BIG DATA PROTECTION

Fouad Khalil *reports of the varied difficulties of keeping up with changing data regulations around the world*

For decades the personal information of individuals has largely been treated as a commodity to be harvested, bought and sold like any other resource. The trend accelerated as we entered the digital era, with the vogue for big data analysis meaning companies increasingly sought to collect as much information as they could get their hands on in the hopes of wringing useful insights out of it.

This fascination with data has enabled many companies to unlock powerful new opportunities, from shaping product development to enabling more effective, targeted marketing and sales activity. Indeed, some of the world's largest and influential companies, such as Facebook, are built primarily around commoditising the data of their users.

In many cases though, the data economy has come at the expense of the privacy and security of the consumer. Unscrupulous or opaque practices around harvesting and selling data meant individuals had little way of knowing what personal information was being collected and where it ended up.

As a result, we have all endured years of unwanted sales calls and spam emails, or even outright fraud and cyber crime when data has fallen into the wrong hands. And, thanks to widespread poor practice around managing and securing data, personal information has ended up in the grasp of criminals and hackers with alarming regularity.

Ute con corum quo comnis ad es remquasperum is res sit et diatiusam voluptatem repratu

Picture credit: Getty

However, the status quo has finally begun to shift. The last few years have seen a tidal wave of regulatory changes sweeping the world with the intent of washing away the careless and malicious treatment of personal data. All around the globe, citizens now have more control and ownership of their personal information, while regulatory bodies have the power to punish companies that fail in their duty to protect the security and privacy of data in their care.

While this global movement towards greater data protection can only be a good thing for the wellbeing of the consumer, it also means that businesses must navigate an increasingly complicated regulatory landscape as new laws and restrictions are added in different parts of the world.

Businesses must be able to keep track of how different regulations will affect their operations, and ensure they have the resources to stay compliant regardless of geographical location.

The EU General Data Protection Regulation (GDPR) is often credited with setting the new era of data protection into motion. EU citizens had been covered by the Data Protection Directive since 1995, and most European countries had their own individual laws in place, such as the UK's Data Protection Act 1998. However, the GDPR took a much stronger stance than any before, with greater, more specific rights for individuals and clearer-cut obligations and consequences for organisations.

One of the most important aspects of the GDPR is the introduction of the Data Subject Access Request (DSAR), which enables all EU citizens to request from any organisation details on any data they hold on them, request a copy, have its use limited, or demand it is deleted entirely. It is also notable that these rights are extended to any citizen of the EU regardless of their current residence and can be applied to any organisation around the world that collects or manages relevant data.

After its entry into law in May 2018, enforcement of the GDPR has varied from country to country, with some nations appearing to make little headway toward the sea change set out by the regulation. That said, the GDPR has been responsible for several landmark actions against companies that have failed to comply with the regulation, including some eye-watering fines.

In particular, the UK's Information Commissioner's Office (ICO) has issued two extremely large fines, with British Airways and Marriott International being fined £183-million and £99-million respectively for serious breaches in 2018.

While these high-value fines get the most attention, many other EU nations have been quietly enforcing the regulation in a bid to improve the overall quality of data protection. The DLA Piper GDPR Data Breach Survey, published in February 2019, found the Netherlands had raised 15,400 issues, the most of any EU nation when weighted against the population.

The GDPR currently represents the strongest set of data privacy and security laws around the world, and organisations that are looking to tighten their data management would do well to use it as the basis for any new policies.

Outside of Europe, the United States has also been making progress towards better data protection. Somewhat ironically, the country currently lacks the unified approach of the EU GDPR, with new regulations being issued on a state level rather than as federal law. This means US citizens in different states will experience different levels of protection, and businesses will need to be particularly careful about privacy mandates that differ from state to state.

California has the distinction of being the first state to introduce new laws, with the California Consumer Protection Act (CCPA) came into effect in January 2020. The regulation follows a similar path to the GDPR, including granting key rights around the disclosure, deletion, opt-out and non-discrimination of personal data. It also introduces punitive fines for companies that are noncompliant or are deemed to have failed to implement sufficient security in the event of a breach. Although deemed as 'GDPR-lite' for not going far enough, the CCPA does represent a step forward for American citizens – albeit only Californians for now.

