Navigating the regulatory landscape: How compliance can protect your business from data breaches

Compliance with regulatory requirements is fundamental to protecting businesses from data breaches. Understanding and adhering to those requirements means putting processes in place, from staff education to using the right tools to fight fraudsters. Doing so can help businesses keep their data safe and avoid reputational damage and hefty fines.

Temps de lecture : minute

---

10 May 2023

Why is regulatory compliance important?

Compliance is important because regulators' requirements are designed to keep data safe, based on international examples of best practice and with full awareness of the latest threats from around the globe. By complying, businesses can help avoid the reputational damage and loss of customer trust that results from a data breach.

Businesses can also protect each other through regulatory compliance. After all, if one company's data is breached, that data can then be used for *credential stuffing* attacks on other businesses, with fraudsters using leaked or stolen databases of login credentials to try and gain access. The more companies keep their data safe through compliance, the fewer opportunities they give to fraudsters.

Regulatory compliance is also essential for businesses that want to avoid eye-watering fines. British Airways' breach of the General Data Protection Regulation (GDPR) led to the UK Information Commissioner's Office (ICO) announcing it would be fining the airline *£183.39M* in July 2019. While that sum was ultimately whittled down to a fine of £20M by October 2020, it was still the largest fine the ICO had issued under the GDPR.

That said, the British Airways fine felt like pocket change in comparison to the fine that the Cyberspace Administration of China (CAC) issued to ride-hailing conglomerate Didi in July 2022. The CAC fined Didi *¥8.026B*, equating to approximately $1.18B, for breaches of cybersecurity and data laws.

What are the key pieces of legislation that businesses need to comply with?

Regulatory compliance requirements depend not just on where a business is based but also where its customers reside. This is a key consideration for companies that are entering new markets. *Breaking into the US*, for example, means understanding the regulatory landscape there. Instead of one overarching piece of data protection legislation, the issue is dealt with by hundreds of laws, some at federal level and others at state level. One of the most well-known of these is the California Consumer Privacy Act, which is seen by many states as the gold standard of data protection legislation.

Over in Europe, meanwhile, the situation is much clearer for businesses, thanks to the introduction of the GDPR. The regulation requires compliance by any business that collects or processes the personal data of European Union (EU) residents, regardless of where that business is based. This has effectively standardised compliance requirements not just for businesses in Europe but for companies based all over the world that have customers in the EU.

Other significant pieces of data protection legislation exist all over the globe, from the Lei Geral de Proteção de Dados (General Data Protection Law) in Brazil to China's Cybersecurity Law.

How compliance can protect your business – practical tips

Compliance with data protection regulations can protect your business from data breaches in multiple ways. The first is that compliance requires that your staff are knowledgeable about how to keep company data safe. This means you need to implement training for your teams, to ensure that everyone is aware of the company's obligations and how they can help. Any member of staff could fall victim to a phishing scam. Some *3.4 billion spam emails* are sent out every day, with phishing by far the most common type of cybercrime. This is why your business needs to train every member of staff as part of its compliance work.

Policies and procedures also have a major role to play in protecting your business. These provide you with the opportunity to clearly state expectations in terms of data security and to define processes for everything from issuing invoices to setting up new supplier accounts. By training your staff to follow these procedures to the letter, you can reduce opportunities for potential data breaches as much as possible.

Using the right tools is also key. There is a wide range of cybersecurity solutions on the market, which can assist with keeping customer data secure in multiple ways. Not only can the right tools help keep data secure in the first place, they can also help to reduce the length of the breach lifecycle and reduce financial losses.

Of course, data protection is just one area of compliance, and crossing regulators can be a costly business in many areas (as Fiat Chrysler found out when it *fell afoul of the Securities and Exchange Commission* in the

US). As such, it is essential for any business to gain an in-depth understanding of *all* of its compliance obligations and to put robust processes in place to ensure that compliance. Having an appointed person to lead on compliance matters is essential, as is having access to specialist advice on regulatory requirements.

Finally, it is important that businesses regularly test the systems and procedures they have put in place in order to ensure compliance. Personnel changes, staff holidays and all sorts of other routine business matters can move the spotlight off compliance, in which case it's easy for standards to slip. Testing the processes and systems can highlight any flaws and enable the business to take remedial action where needed.

By following these tips, companies can ensure they are doing all they can to protect themselves from data breaches, keeping their customers safe, protecting their reputations and minimizing their chance of fines through rigorous regulatory compliance.

Eva Kozar is a S~enior Account Executive at *SEON*.

Article by Eva Kozar