

# Don't be caught short with corporate governance and GDPR compliance

By [Stuart Scanlon](#)

14 Nov 2018

As implementation of new EU General Data Protection Regulations continues, many South African companies are finding themselves unprepared and likely to face stiff penalties if they don't seek compliance as a matter of urgency.



Protection of personal information has been thrust squarely into the spotlight in recent years, spearheaded by the recent [Facebook Cambridge Analytica](#) scandal where a third party app scraped millions of users' data, allegedly to influence the outcome of the 2016 US election. While local laws such as PoPI exist, the EU is taking a far more aggressive stance on just how much control citizens have over their personal data – specifically regarding sensitive subjects such as race, ethnicity, gender, bio-data, sexual orientation, and political and religious opinions – which cannot be handled without explicit consent. Companies must also delete information about a contact as and when requested. The regulations stipulate that it must be as easy for someone to withdraw their consent as it was to grant it. This has been termed “The Right to be Forgotten”.

According to the regulation, individuals have the right to:

- Be informed
- Be forgotten
- Rectification
- Object
- Portability

In the case of a security breach, which poses a high risk for an individual's rights, the controller must contact and inform them. If the person requires more details about the breach, this information must be conveyed in an easy and understandable language.

Even if a company is not based in the EU, it must adhere to these regulations if it holds data belonging to EU citizens. This is where many South African companies are getting caught short. If found to be in breach, they could be fined by the UK's Information Commissioner's Office (ICO) up to 2% of their global turnover or up to €20 million (R326 million), which is a significant amount.

So what can local businesses do to navigate the somewhat daunting road to compliance? There are options available, such as epic ERP, which consolidates multiple data pools into a system that prioritises security, easy auditing and strict data access management, along with traceability and the use of accredited, certified data centres. When it comes to compliance, it pays to treat users' data as seriously as the new regulations demand. And it is time for a renewed focus on effective, ethical corporate governance.

Far from being a reason to panic, the UK Direct Marketing Association sees this evolution as an opportunity for businesses to transform the way they see people, and how they interact with prospects and consumers. In their words: "Businesses should seize upon GDPR as the catalyst to transform their businesses into human-centric ones. They should use the GDPR framework as the foundation for an authentic and transparent relationship with their customers." By streamlining, refining and focusing on improved data governance, the benefits of more effective data-driven marketing can certainly outweigh the effort required to be compliant.

## ABOUT THE AUTHOR

Stuart Scanlon is the managing director of epic ERP - a leading ERP planning software systems specialist.

For more, visit: <https://www.bizcommunity.com>