AM, OPTA NIMIL INCIIS ES EATI ANTIBUS IL MOLUPTAS SIT PRERUM FUGIATIA VOLUME SITIUM REPTATIS

On the other side of the country, the proposed New York Privacy Act aims to take a stronger stance, potentially becoming one of the strictest sets of data laws in the world. The act would require a high degree of transparency about how data is collected, stored and used, including a more proactive approach to alerting users when data is to be shared with third parties. It would also grant consumers the power to launch legal action on an individual basis, rather than relying on a regulatory body or class action lawsuits. However, the act has so far failed to pass, with many speculating that its proposed powers go too far and have alienated support from business lobby groups. The proposal will be reintroduced in the next session in 2020, so it will be some time before it is passed into law – if it ever succeeds in its current form.

India is another nation looking to continue the global momentum of data protection. Already home to some of the world's biggest tech companies, it has had a strong focus on bringing the digitalisation revolution to its 1.39-billion strong population. The Digital India project has implemented initiatives including the establishing of high-speed internet to previously isolated areas, and improved access to digital skills. Alongside this, the Government is also working on the Draft Personal Data Protection Bill, 2018, which is expected to be tabled in the near future. The proposed bill includes particularly strict rules around data localisation, with requirements for certain kinds of personal data to be stored in servers located in India – a move which has gathered criticism from sources such as the US-based global tech lobby Information Technology Industry Council

Another notable feature of the bill is the plan to rate organisations on their compliance with the legislation using a data trust score. This approach has seen increasing use around the world as a tool for establishing trust around cyber security, functioning

in a similar manner to a credit score to help businesses ensure partners are reliable. The proposed bill will also apply this concept to consumers, making it easier for Indian citizens to determine if a company can be trusted to safeguard their information.

The global data landscape has become far more complicated in the last few years and will only become more complex as major legislation in the US, India and elsewhere around the world comes into effect. With so many different standards to adhere to, operating a global business that involves the data of international citizens may be an increasingly daunting prospect.

The good news is the landscape is not the minefield it appears to be at first glance. Although organisations will need to pay close attention to new regulations as they come into law, the majority of current and future data protection laws revolve around the same core concepts of transparency and due diligence. While there may be some peculiarities in certain territories, for the most part any organisation that has gained a high level of oversight of its data will be able to operate with few issues.

Keeping pace with the changing tides of data regulation will require increased administrative activity, particularly when it comes to auditing. Businesses must ensure they have an accurate, up-to-date view of their current compliance and risk levels, which they are able to report to the board, stakeholders, any regulatory bodies and individual citizens exercising their rights.

Implementing a continuous compliance program is one of the most effective ways to achieve this without a cripplingly expensive investment in new infrastructure. This will involve implementing policies, procedures, best practices, measurement and oversight for both internal operations and third parties, with key points including:

Implementing common controls such as web application, endpoint and network security to mitigate the risk of a breach.

Designating responsibilities to specific individuals and departments, with clear ownership of data protection tasks.

Ensuring best practice is followed across the organisation for factors including settings, programme configurations and dealing with third-party vendors.

Establishing clear communication and approval for policies for all stakeholders. These should not just be internally focussed, but should also highlight what external policies, laws and regulations the organisation needs to comply with to ensure all bases are covered.

Implementing the ability to measure the success and maturity of data protection activity. This can be achieved through setting baselines and key performance indicators and regularly testing the programme against them.

The organisation must be able to detect any anomalies that might indicate risk and mitigate them effectively. Likewise, it must be able to detect and respond to external factors including legal changes or issues stemming from third parties.

One of the most important steps to achieving continuous compliance is automation. Tying all of these disparate activities together through automated, continuous control monitoring will help to provide a unified view that will reduce the chances of potential risks being overlooked and will minimise the risk of human error. This level of oversight will make it much easier for an organisation to be confident that it is compliant in any given region. In addition, automating as much as possible will ensure compliance is more efficient and less costly.

By achieving a high level control over data based on proper planning, policies and procedures, backed with the right technologies, organisations will not only be able to keep pace with shifting compliance demands, but will be able to confidently operate and expand around the world even as the landscape continues to change.

Fouad Khalil is VP of Compliance at SecurityScorecard and has over 25 years of experience spanning disciplines in software development, IT support, program and project management, and IT security and compliance management.

Ute con corum quo comnis ad es remquasperum is res sit et diatiusam voluptatem repratu