July 5, 2021

POPI Act Guidelines - Processing Personal Information subject to Prior Authorisation



Personal information has become one of the most powerful commodities in the modern world.

In this new age of processing Personal Information, companies that process Personal Information outside the borders of South Africa will be subject to foreign data privacy and protection laws such as the General Data Protection Regulation (GDPR).

In addition to complying with foreign legislation, the *Responsible Party* should obtain prior authorisation from the Information Regulator when processing Personal Information across the border.

The Information Regulator published a media statement on 22 June 2021, extending the applications for prior authorisation to **1 February 2022.**

Section 57 of the Protection of Personal Information Act (POPI) specifically deals with prior authorisation. In a previous article we discussed *the most frequently asked questions about the POPI Act,* the purpose of this article is to explain when to obtain prior authorisation from the Information Regulator and the definitions in this regard.

Important definitions - Section 57 of the POPI Act

- A ***Unique Identifier*** is defined as *"any identifier that is assigned to a Data Subject and is used by the Responsible Party for the purpose of the operations of that Responsible Party and that uniquely identifies that Data Subject in relation to that responsible Party".*

- ***Special Personal Information*** is defined as any information relating to–

1. *the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or*
2. *the criminal behaviour of a data subject to the extent that such information relates to–*

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal

of such proceedings.

- A **Child** is defined as *"a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself".*

- A **Third Party** is defined as any Person, excluding a Company or Personal Requester. *An expression which denotes or includes–*

1. *a natural person, includes a juristic person and vice versa; the singular, includes the plural and vice versa;*
2. *a party, includes a reference to that Party's successors in title and assignees allowed in law;*
3. *the words "include" and "including", means "include without limitation" and "including without limitation". The use of the words "include" and "including" followed by a specific example or examples shall not be construed as limiting the meaning of the general wording preceding it.*

When is Prior Authorisation required from the Information Regulator?

Prior Authorisation is required from the Information Regulator when a Responsible Party–

- plans to process any *Unique Identifiers* of Data Subjects–
  - for a purpose other than the one for which the identifier was specifically intended at collection; and
  - with the aim of linking the information together with information processed by other Responsible Parties.
- processes information of criminal behaviour, or unlawful or objectionable conduct on behalf of Third Parties.
- processes information for credit reporting purposes.
- transfers Special Personal Information or Personal Information of children to a Third Party.

If the Responsible Party applied for a Code of Conduct in any of the above-mentioned circumstances, prior authorisation is not required. Also note that a Responsible Party only needs to obtain prior authorisation once, not every time they plan to process any of the above.

Failure to notify processing subject of prior authorisation is an offence for which your organisation could face a fine and/or imprisonment for a period not more than 12 months. The Information Regulator will also stop your organisation from processing information to ensure that you are unable to do business.

Also bear in mind that there are restrictions on cross-border information transfer when sending Personal Information outside the borders of South Africa. These restrictions are dependent on the laws of the country where Personal Information is being transferred or stored.

SERR Synergy assists businesses in ensuring that Personal Information is processed according to legislation, while simultaneously serving the needs your business may have with regard to such data.

We provide a full range of Information Compliance service offerings, be it compiling Data and Information Protection Reports, drafting the required Data Privacy policies, updating your agreements to handle data considerations, advising on internal data handling requirements or understanding exactly what data privacy role you fulfil. Reputational damage due to non-compliance is a material risk which may lead to directors being declared unfit to be a director in terms of the Companies Act.

We recommend that businesses start the compliance process sooner rather than later. If you want your organisation to be POPIA compliant and ready by **1 July 2021**, feel free to contact us for more information.

***About the Author*:** Retha van Zyl completed her BCom Hons (Economics and Risk Management) studies at the North West University. She joined our team in January 2016 and currently holds the title 'Information Compliance Advisor'. She specialises in POPI and PAIA compliance, which includes compiling and submitting PAIA Manuals to the Human Rights Commission. She also compiles the Data and Information Protection Report to identify risks associated with information security and drafts information security policies for procedural compliance in each department within an organisation.

Sources:

- The Protection of Personal Information Act 4 of 2013.

©SERR Synergy, www.serr.co.za