EBOOK

THE BYOK GAP IN MICROSOFT AZURE AND M365:

WHAT ORGANISATIONS DOING BUSINESS IN THE EU NEED TO KNOW

archTIS

CONTENTS

EXECUTIVE SUMMARY

European Union (EU) organisations and global companies conducting business in Europe are required to maintain high levels of data security and compliance under regulations like the General Data Protection Regulation (GDPR).

The impacts of uncontrolled or unauthorised access by cloud service providers, government authorities and staff located worldwide create serious risks and challenges to providing adequate security and compliance.

This white paper delves into the potential risks of retaining encryption keys with Cloud Service Providers (CSP), including Microsoft Azure and Microsoft 365 (M365), that can lead to data exposure and non-compliance with GDPR and other data protection laws.

The Significant Impact of GDPR Violations[1]

The Irish Data Protection Commission (DPC) imposed a historic fine of **€1.2 billion on US tech giant Meta (Facebook's parent company)** in 2023. The massive fine was issued for the transfer of personal data of European users to the United States without adequate data protection mechanisms.

The Hamburg Commissioner for Data Protection and Freedom of Information (BfDI) issued a **€35,3 million GDPR fine in 2020 to retailer H&M (Hennes & Mauritz)** after a technical error caused the data on the company's network drive, including employees personal and healthcare information, to be accessible to everyone in the company for a few hours.

In 2019, the ICO a **£20 million GDPR fine to British Airways** for violation of GDPR after a breach investigation found the airline was processing a significant amount of personal data without adequate security measures in place.

Marriott International was issued GDPR fine of £18,4 million in 2020 for a lack of due dilligence and appropriate security measures that led to a cyber attack, exposing the personal data of over 339 million guest records.

[1] https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/

INTRODUCTION

Microsoft's Azure and M365 are among the leading cloud services globally. Still, their limited BYOK capabilities pose potential data security and compliance issues, particularly for organisations that must comply with the EU and global data sovereignty laws.

Increased government concern over protecting sensitive personal, business, government and defence data in the Cloud has led to a complex regulatory landscape that aims to maintain control of citizen and government data.

Data sovereignty, where a country or jurisdiction has the right to govern and control digital data collection, storage, processing, and distribution within its borders, comes with both obligations and challenges for global entities. Organisations operating across international borders must comply with each country/jurisdiction's rules where their data resides.

Examples of Laws Impacting Data Sovereignty

Regional standards mandate rigorous data protection measures, including encryption and data control for security, regulatory or privacy purposes. For example:

- **GDPR** – Any information collected from EU citizens must reside in servers located in EU jurisdictions or countries with a similar scope and rigour in their protection laws under GDPR. Art. 32(1) requires the data controller and the processor to implement appropriate technical and organisational measures to secure personal data, with encryption referenced as a viable security measure.
- **International Traffic in Arms Regulations (ITAR) –** Any information or technical data related to items on the United States Munitions List (USML) can only be accessed by U.S. persons unless otherwise authorised by the U.S. Department of State.
- **CLOUD Act –** The US's Clarifying Lawful Overseas Use of Data Act (CLOUD Act) states that U.S. law enforcement agencies may, under certain circumstances, lawfully demand data stored in foreign countries from entities subject to U.S. jurisdiction. Many are concerned that the CLOUD Act will allow the U.S. government to surveil the data of any non-U.S. citizen or business that uses a cloud services provider with operations in the United States. However, many countries across the EU and China also have national access laws.
- **Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018,1 or TOLA Act –** This Australian legislation permits law enforcement and intelligence agencies to obtain warrants to request or force telecommunications providers to provide access to data and devices, including encrypted communications.

ENCRYPTION AND DATA SOVEREIGNTY

As introduced above, the data sovereignty of information hinges on the location of where the data is stored. However, encrypting data changes everything.

Once encrypted, data can be stored anywhere without breaking sovereignty, as the encrypted data is useless without the key. The enforcement of data sovereignty then entails ensuring the encryption keys are stored in the correct jurisdiction and access to the encrypted data only occurs in the correct jurisdiction.

While encryption solves many data sovereignty issues when using CSPs, it also introduces new challenges – encryption key management and tightly controlling data access.

WHAT IS ENCRYPTION?

The encryption process has three main parts:

1. an encryption key,
2. an encryption algorithm, and,
3. the encrypted bytes.

From the perspective of data sovereignty, once encrypted, the bytes can be stored anywhere (the location of storage does not affect the sovereignty of ownership). The keys and algorithm define sovereignty and require tight controls.

The process uses a combination of an encryption algorithm and an encryption key to transform "plaintext" (readable data) into "ciphertext" – a completely unreadable mass of symbols. Ciphertext remains unreadable until it is decrypted or converted back into its original readable form using the encryption key.

Think of encryption as a door that is secured using a lock and a key. The lock is the encryption algorithm, and the key is the encryption/decryption key. If a person does not have the door key, they cannot access what is stored behind it. Encryption renders the data inaccessible to anyone who does not have the decryption key to open it or in this case, decipher it, making it an essential tool for data protection.

WHAT ARE KEY MANAGEMENT AND BYOK?

CSPs, including Microsoft, offer an array of data security capabilities to help organisations protect their data, including key management (KM) and encryption services. However, in CSP-provisioned HSM or KM services, the provider creates, can access and retains control over your keys.

On the other hand, Bring Your Own Key (BYOK) is an option that allows organisations to create, retain control of and manage their encryption keys for added security. The main objective of BYOK is to mitigate the risk that a CSP or SaaS vendor may not provide the desired level of protection and control over your data, given that it has the ability to decrypt your data.

