is architectural: keep your email data on infrastructure you own, in a jurisdiction you control.**

What GFI KerioConnect® does about it

GFI KerioConnect® runs on your server: your hardware, your data center, or a cloud VM with any EU-based provider you choose. Email data never passes through GFI's infrastructure. There is no US cloud provider in the supply chain to whom a CLOUD Act order could be directed.

The technical controls that support GDPR Article 32:

- TLS 1.2/1.3 enforced on all connections; S/MIME for end-to-end encryption
- TOTP two-factor authentication across all access points
- Active Directory integration — user access tied to your directory; deprovisioned instantly
- Full audit logging (9 log types), exportable to SIEM via syslog
- DKIM, SPF, DMARC — email authentication enforced per domain
- Configurable storage location — you decide where mailbox data is written

All controls are under your direct administration and directly documentable for DPA audits, vendor due diligence, and NIS2 Article 21 obligations.

How it played out at one EU firm

An 85-person professional services consultancy across three EU countries had been on M365 since 2021. By 2024, their DPO had three specific problems: dependence on the fragile EU-US DPF, an Article 17 deletion process that took six weeks and remained incomplete, and no direct technical control evidence for a financial sector client's due diligence.

They deployed GFI KerioConnect® on a dedicated server in a German colocation data center, EU jurisdiction, no US corporate parent in the supply chain. Migration from M365 used KEMT over a single weekend. Users kept Outlook. Mobile kept ActiveSync.

Concern	Before	After
CLOUD Act exposure	Structural — US law applied regardless of EU hosting	Eliminated — data on firm's EU server
Article 17 deletion	6-week process; incomplete	Single admin action; fully auditable
Vendor due diligence evidence	Limited — controls managed by Microsoft	Fully documented under firm's direct management
DPO assessment	"Residual exposure I cannot fully mitigate"	"The exposure is resolved at the architecture level"

Why the urgency is real

- **DPF is contested.** A third invalidation would immediately render M365 and Google Workspace subscriptions non-compliant with no immediate fallback
- **NIS2 (October 2024)** requires demonstrable technical controls for a broad set of EU organizations. Controls you own are easier to evidence than controls managed by a cloud provider
- **GDPR enforcement is accelerating.** €1.2 billion in fines issued in 2025 alone, with EU DPAs increasingly focused on cloud transfer issues

How GFI KerioConnect® compares

What matters	GFI KerioConnect®	Microsoft 365	Google Workspace
Data on your infrastructure	✅ Your server, your control	❌ Microsoft-managed	❌ Google-managed
CLOUD Act exposure	✅ None	❌ Structural	❌ Structural
EU-US transfer dependency	✅ None	❌ Dependent on DPF	❌ Dependent on DPF
Article 17 deletion — direct control	✅ Single admin action	⚠️ Via Microsoft process	⚠️ Via Google process
NIS2 controls — directly evidenced	✅ Full admin access	⚠️ Partially vendor-managed	⚠️ Partially vendor-managed
Outlook / mobile compatibility	✅ Full MAPI, ActiveSync	✅ Native	✅ Available

The position: GFI KerioConnect® removes the structural problem US cloud email creates, without requiring a user experience trade-off or an enterprise budget.

Ready to get started?

Talk to GFI at sales@gfi.com or find a partner.

If your organization processes EU personal data and uses a US-headquartered cloud email provider, start with a data flow review: where does your email data go, and what jurisdiction governs it?

Copyright © GFI USA, LLC, All rights reserved.