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

United States Data Privacy at a Glance

Adam Strange

Adam Strange
Global Marketing Manager
Titus, by HelpSystems

Biography

Adam Strange heads up the global marketing function at Boldon James, and is the Global Marketing Manager for Titus, by HelpSystems (https://www.titus.com), working to define and implement our strategic go-to-market campaigns. He brings a proven and successful record of managing integrated business-to-business marketing activity to both increase brand profile and capture leads and opportunities.

Adam has a widespread understanding of enterprise IT infrastructure across areas such as Cybersecurity, Threat Intelligence, Cloud-based Services, Business Applications, Databases and Hardware.

Prior to Boldon James, Adam ran the marketing and alliances function at Becrypt, and has held former marketing and partnering positions at BAE Systems, Oracle and Computacenter.

Keywords Data privacy, Data legislation, Data protection, CUI, United States policy, Data breach
Paper type Research

Abstract

Data privacy protection is both a fundamental right and an economic need, as data breaches grow in impact and frequency. While regulations like GDPR are now well-established, the United States of America has been relatively behind on regulating the collection, storage, and use of personal and sensitive information. Recently, however, the tide is turning. In this article the author examines the momentum of data protection acts at a state level, comparing the various regulations that have passed in recent years and their impact on companies and consumers within those legislative areas.

Introduction

As more and more social and economic activities move online, the importance of privacy and data protection is becoming increasingly recognized. Of equal concern is the collection, use and sharing of personal information with third parties without notice or consent of consumers. In fact, I read recently on the UNCTGAD site[1] that 128 out of 194 countries have put in place legislation to secure the protection of data and privacy.

Whilst the United States of America (US) has been lagging behind other countries in terms of implementing national legislation, the picture is now beginning to take a

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**

different path at state level as legislative bodies introduce regulations. Some states such as California, Vermont, New York, and Ohio have introduced data protection legislation in some form, Alabama has its Data Breach Notification Act 2018 and as recently as last month Colorado passed its new data privacy bill, giving residents the right to stop companies from collecting their data in the future. There is now a significant movement towards safeguarding data privacy and increasing data protection state by state.

We are now seeing moves from the US Federal government as well. In May, President Biden published his Executive Order on improving the nation's cybersecurity as a whole, showing how the thought process has stepped up a notch.

The reason for this is obvious. You don't have to cast your mind too far back to be able to cite high profile cases in the press which showed us how important strong data protection rules are for society, including the very functioning of the democratic process.

These and other developments have shown that the protection of privacy, as a fundamental individual right, but also as an economic necessity, is crucial. Without consumers' trust in the way their data is handled, our data-driven economies will not thrive.

As a practitioner working in the field of data security[2], I'm pleased to see data privacy and protection laws becoming more commonplace across the US Data protection is the "one constant" that must be maintained across all environments. Organizations hold and are responsible for safeguarding vast amounts of data and this data must be appropriately protected, irrespective of its type or location.


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**

With personal data protection and privacy law rapidly evolving in the US, and without principal legislation that governs data protection at the federal level in the US as yet, one could be forgiven for wondering which regulations are most critical to be aware of. With that in mind, let us take a whistle-stop tour of some of the important and forthcoming laws you need to be aware.

General Data Protection Regulation (GDPR)

Though of course not a US piece of legislation, but a critical one to conform to if, as a US company, you transact with the EU or the UK.

The most important data protection legislation enacted to date is the General Data Protection Regulation (GDPR). It governs the collection, use, transmission, and security of data collected from residents of any of the member countries of the European Union. The law applies to all EU residents, regardless of the location of the entity that collects the personal data. Fines of up to €20 million or 4% of total global turnover may be imposed on organizations that fail to comply with the GDPR.

GDPR's seven principles are: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and


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**

confidentiality (security); and accountability. Some important requirements of GDPR include:

- Though GDPR was established in the EU, it applies to businesses all over the world. If your website collects the personal information of someone from one of the EU member states, then you're required to comply. Otherwise, you could be faced with fines and penalties.

- Data subjects must be allowed to give explicit, unambiguous consent before the collection of personal data. Personal data includes information collected through the use of cookies.