However, not all BYOK systems are the same. For the majority of CSPs, BYOK typically involves uploading a customer-specific certificate into the CSP. This certificate is then used to secure the encryption keys. Under this model, however, the CSP still has access to the encryption keys to perform the encrypt/decrypt actions. Therefore, the CSP could still be mandated to hand over the keys by the legislation applying to the CSP itself.

To be secure and compliant, BYOK must put complete control of the encryption keys in the hands of the customer. or example, on a device such as a hardware security module (HSM) that the customer exclusively controls within their secure intranet.

RISKS WHEN CSPs HOLD ENCRYPTION KEYS

Understanding the security and compliance risks of access to data and encryption keys by the CSP is critical. Especially since some of these regulations allow jurisdictions to demand CSPs provide them with a customer's encrypted material.

Potential Data Exposure

With Microsoft or any CSP possessing the encryption keys, there is an inherent risk of unauthorised data exposure. While Microsoft has security protocols in place, the possibility of internal vulnerabilities or successful cyber attacks could expose sensitive data.

Legal and Governmental Access

Without BYOK, any CSP can be compelled to provide access to your data through legal processes. This is especially concerning given the U.S. CLOUD Act and Australian TOLA Act, which can potentially conflict with EU data protection laws.

Loss of Control and Data Sovereignty

Having encryption keys managed by a third-party provider like Microsoft limits an organisation's control over its data, affecting data sovereignty—an essential requirement under EU laws.

Non-Compliance Penalties

Failure to fully control access to sensitive data could result in regulatory non-compliance, subjecting organisations to financial penalties. For example, GDPR fines of up to 10 million euros, or up to 2% of an organisation's global turnover of the preceding fiscal year, whichever is higher, can be levied.

For organisations to remain GDPR compliant, having complete control over their data—down to the encryption keys—is essential. The absence of robust BYOK options in Azure and M365 makes it challenging to manage this.

NC ENCRYPT ADVANTAGES

Encrypt Files & SharePoint Columns

Encrypt individual files in supported applications and SharePoint list column values.

Bring Your Own Key (BYOK)

Supply and manage your own keys or use NC Encrypt's dynamically created keys.

Strong Encryption

Uses secure AES-256 bit encryption that is FIPS 140-2 compatible.

Centrally Manage Policies

Centrally manage encryption and access policies across the Microsoft suite from the NC Protect Administration Portal.

Reporting & Auditing

Real-time activity logging and reporting tracks permitted/denied access requests, and actions taken with accessed files.

GAIN CONTROL OF YOUR KEYS IN M365

NC Protect, paired with NC Encrypt from archTIS, offers a solution with an integrated BYOK alternative for M365. It provides independent key management, policy-based dynamic encryption and data access controls to meet the compliance and information security needs of organisations.

Dynamic Encryption and Independent Key Management

The NC Encrypt module provides dynamic encryption capabilities and critical management services to empower organisations to maintain data sovereignty and control over their encryption keys in the Cloud.

With NC Encrypt, sensitive documents are dynamically secured using a system-generated encryption key based on the policies you define. Data can be dynamically encrypted at rest and in motion. For example, build a policy that automatically encrypts any GDPR-controlled personal data stored in M365 or when emailed via Exchange.

You can also extend the Bring Your Own Key (BYOK) approach through a seamless integration with Thales CipherTrust Manager to utilize keys from other HSM platforms.

NC Encrypt streamlines M365 encryption with automatic key generation and efficient and independent key management to provide dynamic protection and encryption of your valuable data, no matter where it lives or travels.

Segment Access to Data with Attribute-based Access Control

Encrypting data at rest is the bare minimum to protect sensitive data in a public cloud. It's also important to note that Gartner recommends that if specific datasets need more robust access controls, you should deploy more granular protection at the individual file level.[2]

NC Protect uses dynamic attribute-based access control (ABAC) policies to control data access and security. Policies can be based on any combination of user (i.e., position, nationality), content (via discovery process rules) and environment (access point to information) attributes to control access to, usage and sharing of individual files. This allows organisations to apply fine-grain access controls to data based on geographical conditions to meet GDPR requirements.

[2] Gartner: Select the Right Key Management as a Service to Mitigate Data Security and Privacy Risks in the Cloud

Contact us to add dynamic encryption and BYOK to safeguard your Microsoft 365 data and comply with data sovereignty requirements.

KEY TAKEAWAYS

The limited BYOK and ABAC capabilities in M365 represent a substantial risk for European organisations and those who conduct business in the EU regarding potential data exposure and non-compliance with GDPR and other European data protection laws.

Recommendations

- Conduct a GDPR compliance audit to assess risks associated with existing cloud services.
- Identify and prioritise data in document management platforms subject to access and data residency restrictions that will need specific attention for encryption.
- Evaluate BYOK alternatives like NC Encrypt for more robust control over data encryption keys.
- Consider using attribute-based access control (ABAC) to fortify data access controls in your Cloud-based document management platforms.
- Seek legal advice to understand the potential implications of using CSPs based outside the European jurisdiction.

By understanding the limitations of encryption key management and access control capabilities in Azure and M365, European organisations can make more informed decisions to better comply with GDPR and other regional data protection laws.

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, SharePoint Server, NetApp, Nutanix Files and Windows file shares.

For more information visit archtis.com. Follow us on twitter @arch_tis

archTIS

archTIS.com | info@archtis.com
Australia | United States | United Kingdom