Information Regulator shows its teeth with first PoPI fine and businesses must take note

By Lizaan Lewis

17 Nov 2023

After many years of hearing about the Protection of Personal Information (PoPI) Act and the effect it would have on businesses in terms of their responsibility to protect personal data, businesses have finally seen the warning shot fired by the Information Regulator - "Get your house in order or you could easily be next to fall foul of PoPI and pay a fine, suffer reputational damage, and even possible criminal liability."

Lizaan Lewis, head of legal, Altron Systems Integration

The Information Regulator dishing out a R5m fine to the Department of Justice and Constitutional Development ("Department") should cause pause for thought for all businesses that process personal information. Fines can go up to R10m and there can even be jail time if it is found that there was malicious intent leading to a data breach.

In this instance, the Department was fined over a data breach that occurred about two years ago. Despite receiving an enforcement order, the Department did not comply, leading to the country's first fine under the PoPI Act. Perhaps the lesson in this is how easily this could have been averted, as it was found that the Department had not renewed licences for cyber security software - something seemingly so simple but which proved to open the door to the hackers.

Data breaches: The high cost of neglect

The obligation in the event of a data breach is to prove that you did everything in your power to prevent the data breach. In other words, the Information Regulator needs a business to prove that it had put in its best effort to prevent a breach of personal data, and in the case of the Department, it was required to demonstrate the steps it had taken to rectify the problems. Not renewing licences for cyber security software may seem small, but the consequences can be huge.

There absolutely have to be contingencies in place for businesses of all sizes. For example, a monitoring tool may not necessarily give you protection, but it will point you to where there is unusual activity, which could be the site of a data breach. The Information Regulator has been informed of thousands upon thousands of data breaches and so this fine is most certainly a warning shot for businesses across industries.

In the modern digital world, cross-border movement of data is not unusual, and the European Regulator has issued very big fines to household names for flouting obligations related to the General Data Protection Regulation (GDPR). Factoring in exchange rates a fine from that body would be difficult for any organisation to stomach.

Essential cybersecurity steps: Prioritise protection and expertise

As an absolute starting point, businesses should ensure all their software licences are up to date. Just because they don't see it affecting their business does not mean it shouldn't be a priority. It's important to understand that you need the correct software for your type of business, because not all firewalls or virus protection software are identical, and some are not suitable for certain types of organisations. This means that there must be a proper assessment of a business's environment so that it can know exactly what protection is needed.

It may be easy to simply use Google to find tools, but these may not be right for certain environments and may require specialised skills to use. The prudent thing to do would be to engage with industry experts who can immerse themselves into an environment and advise on exactly what the business needs, from systems to processes and tools.

In the event of a data breach, a business needs to have peace of mind that not only can it recover important data and continue its operations, but it must also be confident that it can prove to the Information Regulator that it did everything reasonably possible to prevent a data breach, while also having the capability and skills to mitigate against future attacks. Failing to do this turns a business into a sitting duck in an environment where the Information Regulator has shown its teeth.

ABOUT THE AUTHOR

Lizaan Lewis, Head of Legal, Altron Systems Integration.