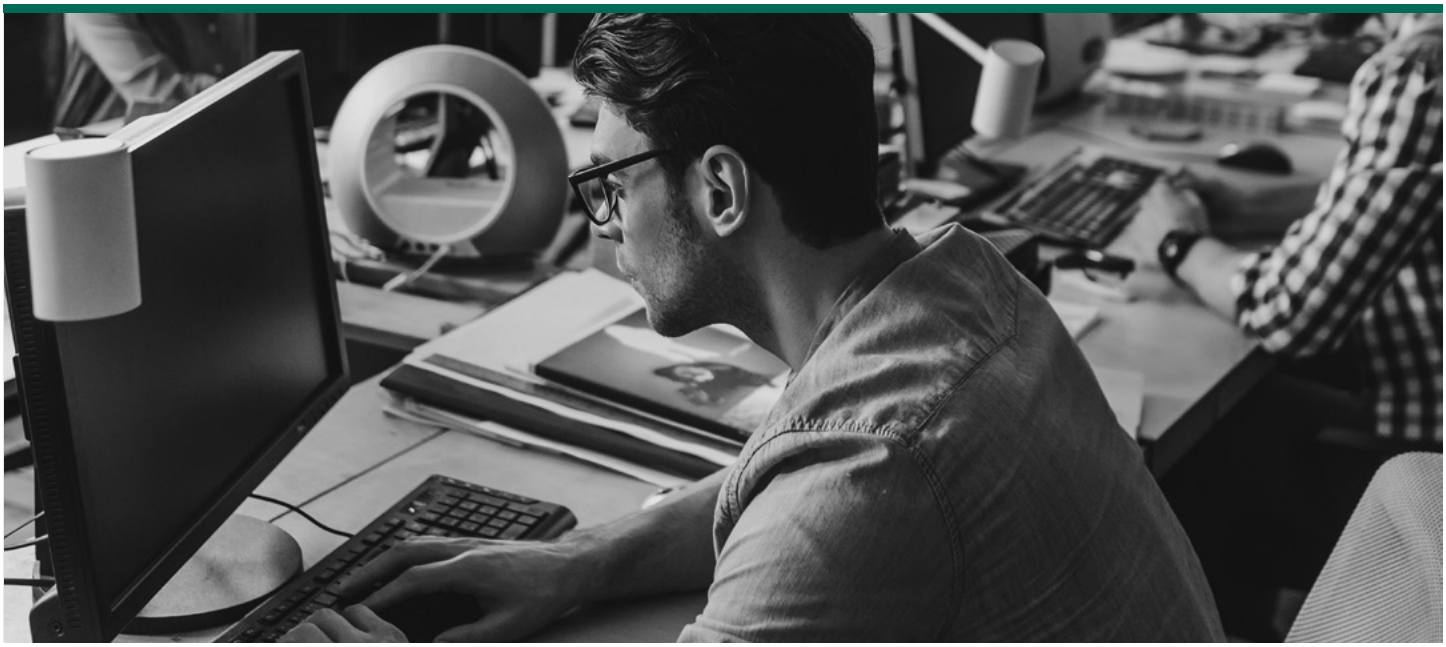
FORTRA

WHITE PAPER (Boldon James)

Classification By Design: The Foundation Of Effective Data Protection Compliance



Including

- How data breaches are driving regulatory change
- Data protection and the COVID-19 pandemic
- An escalating external threat environment
- How insider breaches are catching organisations out
- The approach organisations should be taking to achieve robust compliance and mitigate data breaches
- Classification by Design
- How privacy will reign as the top compliance regime

Executive Summary

In this paper we look in detail as to why achieving compliance across a wealth of new international data privacy laws and regulations is such a growing challenge. As more and more legislation impacts businesses worldwide and organisations struggle to keep pace, we cite leading research undertaken by analyst firm Forrester. In their research, Forrester demonstrate that for the global security decision makers surveyed, a significant proportion have not yet invested in data discovery and classification (45%) and in other data security controls (44%) in their efforts to help fulfil their compliance obligations. We discuss why. Are they apathetic? Do organisations deem that compliance is unimportant or is it too big a problem? Are they too busy and not prioritising compliance, or do they simply not know where to start?

The reality is that all of these factors are in play to varying degrees. One thing that is certain is the growing complexity within the compliance landscape will increasingly impact organisations not just in terms of regulatory fines and financial costs, but also in reputational damage should they be (or when they are) breached.

We examine the evolving external and internal risk landscape, particularly in light of COVID-19. We home in on the fact that Forrester identifies that nearly half of breaches happen as a result of human error, which is why it is more important than ever for organisations to take compliance seriously.

Finally, the paper will lay out key steps to help organisations sensibly adopt a better data protection posture and with it, build a firm foundation towards onward compliance. The key principles of Classification by Design will be introduced as a logical, yet robust start point. We summarise with the overarching takeaway that organisations should not view compliance as an expense, but as a positive competitive differentiator and one that, over the long term, will prove to deliver efficiencies back to the business.

Introduction

Organisations are increasingly adopting new technologies to communicate with their customers and their supply chain, often taking advantage of cloud-based technologies to expand their capabilities and further reduce their cost base. The emphasis is on broadening methods of accessing and distributing data allowing, for example, customers to interact with their data on an organisation's systems by inputting their own orders and address details.

As a result, opportunities have run ahead of both the regulators and security professionals. As the cyber risk environment has intensified, regulatory authorities have scrambled to catch up. Consequently, as they have done so, businesses worldwide now face a barrage of new privacy regulations, some of which have yet to be put to the test. The risks of non-compliance are severe, security professionals caught off guard by the speed of change are wondering how their organisation can protect data and mitigate risk in today's volatile, complex and uncertain world?

Not long ago organisations operated closed systems, with most data processing on their own systems and the ability to communicate directly with the outside world limited to email and telephone. The data protection laws in place were benign, with only repeat or very serious offenders receiving a fine. The data protection landscape and its associated compliance environment changed fundamentally with the implementation of the European-wide GDPR in May 2018, with many other privacy regulations following suit around the globe. A year after the launch of GDPR, the first fines issued by the ICO left no one in doubt that this regulation has teeth. Record financial penalties for organisations such as Google, Facebook, Marriott and British Airways were a salutary lesson to businesses across the board that they cannot afford to fail against these regulations. Increasing public awareness of privacy rights means the damage is not just financial, but reputational too, a factor that is infinitely more difficult to measure, but can be catastrophic and long-lasting.

It is too early to say whether the appeals against some of these fines will adjust our understanding of the impact of GDPR, however a recent case against the backdrop of the UK 1998 Data protection Act held that companies were liable for ensuring that data protection by design and default was a company responsibility. If an employee deliberately stole data and circumvented systems, they could mount that as a defence, but if the leak was accidental and the systems not strong enough to protect their users from error then it is the responsibility of the company, not the user.

And in 2020, the lock down caused by COVID-19 introduced a scale of home working on a level that we've never experienced before. This is the very definition of disruption and exactly the kind of scenario where data protection and security can fall through the cracks as new threats – both insider and external - emerge. As more organisations, under government guidance, move to home working, concerns around how organisations keep data safe and secure whilst remaining compliant should be front of mind for both security teams and employees alike.

The ICO Signals Serious Intent

In July 2019, the UK's Information Commissioner's Office (ICO) announced its intention to issue the first fines levied as a result of breaches to GDPR. British Airways (BA) was ordered to pay the sum of £183.39m for a data breach it reported in September 2018, which saw the personal data of around 500,000 customers compromised. The ICO's investigation into the breach found evidence of poor security arrangements by BA.

A second intention to fine was announced just over a week later in relation to Marriott Hotels, whose Starwood subsidiary was the subject of a long-term breach that exposed personally identifiable information (PII) in around 339 million guest records, including 30 million belonging to European Economic Area residents and 7 million belonging to UK residents.

Breaches Are Driving Regulatory Change

Serious data breaches and incidents of cyber-intrusion have a powerful effect on driving regulatory focus and change. To this point, since 2018 there have been a flurry of new global privacy acts including GDPR, CCPA, the Australian Privacy Act, DPTM, Japanese Privacy Law and others around the world, which have come into force and have seen organisations scramble to get their houses in order.

The extent to which businesses are concerned about meeting new regulations was evidenced by recent calls to delay the start of enforcement of the CCPA - scheduled for July 1, 2020 - because of disruption caused by the COVID-19 pandemic. However, authorities are unmoved, with California's Attorney General Xavier Becerra stating that enforcement of the regulation, which has been in place since January 1, 2020, will commence on schedule. Ominously, Becerra added: "We encourage businesses to be particularly mindful of data security in this time of emergency."[1]

Consumer awareness of privacy laws has grown exponentially:

"We received around 14,000 PDB reports from 25 May 2018 to 1 May 2019. For comparison, we received around 3,300 PDB reports in the year from 1 April 2017."

Source: *The ICO*

"There is more and more regulatory complexity around the world, and GDPR, CCPA and other privacy laws are driving this "

For the most part, all these different compliance regimes are in fact very similar in their desire to value data and protect it accordingly - the difference between these various regulations is the data in question. There is no doubt that businesses are facing a heavier burden than ever before when it comes to proving they are meeting data protection and cybersecurity obligations.

Data Protection And The COVID-19 Pandemic

The Information Commissioner's Office (ICO) recognises the extraordinary challenges organisations are facing in relation to COVID-19, but it is also advising that data protection should not be viewed as a barrier. Concerns about data sharing risks should not prevent employees working from home, using a mix of their own and work devices, but the ICO is advising companies that businesses need to consider the same kinds of appropriate security measures for home working that they would use in normal circumstances, and it states: "We know you might need to share information quickly or adapt the way you work. Data protection will not stop you doing that. It's about being proportionate."

Likewise, the Financial Conduct Authority (FCA) is working closely with Government, the Bank of England and the Payment Systems regulator to take the necessary steps to ensure customers are protected and markets continue to function well. It is advising firms to take all reasonable actions to meet the regulatory obligations which are in place to protect their consumers and maintain market integrity.

The underlying tone of both these messages is that a crisis situation is not an excuse for failing to meet data security obligations and that, as organisations rapidly adapt working practices, productivity must not be achieved at the expense of protection. The perception of the regulator is that organisations are prepared, they understand their data, what it is, where it is and who should access it or who it should be shared with. Decisions on how to cope with extended homeworking, a broader use of personal devices and increased reporting requirements, such as who is working, self-isolating or sick using unstructured data streams like email or a Zoom meeting, are much easier if organisations are as prepared as the regulator assumes.

[1] Duball, J. "California attorney general's office: No delay on CCPA enforcement amid COVID-19". www.iapp.org. 24 March 2019. Accessed at https://iapp.org/news/a/making-sense-of-calls-to-delay-ccpa-enforcement-amidst-covid-19/

An Escalating External Threat Environment

There is no doubt that COVID-19 will create additional security threats as threat actors attempt to take advantage of the increased proportion of the workforce spending more time online while at home and working in unfamiliar circumstances. Some of the biggest threats associated with the pandemic include phishing emails, spearphishing attachments, cybercriminals masquerading fake VPNs, remote meeting software and mobile apps and a new family of ransomware known as Coronavirus that has recently been reported.

In response to this heightened threat environment the frequency of breaches will likely increase. However, as the tone of communications from the ICO and FCA indicates, regulators will continue to expect frameworks, guidelines and legislation to be adhered to, as compliance becomes even more important. GDPR and similar laws require companies to demonstrate compliance and provide mechanisms for individuals to check that a company is handling their data appropriately. These compliance regimes are not suspended during the pandemic.

The Internal Threat Environment: Insider Data Breaches Are Catching Organisations Out

One area that is still causing considerable concern from a compliance perspective is the threat of an insider data breach. In fact, according to a recent Forrester report by analyst Heidi Shey entitled: "The State of Data Security and Privacy, 2020", among breaches in the past 12 months, 46% involved insiders like employees and third-party partners - the majority of which were simple errors.

> "Personally Identifiable Information (PII) remains the top type of data that global security decision makers most often say has been compromised or breached. IP is also high on the list along with sensitive corporate data."
>
> ***Source:*** *The State Of Data Security And Privacy, 2020, Heidi Shey, Forrester*

This is consistent with what Forrester witnessed in 2018: "News headlines of insiders stealing trade secrets from companies like Hershey, Philips, and Tesla lead us to assume that insider threats are based on malicious intent, but the reality is that inadvertent misuse of data and lost devices cause a concerning proportion of incidents and breaches. From a compliance perspective, insider breaches are perhaps even more damaging, as organisations have more control here than with external threats."

What Approach Should Organisations Take To Mitigate The Risk Of A Data Breach?

Today every investment an organisation makes in cybersecurity and privacy technology has to be about protecting data, with the goal of improving security performance and boosting its ability to demonstrate a compliance position in this highly regulated environment.

In its report, Forrester defines data security and privacy technology as technologies that directly touch the data itself and that help organisations: 1) understand where their data is located and identify what data is sensitive; 2) control data movement as well as introduce data-centric controls that protect the data no matter where it is; and 3) enable least privilege access and use.

The report went on to highlight that among global security decision makers, 49% indicated that they had invested in privacy management software to comply with data protection regulations. They also reported investing in data discovery and classification (45%) and other data security controls (44%) to help fulfil their compliance obligations. This highlights that, while some businesses recognise that technology investment is critical to meeting regulatory requirements, more than half of those surveyed haven't invested in privacy management technology, which is concerning and demonstrates a level of apathy or uncertainty over the most effective approach to take.

Classification By Design

One of the best methodologies that an organisation can use to fulfil their compliance obligations is adopting a data protection by design and default approach. This is an approach that takes privacy into account throughout the whole process, ensuring that this approach includes your systems, policies and processes and your technologies. Data protection by design and default needs to start with data classification.

The sheer volume of unstructured data within organisations combined with the ever-increasing technical abilities of hackers and the fallibility of employees makes it impossible to rely on people and processes alone to ensure that sensitive data is handled appropriately. Data classification embeds a culture of compliance by involving users to identify, manage and control the regulated data they work with, while automating parts of the protection process to enforce rules and policies consistently. Data is classified at source so the organisation's rules can be applied at the outset.

> "Data stewardship will correctly align to regulations only when the data owners are identified and engaged."

Let's face it, you can't properly protect what you don't know you have. Therefore, understanding what data you have, who is using it, how it is being stored, classified and shared, and whether it is company-sensitive, is key to any data protection strategy.

Once you have defined what data you have, you will be able to classify it. Data classification is the categorisation of data according to its level of sensitivity or value, using labels. These are attached as visual markings and metadata within the file. When classification is applied the metadata ensures that the data can only be accessed or used in accordance with the rules that correspond with its label.

Clearly you need to define your classification policy first and decide who should have access to each type of data. Once you have done this you will need to select an appropriate classification tool; the right technology will help your users to consistently apply the classification scheme with ease. The most effective tools make classification a seamless part of business-as-usual.

Once data is appropriately classified, security tools such as Data Loss Prevention (DLP), policy-based email encryption, access control and data governance tools are exponentially more effective, as they can access the information provided by the classification label and metadata that tells them how data should be managed and protected.

Privacy Will Reign As The Top Compliance Regime

Numerous regulatory regimes will continue to be developed but privacy will reign moving forward. The tone from the various regulatory bodies' communications around COVID-19 indicates that businesses cannot afford to take their eye of the data protection ball, even during these challenging times.

When it comes to privacy, most countries have aligned to the standard of GDPR with some appropriate domestic legislation incorporated. Therefore, if organisations work to incorporate GDPR requirements - including the mandate to ensure data protection by design and default - into their compliance regime, they won't go far wrong.

While compliance with data protection regulations is non-negotiable and the penalties for failure are severe, it is a mistake to see compliance solely as an inevitable burden. With an intelligent and proactive approach, organisations can pivot from viewing compliance only as an expense and turn it into a positive competitive differentiator and one that, over the long term, will prove to deliver efficiencies. Organisations need to focus on lowering the barriers to data privacy compliance because their data classification tools provide a faster, more intuitive path to finding sensitive data - a critical first step in any compliance and data protection strategy.

Here are a few pointers to keep top of mind when looking at data classification and your compliance strategy:

- IT security and operations do not own business data – so don't look to the CISO for all the answers.
- Data stewardship will correctly align to regulations only when the data owners are identified and engaged.
- Identify and engage stakeholders right across the business, including risk, legal, and compliance. This is critical to the success of your compliance programme.
- Organisations must educate users as a whole about the sensitivity of data and ensure the appropriate controls are in place around confidential and sensitive information.
- Alert users when data is leaving the organisation to warn them before sending messages that contain sensitive information.
- The first step is the need to classify or label data with visual labels to highlight any specific handling requirements.
- Then, secondly, ensure metadata labels enforce security controls to stop unauthorised distribution of data.
- Link data classification tools to solutions such as DLP, encryption and rights management to enhance overall data protection.
- Make sure you provide critical audit information on classification events to enable remediation activity and determine your compliance position to the regulatory authorities.

A Flurry Of New Or Updated Privacy Laws

The **Australian Privacy Act** was recently amended to include mandatory data breach notification provisions that require certain entities to notify individuals and the regulator of 'eligible' breaches.

The Singapore government announced the **Data Protection Trustmark Scheme (DPTM)** in July 2018, following the theft of the personal data of 1.5 million SingHealth patients.

The **Personal Information Protection Commission** was set up in 2016 under the **Japanese Privacy Law**. A subsequent amendment of the law in 2017 introduced the definition of "Special care required around personal information".

The Information Technology Personal Information Security Specification was effective in China in May 2018. It provides a set of data protection rules for companies that obtain and use personal information.

New Zealand introduced a bill to amend its privacy legislation in March 2018. **The Privacy Bill** repeals and replaces the 25-year-old Privacy Act of 1993.
May 2018 marked a significant shift in privacy and information rights with the implementation of the EU **General Data Protection Regulation (GDPR)** and the UK **Data Protection Act 2018**.

The California Consumer Privacy Act (CCPA) came into force in January 2020. It is considered to be the US counterpart of GDPR.

Summary

Adopting a data protection strategy with effective classification as its foundation means that the pillars of people, process, training and technology have a strong base on which to build. When data is effectively classified, users and the other layers of security that support them gain certainty over how data should be handled. Grey areas are reduced and mistakes are less easily made or eradicated, especially when users are supported by automatically applied policies based on the data's classification status.

Data that has been classified becomes the foundation on which the next layers of security can be built. Once you have identified what the data is, you can then introduce the 'how' in terms of how to protect it. Since not all data is equal, protecting it will vary. From a compliance point of view, getting this right is fundamental.

Ultimately, in today's highly regulated data environment, organisations need to be positive and proactive about building an effective compliance strategy, not overawed by

the scale of the challenge. Those with low levels of privacy management software adoption identified by Forrester need to rise, but more broadly, companies need to obtain better visibility of their unstructured data before they can consider themselves compliant with relevant privacy regulations. By starting with data classification, they can achieve the confidence they need to overcome uncertainty and start turning compliance into competitive advantage.

Global Brands Trust Us to Protect Their Sensitive Data:

More Information

For more information about how you can implement a data classification solution as part of your data protection strategy, please **contact us**

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.