ITProPortal

Three IT steps to make your GDPR compliance journey smoother

Businesses are constantly having to overcome the various obstacles that come their way — some might argue this is a large part of how success is defined. But the deadline for General Data Protection Regulation (GDPR) compliance is a considerable and unavoidable hurdle, and one that all businesses should be thinking about now before it is too late. T

here is no denying that the journey to GDPR compliance is complicated, with business having to re-evaluate the way they deal with data and approach the issue of privacy, among numerous other areas. A good place for any business to start is to review what the Information Commissioner's Office (ICO) recommends, and their '12 steps towards GDPR compliance' paper is particularly useful. There are also many other briefings and webinars on offer that are designed to answer any GDPR-related questions businesses might have.

While these are a great way of making high-level decisions, the role of the IT department in achieving GDPR compliance should not be underestimated. Their

Understanding the data that you hold

Businesses need to document the personally identifiable data (PII) that they hold, where it came from and who they share it with. Most businesses are approaching this task with trepidation as the number of files that a business holds can be in the millions (typically over five million for a business with 100 users).

However, there are products on the market that will help make this task easier – look for 'GDPR automated data discovery' and 'GDPR analysis' tools. These will scan your network and identify any files that contain PII – names, email addresses, IP addresses etc. — and report back to you with the file location and the PII that it has found. This then helps to shape the starting point for the reviews that you need to undertake to achieve compliance, and the scans can be run periodically to ensure that the business remains compliant.

Locating the data

Although subject access requests were already part of the existing Data Protection Act, now that they cannot be charged for, businesses need to be prepared to handle a greater number of these – whether from customers or from staff (both ex- and existing). It is very important that these requests are handled within the prescribed timescale and deliver the relevant information to the requestor.

As well as the previously mentioned scanning tools that can help organisations locate the desired information – both for subject access requests and right to be forgotten requests — there are also various business process tools available that can help to manage these requests more efficiently and effectively.

Businesses have always needed to ensure they're able to restore corporate data in the event of a cyber attack, and one of the most popular ways to do this is through regular system backups (alongside implementing a robust disaster recovery solution). However, this often means businesses are left with multiple copies of the same files. If you consider how the majority of businesses often perform these backups — i.e. using a grandfather, father, son methodology — it is therefore more than likely that a single file could exist in ten or more locations, with even more versions potentially lying undiscovered. Add to this the fact that businesses themselves often structure their data around their clients and internal departments, and that large copies of data are often kept after system upgrades 'just in case', and you start to fully understand just how widespread this problem might be. This is why using these tools to locate data is so vital.

Keeping the data safe

GDPR places an obligation on all businesses to detect, report and investigate personal data breaches, which are becoming more and more commonplace. 2017 alone was riddled with worrying stories of serious hacks on major businesses and organisations including the NHS, Uber and the Houses of Parliament, and this has led the majority of us to look inward at our own businesses and question whether we're taking the issue seriously enough.

However, the IT department of a business can play a key role in preventing these breaches happening in the first place.

Data lies at the heart of GDPR, and so every possible effort should be made to protect any personally identifiable data your business holds. However, this can prove problematic — especially considering that IT infrastructures are so susceptible to vulnerabilities.

The stark truth is that there will be very few businesses who are sufficiently protected from the threat of cyber attacks, and so they must work on bolstering their defences if they are to stay out of the firing line. This involves looking at every aspect of a business' IT infrastructure, from security features of the hardware itself to ensuring that all confidential corporate data is protected from data breaches.

One of the most popular ways of plugging this gap is to introduce security solutions, such as vulnerability management tools, that can scan your IT infrastructure and identify known security vulnerabilities — the IT function will then upgrade operating systems and apply patches to fix these, therefore minimising the chances of a data breach. Alternatively, there are numerous regulation management tools that can ensure compliance across an entire company rather than just a single team or department.

Conclusion

As the deadline for GDPR compliance gets ever closer with each passing day, businesses seem to be firmly divided into two camps. While half of us struggle to wrap our heads around what exactly is required to operate safely in a post-GDPR era, the rest of us are finding rocks to hide under in the hope that the storm passes and leaves us unharmed.

Link to the original article:
https://www.itproportal.com/features/three-it-steps-to-make-your-gdpr-compliance-journey-smoother/