IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

GDPR – The Benchmark for a Global Privacy Framework

Alasdair Anderson

Alasdair Anderson
Vice President, EMEA
Protegrity

Biography

Alasdair Anderson is Vice President, EMEA at Protegrity (https://www.protegrity.com), and has spent over 20 years working with data technology. Alasdair has spent much of his career in Financial Services with the likes of HSBC, Nordea, ABN AMRO, JP Morgan, RBS & BNP Paribas.

He has been a board advisor for innovative players in the industry such as Trifacta (Alteryx), Waterline Data (Hitachi) and Praxi Data. In recognition of his achievements within the industry, he was appointed to the Global Scot Network.

Alasdair played for Scotland's national handball team and was also Vice Chairperson of the national handball association. Originally from Glasgow, Scotland, Alasdair now resides in Amsterdam.

Keywords General Data Protection Regulation (GDPR), Data security, Data privacy, Data breach fines, Supply chains
Paper type Research

Abstract

The introduction of the General Data Protection Regulation (GDPR) set the precedent for privacy and data laws around the world with 71% of countries now having data protection regulations in place and a further 9% with legislation in development. But as we reflect on the fifth anniversary of GDPR's introduction the complexity, volatility and diverse requirements of the regulation continue to add a challenge to the international data flows driving growth and innovation globally. But what is next for GDPR and wider international regulations? In the article, the author looks back on the last five years of GDPR, the benefits, issues and what the future could hope for the regulation.

Introduction

General Data Protection Regulation (GDPR) continues to be a game-changer, setting the precedent for privacy and data laws around the world. In fact, the United Nations Conference on Trade and Development (UNCTAD) recently reported[1] that 71% of countries now have data protection regulations in place and a further 9% have legislation in development. Countries such as Vietnam and Saudi Arabia have recently introduced new privacy laws.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

But, as we reflect on the fifth anniversary of GDPR's introduction, the first billion-dollar fine has been issued. So, what does this mean for data privacy moving forward?

The impact of GDPR

Where once enterprises could buy, sell, share, and store customer data with relative freedom, for the last five years every organization that operates under the GDPR has been subject to scrupulous regulatory compliance requirements. Brands like Amazon, WhatsApp and Google are just a few of many that have been fined for breaches.

In many cases, the GDPR has been successful in protecting consumer privacy by setting clear guardrails for how businesses should protect data travelling through the EU. However, today's global supply chains and international corporate footprints require data to be shared across borders, and whilst we understand the intentions behind data sovereignty regulations, the GDPR has enforced antiquated policies that have stifled innovation, arrested economic growth, and overlooked the many technologies that are transforming data privacy for the better. It has also raised issues around the data transfers needed for businesses to comply with important international regulations such as anti-money laundering and sanctions. Therefore, while the GDPR has been hailed as one of the most robust data governance, data management and data transparency regulations in history, many organizations, particularly those in the US, are still ill-equipped to comply with it.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Does the decision on Meta shift the needle?

One clear challenge of the GDPR has been that there is no definitive way for business leaders to achieve compliance. The language used is performance-based, meaning that while the mandated outcomes of GDPR are clear, for example, ensuring user data doesn't fall into the wrong hands, the ways to get there are very generalized and largely seen as 'up to the company' to put in place.

Additionally, fines to date haven't been that onerous. That changed with the Meta fine and six-month window to stop data transfers from the EU to the US. Effectively, the basis of Meta's fine is that, while it had contractual language in place to treat EU data differently from a legal standpoint, it had no demonstrable controls in place to show that it was actually doing so. This ruling puts an end to paying lip-service to compliance; without demonstrable controls governing data movement, a company will find itself outside the law and therefore liable.

This clearly shifts the needle on the importance of data protection to business. It firmly cements data protection – and proof of data protection – as not a 'nice-to-have' but a necessity to operating, and one that every organization must take seriously.

Fines in the billions have previously been reserved for the worst breaches of corporate responsibility. Now, however, the €1.2 billion figure casts a large shadow over the previous EU record fine of €746 million handed to Amazon. The fact that the figure is comparable to fines relating to the money laundering scandals of

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Westpac ($1.3 billion), Danske Bank ($2 billion), and HSBC ($1.9 billion) only further highlights the importance of this decision to the future of data protection and EU-US data flows.

The decision will have implications that will ripple far beyond the tech ecosystem. Industries that are heavily reliant on cross-border data flows – particularly supply chain, manufacturing, and petroleum/chemical – will now be scrutinizing their use of data more than ever before.

Raising the privacy bar

As a result, we are likely to see the bar being raised in terms of how organizations prioritize privacy regulation. It will certainly get organizations to reflect on adequacy and what they need to do to achieve it.

Without a doubt it is challenging to be fully globally compliant. There will never be a single global regulation covering all territories, instead there will be a patchwork of bilateral regulations. Therefore, industry as a whole needs to reach consensus on what is acceptable, or deemed the gold standard? What is going to be the standard that organizations follow and how does that have equivalence across the world? In pursuit of that goal, we're seeing two words are becoming highly significant: 'adequacy' and 'equivalence'. Adequacy – in other words has the organization done enough? And the issue for US companies is equivalence. The EU has determined that US law doesn't fulfil EU standards so, because of this lack of equivalence, they must comply with GDPR as the superior standard.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

GDPR paves the way for an international framework

While challenges undoubtedly exist, the fact that GDPR has had such strong influence over the shape of national privacy regulations worldwide offers the opportunity to use it as a foundation for a workable international data governance framework. Such a framework would need to be flexible enough to accommodate changes to national privacy regulations, while ensuring equivalence with the key principles of GDPR is maintained.

The framework would establish and clearly articulate the controls required for data to move safely, allowing organizations to build and deploy compliant protections. Once built, these protections can be automated and audited to ensure strong governance.

This approach provides a wealth of benefits to organizations as they focus on achieving workable data protection and compliance. It allows them to build scalable data protection and control systems at speed, based on universal principles. It avoids having to tailor systems to every jurisdiction, with the associated risk of human error in decision-making. Also, by deploying a platform-based controls system, organizations can achieve the agility they need to stay up to date with any changes; when a regulatory change happens, the relevant control is adjusted accordingly, allowing data flows to continue uninterrupted.

In conclusion – GDPR has set the gold standard

Ultimately, the free flow of data is a driver in the global economy and essential for organizations across every sector. Data must be moved not just for commercial purposes, but also to address a variety of critical issues such as compliance with regulations around sanctions and Environmental, social, and corporate governance (ESG), so it is essential to find a route forward that balances privacy with compliance obligations. GDPR has set the gold standard for data sharing while keeping it protected and should form the basis of an international data governance framework that facilitates protected, effective cross-border data flows.

Reference

1 United Nations Conference on Trade and Development (UNCTAD), Data Protection and Privacy Legislation Worldwide. Available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide