FEATURE

Protection From GDPR Penalties With an MFT Strategy

Do you have something to say about this article?

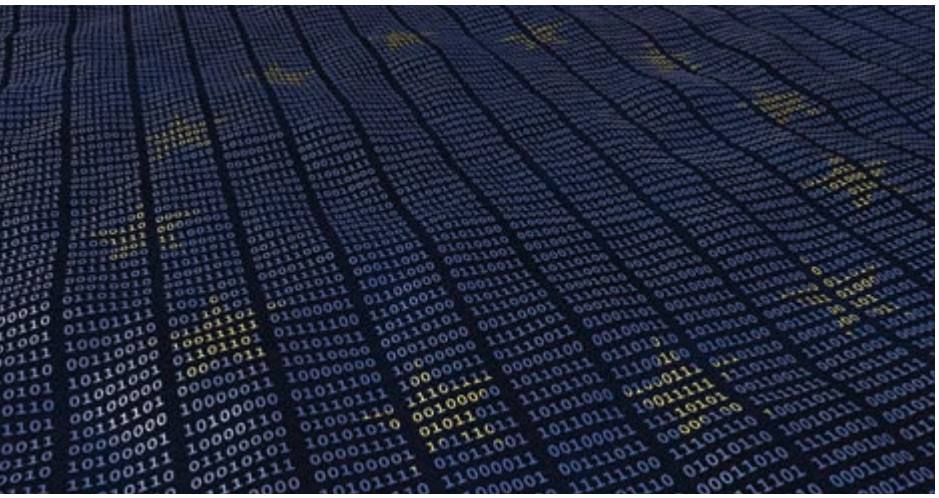
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2sJuwmh

Companies facing the EU's looming General Data Protection Regulation (GDPR) compliance mandate could benefit from a modernized managed file transfer (MFT) solution.

GDPR aims to streamline data protection regulations and strengthen data protection for all individuals affiliated with the European Union. The new mandate applies to any EU company that has an establishment in the European Union, provides goods and services to EU residents, and monitors the behavior of EU residents. What it all comes down to is protecting the rights of an individual's data privacy.

But the GDPR reaches beyond European borders. Any organization, no matter where it operates in the world, selling goods or services to businesses or citizens in EU member countries must comply with GDPR. This applies to any private citizen who simply lives, works or travels through the EU countries—meaning, anyone's personal data can fall within GDPR's scope. Personal data are defined as any information (legal names, bank details, medical information, email addresses, IP addresses, global positioning system [GPS] data and photos among others) related to a natural person or "data subject" that can be used to directly or indirectly identify a person.



Knowing how GDPR compliance involves a complex combination of on-premise and cloud systems and tools, a robust MFT solution and integration platform are useful for any organization in the business of data movement. MFT supports organizational security by enhancing operational visibility and efficiency, and safeguarding sensitive data is an integral part of this new EU mandate. Outdated file transfer solutions will not deliver the auditing, logging, reporting and automation that will help with compliance.

Impact of GDPR

Missing GDPR's 25 May 2018 compliance deadline will be costly when the UK Information Commissioner's Office (ICO) and other EU agencies start auditing companies. Simply failing a GDPR audit means a fine of 2 percent of an organization's annual global turnover or US $12.3 million (€10 million). Data breaches will cost organizations even more. Breached organizations face a hefty fine of 4 percent of annual global turnover or US $21.2 million (€20 million), whichever amount is higher. And gone are the days that organizations could wait months—even years—without divulging information about compromised data. The window to report breaches is tightening. Once an organization is made aware of a breach, hacks that may pose a risk must be reported to affected individuals and to the data protection authorities within 72 hours.

Dave Brunswick
Has more than 25 years of experience in technical sales, presales, technology strategy, engineering, product management and product development, including holding senior consulting and architecture roles throughout the managed file transfer software market. He currently serves as vice president of North America presales and solution support for Cleo.

The fact is, attacks on systems that store personal information, unfortunately, are more and more common in the digital age. This just goes to show that even the most technologically savvy organizations struggle to cover all their bases, leaving them prone to breaches, big or small. But the European Union is trying to raise the bar with GDPR, which aims to streamline the data protection regulations and strengthen protection for all individuals affiliated with the European Union.

Equifax is an example of how hard the GDPR hammer can drop. By now, nearly everyone with a credit report is familiar with the bureau's high-profile data breach.[1] Many people viewed Equifax's fiasco as staggering, egregious and historic. As one of the three major credit reporting agencies in the United States, the Atlanta-based bureau compromised the names, Social Security numbers, home addresses, dates of birth, driver's license numbers and credit card information of nearly 146 million Americans and even 700,000 British citizens.[2]

Arguably, the major concern throughout the credit report breach incident and others like it, such as those targeting Uber and Facebook, has been the lack of immediate transparency, communication and accountability. Equifax's data breach reportedly occurred in mid-May, but it was not discovered by bureau officials until 29 July and was not reported to consumers until 7 September—a 41-day delay before those affected were notified that sensitive personal information had been hacked.

If GDPR had been in effect when Equifax was breached, the credit reporting bureau giant would be facing fines of approximately US $130 million. With that thought in mind, organizations are being forced to think more about digital transformation and adapt new technologies because of a new EU mandate.

Yes, GDPR puts an increased weight of data security on the shoulders of organizations, but that does not mean the majority of organizations that must be compliant are taking necessary action. According to a recent survey,of the nearly 3,000-plus security decision makers in organizations with more than 20 employees in the United States and nine other countries, roughly 30 percent think their organization is GDPR-ready.[3] The report goes on to state that only 26 percent of Europe-based enterprises say they are GDPR-compliant. When it comes down to it, the report says, "the percentage of companies not affected by GDPR is small."[4]

> "AN ADVANCED MFT SOLUTION WILL GO A LONG WAY IN ENSURING THAT ROUTINE BUSINESS-CRITICAL INFORMATION FLOWS ARE NOT RISKING HEFTY NONCOMPLIANCE PENALTIES."

Everything an organization does with data constitutes processing, and virtually every process involves data transfer at some level. MFT is key to ensuring those processes meet GDPR requirements. For industries such as healthcare, supply chain and logistics, financial services, and Software as a Service (SaaS), data transfer is the lifeblood of an organization's operation, keeping in mind that any action on data is technically a processing event, including internal transfers, external transfers, storage, viewing, analyzing, changing, synchronizing and replicating. By deploying a steadfast and secure

Enjoying this article?

- Read *Implementing the General Data Protection Regulation www.isaca.org/implementing-GDPR*

file transfer system that tracks the who, what, where and when of transactions, organizations have the functionality and documentation required to comply with GDPR and beyond.

MFT Solution for GDPR Compliance

An advanced MFT solution will go a long way in ensuring that routine business-critical information flows are not risking hefty noncompliance penalties. Modernization provides advanced security and the control and governance needed to ensure GDPR-compliant data transfers, and the clear, accurate documentary evidence to prove it.

MFT solutions assist enterprises in the management, control and governance of the data flows that power their business ecosystem. A centralized, reliable, scalable and secure file transfer solution can improve business performance, reduce IT complexity and inefficiencies, support corporate cloud and big data initiatives, and reduce risk associated with GDPR data breaches and noncompliance.

The security and visibility of an MFT solution, combined with a data management strategy, will enable an organization to enforce and facilitate compliance directives. Proper procedures, policies and technologies allow for better control and transparency over data that must be protected—whether in movement or at rest. MFT helps enhance organizational security details through operational visibility and efficiency.

A complete MFT solution securely transports personally identifiable information (PII), payment card industry (PCI) and protected health information (PHI) data to and from organizations that must adhere to GDPR compliance by using encryption of data in motion and at rest, nonrepudiation, data integrity checks, comprehensive transfer logging, and integration with existing security systems.

How can a modern and robust MFT solution enable secure PII, PCI and PHI data transfer compliance for GDPR?

- According to GDPR article 5.1, personal data must be processed to ensure the appropriate security of the personal data. With the right MFT solution in place, a two-tier architecture method secures demilitarized zone (DMZ) streaming while data are secured in transit and at rest: Secure Sockets Layer (SSL), Secure Shell (SSH), Pretty Good Privacy (PGP), Secure/Multipurpose Internet Mail Extensions (S/MIME), Extensible Markup Language (XML), Internet Protocol (IP) whitelisting/blacklisting, and US Federal Information Processing Standards (FIPS) 140 -S compliance.
- According to GDPR articles 7 and 8, individuals may give consent to have their personal data collected and/or used when there is no other legal basis to process an individual's information (e.g., vital interest, legitimate interest, contractual obligation), and consent must be separable from other written agreements. GDPR articles 15 and 20 state that EU citizens may request a copy of their data and request a transfer of personal data from organization to organization upon request. That is where an MFT solution can offer nonrepudiation via digital receipts and signatures to ensure the authenticity of a message or document. User authentication is delivered via Lightweight Directory Access Protocol (LDAP) and Active Directory mechanisms.
- According to GDPR article 25, organizations must be able to provide a reasonable level of data protection and privacy. A modern MFT solution has multiple advanced protocols to deliver the flexibility to securely connect a business to all kinds of trading partners (business-to-business [B2B], application-to-application, peer-to-peer). It stores personal data securely by using industry-leading algorithms such as SHA-256 to ensure that personal data are kept secure.
- According to GDPR article 30, records of processing activities must be maintained, including the type of data processed and purpose for which they are used. With MFT, detailed audit trailing and logging centralizes file tracking; filters searchable content; enables dashboards for

enhanced data tracking; and provides alerts and notifications, even non-event alerting.

- According to GDPR articles 39.1(b) and 39.2, a data protection officer (DPO) must be able to monitor compliance with the GDPR regulation. GDPR article 32 says a controller and processor will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. MFT offers delegated administration to distribute supervision capabilities across business units on a centralized browser.

Conclusion

It is up to each organization to determine how it will meet this new EU compliance and avoid mistakes that could be Equifax-like in proportion. GDPR guidelines do not specifically dictate how compliance is done, it just orders what needs to be done, why it needs to be done and when it needs to be done. But accurate management of organizational data cannot happen without the right strategy and tools.

Most likely, the GDPR mandate is just the first wave of what constitutes a global reenvisioning of data security and personal privacy regulation. And, while data integration is not the be-all nor end-all to becoming completely GDPR-compliant, with robust, scalable MFT and B2B solutions in place to centralize and govern all data moving throughout an organization with quick and secure protocols, organizations that must be GDPR-compliant can avoid delaying the inevitable and become a modernized commodity in the continued globalization of data.

Endnotes

1 Equifax, "2017 Cybersecurity Incident & Important Consumer Information," 1 March 2018, *https://www.equifaxsecurity2017.com/*
2 BBC, "Equifax to be Investigated by FCA Over Data Breach," 24 October 2017, *www.bbc.com/news/technology-41737241*
3 Iannopollo, E., *et al*; "The State of GDPR Readiness," Forrester, 31 January 2018, *https://www.forrester.com/report/The+State+Of+GDPR+Readiness/-/E-RES141679*
4 *Ibid*.

"MOST LIKELY, THE GDPR MANDATE IS JUST THE FIRST WAVE OF WHAT CONSTITUTES A GLOBAL REENVISIONING OF DATA SECURITY AND PERSONAL PRIVACY REGULATION."