POPIA – What Do You Need to Know?

SHL.

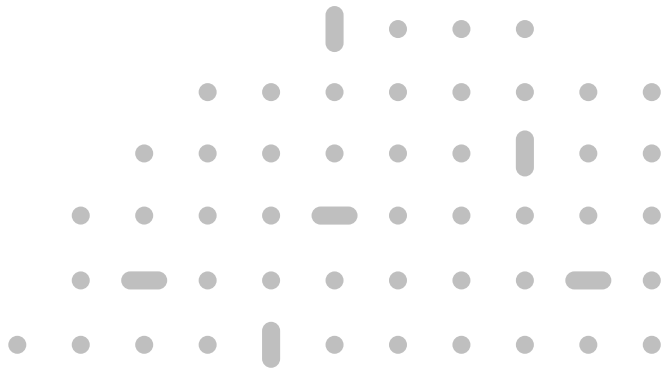
1 Introduction

As the leading global provider of Talent Assessment solutions, we take our obligations to ensure the highest level of protection over the personal data you entrust to us very seriously. Maintaining compliance with applicable data protection legislation continues to be a core business priority.

South Africa's POPIA is the most recent major data privacy law in the world to be modelled closely after GDPR. The European Union's General Data Protection Regulation (EU) 2016/679)('GDPR') came into effect on 25 May 2018.GDPR is not just a European data privacy law, it is considered the word's highest standard on data privacy.

This statement provides you information regarding our compliance with, and our programs to support your compliance with POPIA, South Africa's data protection law. Protection of Personal Information Act, 4 of 2013 **("POPIA")** gives substantive content to the constitutional right to privacy by establishing a threshold of minimum conditions for the processing of personal information and providing individuals with rights and remedies to protect their personal information.The President of South Africa signed POPIA into law on 19 November 2013. Certain provisions in POPIA came into effect (the provisions relating to the establishment of the office of the Information Regulator and provisions relating to the issuing of regulations) on 26 November 2016. The majority of the remaining provisions in POPIA came into effect by Presidential declaration on 1 July 2020.

In our role as data processor we have a demonstrated track record of data security and sound practices. We are committed to being POPIA compliant, as further detailed in Section 3 and are on a continuous improvement journey.

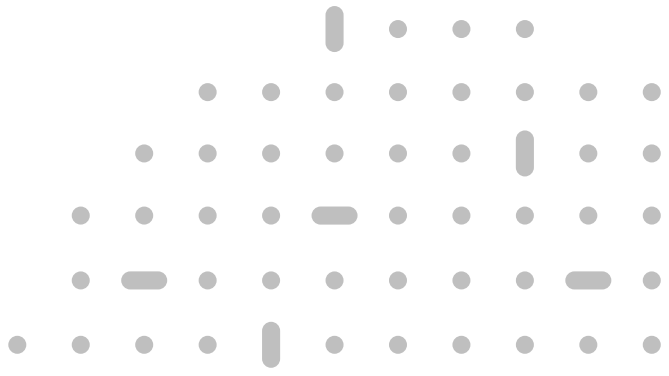


2 What Is POPIA and What Does It Mean for You?

Section 114(1) of POPIA states that all processing (as defined in POPIA) of personal information must, within one year of the commencement of section 114(1), be made to conform to POPIA. This means that parties who process personal information will have a 12-month grace period (or such longer period as may be determined by the President) from the commencement of section 114(1) of POPIA to comply with the requirements and obligations in POPIA. Section 114(1) came into force on 1 July 2020, which means that the **12-month grace period has commenced and is due to expire on 30 June 2021. Enforcement will officially begin on July 1, 2021.**

POPIA is a significant change to the South Africa data protection framework and introduces several key changes that impact our services and our clients:

- **Accountability:** POPIA introduces eight conditions for lawful processing of personal data as a minimum standard for compliance with the POPIA principles.
- **Enforceable Rights:** POPIA empowers citzens with enforceable rights over their personal information (rights of access, rectification, to object to data processing and to restrict processing) for each data subject.
- **Governance framework:** Intertwined with the accountability principle, is the requirement on responsible party and the operator to implement appropriate technical and organisational measures and to demonstrate any processing of personal data is in compliance with POPIA.
- **Sanctions:** Breach of POPIA may give rise to a range of sanctions, including civil remedies and criminal offences. A responsible party alleged to have committed an offence under POPIA may be liable for an administrative fine, not to exceed 10 Million ZAR (South Africa Rand) or imprisonment not exceeding 10 years.
- **Territorial Scope:** POPIA applies to any company or organization processing personal information in South Africa, who is domiciled in the country, or not domiciled but making use of automated or non-automated means of processing in the country. POPIA does not have extra- territorial application as contemplated under the GDPR.



3 Why Choose SHL

We prioritise data security:
We understand and have always taken our security obligations seriously, long before the GDPR. Our commitment to security is demonstrated by our on-going certification programs that have been in place for many years. In particular, we have developed and implemented an ISO 27001 certified Information Security Management System for over 10 years running. Additionally, we have obtained ISO 22301 certification for our Business Continuity Practices and we have ISO 20000 certifications for our ability to professionally maintain, support and manage our IT services using best practices.

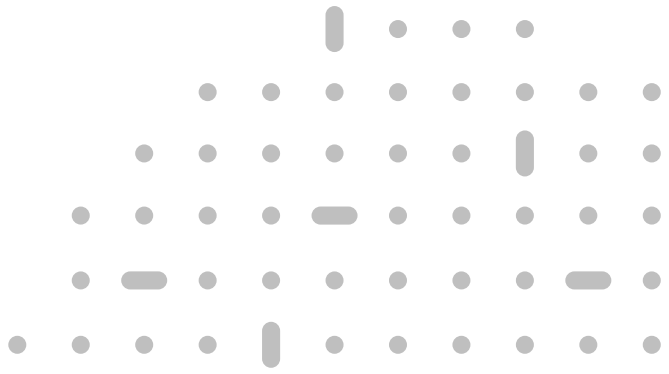
We have taken all required actions under POPIA. We took the following actions to further enhance our robust data protection systems to comply with the GDPR back in May 2018 and this compliance programme has meant that we are many steps ahead of other organisations with regards to our POPIA compliance programme.

- **Upgraded policies and procedures:**
  As part of our GDPR compliance strategy we reviewed and upgraded existing policies and procedures including our data protection notices to ensure that we comply with the GDPR. All our staff and key individuals are continually trained on these policies for our compliance and to offer you assistance with your compliance efforts.
- **Personal data breach notification:** POPIA requires that notification of a data breach to the Information Regulator be given "as soon as reasonably possible". In the event we become aware of a breach affecting your personal data, we will notify you without undue delay in no more than 48 hours and assist you in complying with your POPIA obligations by providing you the required information related to the personal data breach in a timely manner.
- **POPIA Compliance monitoring:**
  We will continue to regularly review and audit the security of our services and our compliance with our POPIA & GDPR policies and procedures.
- **Training:** Continuing on from our long-standing data protection training program, we will continue to train our staff globally on data protection requirements, including POPIA and the GDPR, as part of our ISO 27001 certification.
- **Individual enforceable rights:** Under POPIA as the responsible party, you are obliged to facilitate the exercise of each data subject's rights. As your operator, we have set out below in Section 5 the ways in which our systems and processes can support you in meeting your obligations to the data subjects:

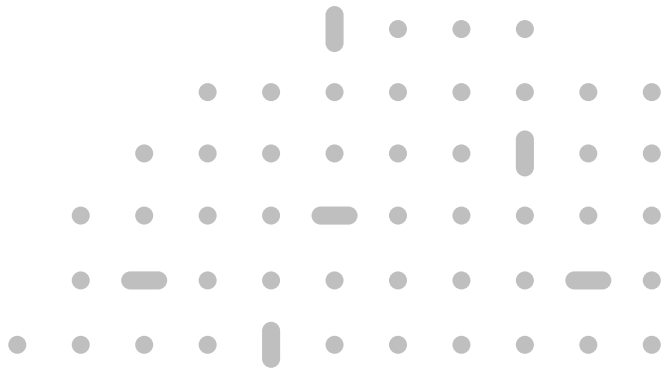
4 Key Differences between the GDPR and POPIA

Most of the work required to comply with POPIA was already completed as part of our GDPR compliance programme back in May 2018 but there are a few differences between GDPR and POPIA. POPIA was based on the early drafts of GDPR and therefore many principles are very similar.

- **New Definition of Responsible Party rather than Data Controller:** GDPR clearly defines a data processor (as a natural or legal person processing personal data on behalf of the data controller) . The definitions for "controller" and "responsible party" are similar in their content and import.
- **New Definition of Operator rather than Data Processor:** The GDPR and POPIA contain similar definitions for "processor" and "operator" respectively. Importantly, both are third parties acting on the instructions of the controller/ responsible party.
- **POPIA Definition of Personal Information:** POPIA defines personal information broadly as any information relating to not only a living person, but also a company or legal entity, unlike the GDPR which only applies to personal data of natural persons.
- **Requirement for an Information Officer:** POPIA requires all companies and organizations to appoint an Information Officer (automatically assigned to the CEO), who's role and responsibilities differ in important areas from the GDPR's Data Protection Officer. In addition, POPIA also permits companies and organizations to appoint a Deputy Information Officer.
- **Restriction of Transfers:** POPIA only allows for the transfer of personal information outside South Africa provided certain conditions are met, such as an adequate level of protection that effectively uphold principles for reasonable processing of the information in a manner similar to POPIA.
- **Individual enforceable rights:** POPIA gives natural and juristic persons (data subjects) several actionable rights in respect of their personal data, including but not limited to the right to access, right to correction and right to deletion of their personal data.



- **Lawful Data Processing Conditions:** POPIA also creates eight conditions for lawful data processing. It is up to websites, companies and organizations ("responsible parties") to prove that their processing is lawful, e.g. that correct consents have been obtained from users. The principles and conditions for processing of personal information in each of the GDPR and POPIA respectively, and the fundamental concepts underpinning both, are largely similar.
- **Definition of Consent:** POPIA defines consent as any voluntary, specific and informed expression of will. While the definition of consent is similar in both, the GDPR also requires that consent be unambiguous.
- **Direct Marketing:** POPIA regulates the processing of personal information during direct marketing activities by means of electronic communications such as email, text and fax. Importantly, it requires an opt-in by data subjects who are not existing customers of the responsible party. SHL has undertaken a review of its marketing practices to ensure that for all prospective South African clients, we have documented opt in.



5 Compliance with specific POPIA provisions

POPIA Section	Compliance
Section 18 **The right to be informed**	Our assessment platform includes a data protection notice which individuals are presented with prior to taking the assessment. This notice provides information to the individual about the collection and processing that we perform, in accordance with data protection legislation requirements. As the assessment makes up one part of an overall recruitment process, (and the assessment is generally not your first point of candidate data collection) the Section 18 notice requirements may also need to be satisfied earlier than our assessment platform. You may employ several different methods, such as your careers website, an online application form, or applicant tracking system to receive initial applications, and collect other personal information e.g. CV or résumé information, residential address etc. In each of these systems, a data protection notice that addresses the full recruitment cycle would be required at the point of data collection.
Section 23 **The right of access**	A candidate's request to access their personal data should be directed to you, as the responsible party. We occasionally receive requests directly from candidates to delete their information, or to provide access to their assessment results. We redirect these candidate requests back to the organisation for whom they completed the assessment as the data controller. We then provide support and information to you as you require to meet your obligation to the candidate. If we receive such a request directly from you as our client, we already have processes in place to carry out that request, whether that is promptly responding to a data subject access request, or a request for deletion of data. Clients often ask "how long do you retain data?" As a data processor, we retain data in accordance with our client agreements, meaning we delete data following a request from you.

We observe POPIA data transfer rules: Section 72 of POPIA prohibits the international transfer of personal information unless the recipient is subject to a binding agreement which provides an adequate level of protection. We are happy to enter into appropriate data transfer agreements which provide an adequate level of protection as required.

We will continue to monitor any proposed changed to the Model Clauses and ensure we upgrade our agreements as required.

Data protection agreements:
We regularly enter into data protection agreements with our clients. Please workwith your sales representative to contact us to update or implement appropriate additional data protection terms to meet your requirements.

If you have any further questions please either speak to your account manager or email dpo@shl.com

© 2023 SHL and its affiliates. All rights reserved.