Microsoft Non-Transparency and Compliance

URL: https://www.computerweekly.com/news/366632040/Microsoft-hides-key-data-flow-information-in-plain-sight

Published: September 26, 2025

Situation: Part Three of the UK's Data Protection Act 2018 (DPA18) places strict limits on the transfer of policing data outside the UK. During the rollout of Police Scotland and the SPA to Microsoft 365, the entities were not informed that their proprietary data on the Azure Hyperscale infrastructure would be processed across more than 100 countries using 148 sub-processors.

As a result, proprietary data, including sensitive arrest records, could potentially be accessed by Microsoft staff/contractors, and potentially from jurisdictions like China. Of these 100+ countries, only the UK complies with the law enforcement data adequacy policy in DPA18.

Task: The installation allowed remote access from hostile regions, heightening breach potentials through non-adequate data protection environments. The challenge was to ensure compliant data flows, provide transparency for risk assessments, and prevent unlawful transfers of proprietary data.

Action: Microsoft data flow details are hard to find, and they are reportedly refusing full disclosure under freedom of information requests, leading to compliance struggles for clients like Police Scotland. Microsoft has admitted that it cannot guarantee the sovereignty of European data stored and processed in its services.

To mitigate this, it is recommended that services such as this deploy geofencing and limit customer data to specific geographical regions. Microsoft is reportedly not doing this currently.

Result: The opacity around where customers' data resides or is processed has resulted in potential compensation claims from data subjects, non-compliance fines, and eroded trust. This could be very expensive for the UK government. Microsoft has now begun providing more transparency regarding where the data on its infrastructure resides or is processed.

Zerowait's Approach

Zerowait's engineering expertise and custom SimplStor hardware offer on-premises solutions to localize sensitive data, mitigating international transfer vulnerabilities. With SimplStor, data would reside on and be processed by on-premises servers, using advanced encryption, immutable backups, and access logging to prevent remote exposures. This includes deploying air-gapped systems and firewalls, ensuring data stays within jurisdictional boundaries through physical control.

1) Zerowait's on-premises solutions eliminate cloud data transfer risks, keeping proprietary information local and under complete control.
2) Simplstor.com hardware offers high-security encryption and air-gapping, preventing remote hacks common in Azure, AWS, and Google Cloud.
3) Avoid regulatory fines from international data flows by using Zerowait to ensure compliance with local laws.
4) Reduce downtime from cloud breaches with SimplStor's redundant, offline backups for quick recovery.
5) Cut costs on cloud subscriptions while enhancing security against phishing and misconfigurations via Zerowait's customizable systems.

Want to know more? Contact Zerowait today!

Email: engineering@zerowait.com
info@zerowait.com
TEL: (302) 996-9408
Web: www.zerowait.com
www.simplstor.com