mimecast | FAQ

POPIA vs GDPR – What you need to know

The European Union's General Data Protection Regulation (GDPR) and South Africa's Protection of Personal Information Act (POPIA) are two sets of legislation for residents of the European Union and South Africa respectively. They are designed to enhance personal privacy rights, place greater duty on organisations to protect data, institute mandatory disclosure of data breaches involving personal data, and introduce significant penalties for non-compliance.

What do GDPR and POPIA have in common?

Key concepts common to GDPR and POPIA include:

Personal Data	Both GDPR and POPIA regulate the collection, storage, use and sharing of personal data, which is defined as any data that relates to an identified or identifiable natural person. However, POPIA also includes a non-juristic person, such as a company, trust or partnership.
Data Subject	An individual (or juristic person, in the case of POPIA) about whom the personal data being processed relates.
Data Controller/ Responsible Party	The entity or organisation that receives the personal data and provides the services. In both the case of POPIA and GDPR, the Data Controller/ Responsible Party is liable for the data.
Data Processor/ Operator	A service provider engaged by the Data Controller/Responsible Party that helps to deliver the service, such as a cloud provider. In both the case of POPIA and GDPR, the Data Processor/Operator is liable for the personal data during the time it is processing such data.

Similarities and differences between GDPR and POPIA

	POPIA	GDPR
Right to Be Informed	Yes – Section 18	Yes – Condition 6
Right to Access	Yes – Section 23	Yes – Condition 8
Right to Rectification and Erasure	Yes – Section 23	Yes – Chapter 3 Section 3
Right to Restrict Data Processing	Yes – Section 14(6) allows a data subject to contest the accuracy or objects to the processing of personal data	Yes – data subjects can contest the accuracy or object to the processing of personal data
Right to Portability	No	Yes – users can obtain and reuse their own data
Right to Object	Partial – Section 68 refers to direct marketing only	Yes – data used for direct marketing, research or public interest
Automated Decision-making and Profiling	Yes – Section 71 provides safeguards against decision-making without any human intervention	Yes - provides safeguards against decision-making without any human intervention
Privacy Impact Assessments	No	Yes
Applicability	Natural and juristic persons, South Africa only	Natural persons only, extra-territorial
Fines	Up to R10-million or 10 years' imprisonment	Up to €20-million or 4% of total global turnover

Conclusion

The General Data Protection Regulation and Protection of Personal Information Act both aim to give more control to citizens over their personal data. Both sets of regulations place significant additional pressure on organisations to implement appropriate controls to monitor, protect and regulate the processing and flow of personal information within and outside organisations to ensure the legitimate use of personal data.

Technology plays a pivotal role in supporting organisations in their compliance efforts, by improving security, improving how data is stored and processed, and ensuring organisations can respond quickly and accurately to requests from individuals and organisations regarding their personal data.

For more information about how Mimecast can support organisations with their compliance efforts, please visit www.mimecast.com.