How African businesses can comply with new EU data laws

The European Union's General Data Protection Regulation (GDPR) comes into force on 25 May 2018. African businesses that collect, process or store personal data about European citizens and residents will need to comp

By Pieter Bensch 9 May 2018

© Benjamin Haas via 123RF

That's the case even if they don't have a direct presence on the continent; even more so if they are Small & Medium Businesses.

The GDPR sets out the minimum requirements for the treatment of all personal data. Personal data can be defined as any data identifying or relating to an individual, including things like physical appearance, biometric data, an individual's recor on a customer relationship management system, or even something as simple as website tracking data collected via cooki

> ***GDPR is one of the biggest shake-ups ever seen affecting how data relating to an individual should be handled - and many African organisations are not yet ready.***

Here are six practical steps your African business can take to ensure that it complies with Europe's stringent new data privacy and protection regulation:

1. Get informed

The first step towards complying with the GDPR is to understand the new demands the regulation places on how your business collects, manages and stores the personal data of European citizens and residents. There is a wealth of informat available online; a good starting point is the EU GDPR Portal.

Many law firms and IT consulting groups in Africa have also been studying the GDPR. They will be able advise you on the practical aspects of compliance as well as how the GDRP will interact with the data privacy and protection laws and regulations in place in your own country, for example, the Protection of Personal Information Act (POPI) in South Africa.

2. Do an audit

The GDPR is an opportunity to evaluate why you collect and store personal data, as well as the data you are already holdi in your databases. You will need to know this so that you can explain to European individuals which data of theirs you are collecting as well as how you use it. If you find that you are gathering data for which you have no real business need, dele it.

This will help you reduce your exposure to risk, as well as show a commitment to responsible usage of your customers' da

Also look at how long you retain data for, as well as how you store and secure it. You might consider a GDPR audit from legal and technological standpoints. Only once you understand what you are doing today, can you start to revamp your systems and processes to align them with GDPR.

Some other important points to consider:

- Do you have processes in place to enable people to move, copy or transfer their personal data from your organisatic to another, as it is their right under GDPR?
- Do your processes live up the GDPR's expectation of 'privacy from start to finish' i.e. from first contact with your company to the end of the relationship?
- Do you have a process in place to tell regulators and customers of a breach within 72 hours of becoming aware of it
- Are your business partners and suppliers with access to your data about European users aware of the requirements GDPR?
- Can you prove your compliance with GDPR if necessary?

3. Review your consent mechanisms

EU data protection legislation has always required that customers must give specific and informed consent to organisation that gather their data. GDPR takes this a step further by demanding that customers give their consent with a statement or other clear affirmative action. If you are still treating silence as consent, or using pre-ticked consent boxes on your websit you will need to review your processes.

CLOUD

Pieter Bensch appointed Sage executive VP Africa, Middle East

20 Sep 2017

4. Refresh your privacy policies and contracts

You will need to update your privacy notices to provide the additional information required by the GDPR, and you may we need to relook the portions of any contracts with EU residents and citizens that deal with their data rights.

5. Train your extended workforce

Ensure your employees and partners are aware of the GDPR and secure training to prepare them. Remember the GDPR makes you responsible for third parties who process personal data for you.

6. Appoint your Data Protection Officer

According to the GDPR, organisations processing large amounts of personal information or particularly sensitive personal information should have a data protection officer (DPO). The DPO needs to have expert knowledge of data protection law he or she could be an employee or a service provider. Laws like POPI in South Africa also expect companies to have an information officer - it makes sense for the same person to hold both roles.

GDPR is one of the biggest shake-ups ever seen affecting how data relating to an individual should be handled - and many African organisations that process the personal data of individuals who are based in the EU are not yet ready for it. Time i

running out for them to get their houses in order and there are serious implications if you are a business not taking this seriously.

ABOUT THE AUTHOR

Pieter Bensch is executive vice president, Africa & Middle East: Sage.