Five steps to managing GDPR compliance

By Obed Lesejane

1 Mar 2018

South African businesses should care as much about the European Union's General Data Protection Regulation (GDPR) as they do about the Protection of Personal Information (POPI) Act.

© everythingpossible via 123RF

Even though local businesses might not deal with customers or staff in Europe today, there's a good chance they might in future, thanks to the hyper-connected world we live and work in.

> *"It makes sense, then, for businesses to start preparing their systems and processes for compliance, ahead of the 25 May 2018 deadline. And the biggest motivator should be the penalties for non-compliance – up to €20 million or 4% of annual global revenue. Losing this amount of money could force most businesses into liquidity issues."*

Good enough?

Yet, recent SAS research found that a massive 98% of organisations experience challenges in complying with GDPR and 20% of respondents don't know if the actions they've taken to comply are sufficient.

Ultimately, compliance will depend on how well your business processes are organised and structured. The GDPR and POPI will force you to change the way you store and process personal information and also how you run and manage data projects.

GDPR: What it means for data management

Kerry Hope 14 Dec 2017

Five steps to success

Implementing the GDPR will affect your entire organisation. You'll need to go back to the drawing board and rethink how personal data is handled, from the source to the point of consumption. You'll also need to consider how your data management and data governance frameworks will support GDPR requirements.

While it may sound overwhelming, our five-step approach can make the path to GDPR compliance easier to manage.

Step 1: Access

You need to be able to prove that you know where personal data is stored. To do this, you need to be able to access all your data sources.

No matter what technology you use, you need to investigate and audit what personal data is being used and stored within your organisation.

Seamless access to all data sources is a prerequisite for building an inventory of personal data so you can evaluate your privacy risk exposure and enforce enterprise-wide privacy rules.

Step 2: Identify

Once you've accessed all your data sources, you need to identify personal data that can be found in each source. You need to be able to extract, categorise and catalogue personal data elements from semi-structured fields.

PoPI requires effective data management structures

Claude Schuck 31 Oct 2017

Because there is so much data available, and because you need to accommodate varying levels of data quality, this cannot be a manual process.

Things like pattern recognition, data quality rules and standardisation are vital elements of this process, so you need the right tools for the job.

Step 3: Govern

Everyone in your organisation must be able to define personal data. The GDPR requires that privacy rules be documented and shared across all lines of business and that organisations enforce rules to ensure that only those with proper rights can access data.

To achieve this, roles and definitions must be established in a governance model. You can then link business terms to physical data sources and establish data lineage from the point of creation to the point of consumption. This provides you with the required level of control.

Step 4: Protect

Once you've established the personal data inventory and governance model, it's time to set up the correct level of data protection.

You can use three techniques to protect data:

- Anonymisation, which removes personally identifiable information from data.
- Pseudonymisation, which replaces personally identifiable information in data.
- Encryption, which encodes personally identifiable information in data.

You will need to apply the appropriate technique based on the user's rights and the usage context – without compromising your growing needs for analysis, forecasting, querying and reporting.

The easiest way to protect data privacy is to press the delete button, keeping only the data you need to run critical business processes and added-value analysis.

Step 5: Audit

Another vital element of GDPR is auditing.

At this stage, the regulator will ask you to prove that you:

- Know what personal data you have and where it's located, across your data landscape.
- Properly manage the process for getting consent from individuals who are involved.
- Track and document how personal data is used, who uses it, and for what purpose.
- Have the appropriate processes in place to manage the right to be forgotten, data breach notifications and more.

While non-compliance with GDPR could be a real threat to the future of many organisations, the upside is that personal data has tremendous value and can create significant competitive advantage if it's managed properly. I can't think of a better reason to comply.

ABOUT THE AUTHOR

Obed Lesejane, senior solutions manager: data management, SAS South Africa.