EU GDPR Article for Africa Cyber Security Report 2017 – 18

Article title: Love it or hate the GDPR is here to stay

Article submitted by Dr Peter Tobin, BDO IT Consulting Ltd, Mauritius

Historical context for the GDPR

Global recognition of the importance of data privacy can be traced back to the United Nations (UN) which has a long history of promoting the right to privacy through its Human Rights treaties. This includes article 12 of the Universal Declaration of Human Rights in 1948 and article 17 of the International Covenant on Civil and Political Rights in 1966. More recently in July 2015 the UN appointed a "Special Rapporteur on the right to privacy" to bring additional focus to the importance of data privacy. Supporting the UN is the Organisation for Economic Co-operation and Development (OECD) which in 1980 issued its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" which were revised and re-issued in 2013, just as the POPI Act (POPIA) was gazetted in South Africa, allowing that country to join the growing list of those forming part of the African community of nations that have embraced personal data protection legislation. Following the UN and OECD initiatives, nearly one hundred countries and territories have established or are developing data protection laws.

African personal data privacy and protection developments

In Africa, the African Union (AU) Commission and the Economic Commission for Africa have spearheaded the development of the AU Convention on Cybersecurity and Personal Data Protection, which was adopted by the AU Heads of States and Governments Summit in June 2014 in Malabo, Equatorial Guinea. Eight Countries had already signed the convention by July 2016 according to AU Commission: Benin, Chad, Congo, Guinea Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia. At a regional level in Africa there are also several initiatives, notably the ECOWAS Cybersecurity guidelines and the SADC Model Law on data protection, e-transactions and cybercrime. There is also the HIPSSA initiative (Harmonization of the ICT Policies in Sub-Saharan Africa) which covers 30 countries across the continent. Latest estimates show that 16 African countries have data privacy legislation, with an additional 14 countries working on legislation, leaving a balance of 24 currently having taken no action so far. There are some leading examples in Africa, such as Mauritius which passed the Mauritius Data Protection Act (MDPA) in late 2017, swiftly brought the MDPA into full force in January 2018 and thus positioned itself as a leading nation in Africa and the Indian ocean island states in terms of alignment with the European Union and its General Data Protection Regulation (GDPR).

So what is the European Union GDPR?

During 2016 the General Data Protection Regulation – commonly known as the GDPR – was finalised, with a transition period to full compliance required by those organisations impacted - those processing directly (controllers) or indirectly (processors) the personal data or EU residents - by May 2018. The GDPR has potentially wide-ranging implications for companies based outside the EU (increasingly often in Africa) trading with the EU member states. Of particular interest is the following extract from the GDPR document: "The [European] Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision." This opens the door to leading practice nations and sectors stealing a march over their competitors in the global marketplace for information services provision where personal data is processed.

So what, briefly, is the GDPR (www.eugdpr.org)? The GDPR is a single regulation that automatically applies to all current and future European Union members states from May 2018. In the case of the United Kingdom (UK), there were strong indications at the time of writing this article that the UK would fully align itself with the GDPR even post "BREXIT" (the exit of the UK from the EU). The GDPR has 173 introductory clauses (sometimes referred to as the recitals, a form of explanatory pre-amble), with the main regulation body comprising 11 chapters made up of 99 Articles which come to over 400 numbered paragraphs. It is important to remember that the GDPR works in conjunction with other EU directives and regulations at an EU level, and may be complemented by local legislation, whether in EU member states or in African countries that are seeking to align themselves to the GDPR.

After chapter 1 which contains a series of general provisions and definitions, chapter 2 covers the principles of data processing, which have been refined since the previous EU personal data protection directive of 1995. Chapter 3 addresses the "Rights of the Data Subject", those EU-resident individuals whose personal data may be processed by one of more the main parties who need to comply with the GDPR: the Controller (typically an organisation such as a business or arm of government) that determines and controls the processing of the personal data and the Processor, a service provider which renders personal data processing services to one or more Controllers. There are other Third Parties that may be involved, such as those organisations where the Controller shares personal data for a variety of legitimate reasons. Chapter 4 looks at the duties of the Controller and Processor.

Chapter 5 addresses the Transfer of Personal Data to 3rd Countries or International Organizations, an important consideration when dealing with countries in Africa that, for example, host outsourced personal data processing services for EU-based Controllers. Some of the chapters of the GDPR are really only of interest to the supervisory and regulatory authorities (such as chapters 6, 7, 10 and 11), whilst others discuss important issues such as remedies, liability and penalties (Chapter 8) which can have serious consequences for Controllers or Processors who do not meet the requirements of the GDPR.

Key changes in the GDPR

Compared to the earlier EU-wide directive of 1995, the GDPR contains a number of key changes. These include the increased territorial scope of the GDPR (extra-territorial or non-EU member state applicability; significant increases in potential penalties (rising to up to 2% to 4% of global turnover of either or both of the Controller or Processor found at fault by the supervisory authorities). There have also been changes to the nature of consent which can be used as a justification of lawful processing, including expanded requirements in terms of the record keeping for consent given, refused or withdrawn. Whilst some countries have already implemented strict rules around data breach notification, the GDPR emphasises to requirement to normally notify the supervisory authorities within 72 hours of a data breach being confirmed (perhaps after an initial check that the data breach is real and not imagined or only suspected). Data subject rights have also been clarified and expanded to include the much-discussed "right to be forgotten" (erasure of personal data) as well as the right to data portability, such as when moving between service providers. "Privacy by design and default" also represents not only a new requirement but one which addresses the approach to personal data privacy as "built-in" not just "added-on". The last major change highlighted by the EU is the enhanced and expanded (broader and deeper) role of the Data Protection Officer (DPO).

Beyond the vanilla GDPR

It is important to be aware that the GDPR in its basic format has already been complemented by a number publications by the group that will over time become the collective body for supervisory authorities in the EU (European Data Protection Board, established under Article 68 of the GDPR), although operating at the time of writing under the "Article 29 DPWP" branding (perhaps somewhat confusingly, that's Article 29 under the 1995 directive and not under the GDPR). Further guidance is already planned in areas such as consent, transparency, profiling, high risk processing, certification, administrative fines, breach notification and data transfers.

So how is your compliance status?

Here's a quick review of some of the key considerations when preparing for (or maintaining) compliance with the GDPR. Can you prove that:

1. You comply with the 6 principles relating to personal data processing? (Article 5: Principles relating to personal data processing)
2. You comply with the lawfulness of processing rules? (Article 6: Lawfulness of processing)
3. You have records of consent that meet the required conditions? (Article 7: Conditions for consent)
4. You have provided all necessary information at point of collection? (Article 13: Information to be provided)
5. You have a policy, process and procedures to ensure a) right of access; b) to rectification; c) to erasure; d) to restriction of processing; by the data subject? (Article 15 - 18: Right of access; to rectification; to erasure; to restriction of processing)
6. You are meeting all the responsibilities of the controller? (Article 24: Responsibility of the controller)
7. You have data protection by design and by default? (Article 25: Data protection by design and by default)
8. You have a representative in the EU? (Article 27: Representatives of controllers not established in the Union)
9. You have adequate records of processing? (Article 30: Records of processing activities)
10. You have adequate security of processing? (Article 32: Security of processing)
11. You have a policy, process and procedures for data breach notification to the supervisory authority? (Article 33: Notification of a personal data breach to the supervisory authority)
12. You have a policy, process and procedures for data breach notification to the data subject? (Article 34: Communication of a personal data breach to the data subject)
13. You have conducted data protection impact assessments where necessary according to the screening rules? (Article 35: Data protection impact assessment)
14. You have, where necessary, appointed an appropriate data protection officer following the EU requirements? (Article 39: Tasks of the data protection officer)
15. You have appropriate safeguards for cross-border transfers? (Article 46: Transfers subject to appropriate safeguards)
16. You have trained your staff in all of the above aspects and more (Article 39: Tasks of the data protection officer)

So maybe you didn't score full marks and are beginning to hate the idea of all the effort it might take to climb the GDPR mountain if you need to. But perhaps it's also time to look on the bright side, and learn to love the GDPR. It might just be that the next big contract you land with a client in Europe or service work you perform for an organisation outside the EU but with clients in the EU, provides the bonus you have been promising yourself all year. One way or the other, love it or hate it, the GDPR is here to stay.