- Organizations are required to notify supervisory authorities and data subjects within 72 hours in the event of a data breach affecting users' personal information in most cases.

- In a lot of cases the GDPR can require organizations to appoint a data protection officer (DPO). For example, businesses in the public body, those with large scale monitoring of individuals or processing large amounts of criminal data. This independent data protection expert is responsible for monitoring an organization's GDPR compliance, advising on its data protection obligations, and acting as a contact point for data subjects and the relevant supervisory authority.

California Consumer Privacy Act (CCPA)

Though of course not a US piece of legislation, GDPR is nevertheless a critical one to conform to if, as a US company, you transact with the EU or the UK.

The most comprehensive state data privacy legislation to date is the California Consumer Privacy Act (CCPA). Signed into law on 28 June 2018, it went into effect on 1 January 2020. The CCPA is cross-sector legislation that introduces important definitions and broad individual consumer rights and imposes substantial duties on entities or persons that collect personal information about or from a California resident. These duties include informing data subjects when and how data is collected and giving them the ability to access, correct and delete such information.

This notice must be disclosed in a privacy policy displayed on the website of the entity that collects the data:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

Virginia's Consumer Data Protection Act (CDPA)

Virginia's Consumer Data Protection Act (CDPA)[3] was passed on 2 March 2021. It grants Virginia consumers rights over their data and requires companies covered by the law to comply with rules on the data they collect, how it's treated and protected and with whom it's shared.

The law contains some similarities to the EU General Data Protection Regulation's provisions and the California Consumer Privacy Act. It applies to entities that do business in Virginia or sell products and services targeted to Virginia residents.

Colorado Privacy Act (CPA)

In June 2021, Colorado became the third US state to pass a privacy law. The Colorado Privacy Act[4] grants Colorado residents rights over their data and places obligations on data controllers and processors. It contains some similarities to California's two privacy laws, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), as well as Virginia's recently passed Consumer Data Protection Act (CDPA). It even borrows some terms and ideas from the EU's General Data Protection Regulation.

While there are similarities, such as the opt-in requirement to obtain consent from consumers before collecting sensitive data, and the adoption of some privacy-by-design principles, the significant differences are in the details.

The CPA applies to businesses that collect personal data from 100,000 Colorado residents or collect data from 25,000 Colorado residents and derive a portion of revenue from the sale of that data.

The CPA is scheduled to come into effect on 1 July 2023.

New York SHIELD Act

In July 2019, New York passed the Stop Hacks and Improve Electronic Data Security (SHIELD) Act. This law amends New York's existing data breach notification law and creates more data security requirements for companies that collect information on New York residents. As of March 2020, the law is fully enforceable. This law broadens the scope of consumer privacy and provides better protection for New York residents from data breaches of their personal information.

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**

In conclusion – Importance of privacy policies

Any website should have a privacy policy that explains to its users what information is collected, how it is used, how it may be shared, and how it is secured. To be fully compliant with US and EU data protection laws, all data subjects should have the opportunity to consent to the collection of personal information. While much information about users is voluntarily provided when they sign up for newsletters, complete forms, or send email requests, information gathered from third parties and through the use of cookies should also be disclosed, and users should be given the opportunity to consent to, block, or disable cookies.

With the implementation of data privacy legislation continuing to sweep through countries globally, a list which now increasingly includes the US, awareness of the key tenets of the laws that relate to your organization's business practices are essential. Once you know how you are expected to protect consumer data, you can build a strategy around your people, processes and technology that ensures you comply with prevailing data privacy laws. In so doing, you are safeguarding your customers against theft, loss, or misuse of their personal information, as well as protecting your organization from the risk of hefty penalties for non-compliance.

Reference

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

2 HelpSystems, 'Data Security: ensure sensitive data is well protected', HelpSystems. Available at: https://www.helpsystems.com/solutions/cybersecurity/data-security?

3 Commonwealth of Virginia, *Consumer Data Protection Act (CDPA)*, Virginia's Legislation Information System. Available at: https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+HB2307ER

4 State of Colorado, *The Colorado Privacy Act*. State of Colorado. Available at: https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf