**POPI Privacy Impact Assessment Key Questions**

# Why should I do a Privacy Impact Assessment?

* To identify privacy risks to individuals.
* To identify privacy and DP compliance liabilities for your organisation.
* To protect your reputation.
* To instil public trust and confidence in your project/product.
* To avoid expensive, inadequate “bolt- on” solutions.
* To inform your communications strategy.

**Technology**

# Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?

Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS)and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.

**Identity**

# Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?

Examples of relevant project features include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme, and an intrusive identifier such as biometrics. All schemes of this nature have considerable potential for privacy impact and give rise to substantial public concern and hence project risk.

# Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?

Many agency functions cannot be effectively performed without access to the client's identity. On the other hand, many others do not require identity. An important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.

**Multiple organisations**

# Does the project involve multiple organisations, whether they are government agencies (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?

Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation to preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protection measures should be considered.

**Data**

# Does the project involve new or significantly changed handling of personal data that is of particular concern to individuals?

The Act identifies a number of categories of Special Personal Information that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.

There are other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can enable identity theft.

Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such 'persons at risk' may suffer physical harm if they are found.

# Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database?

Examples include intensive data processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.

# Does the project involve new or significantly changed handling of personal data about a large number of individuals?

Any data processing of this nature is attractive to organisations and individuals seeking to locate people, or to build or enhance profiles of them.

# Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?

This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.

**Exemptions and exceptions**

# Does the project relate to data processing which is in anyway exempt from legislative privacy protections?

Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections have been negated by legislative exemptions or exceptions.

# Does the project's justification include significant contributions to public security measures?

Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight. This has resulted in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme

# Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation? Disclosure may arise through various mechanisms such as sale, exchange, unprotected publication in hard-copy or electronically-accessible form, or outsourcing of aspects of the data-handling to sub-contractors.

Third parties may not be subject to comparable privacy regulation because they are not subject to the provisions of the Act or other relevant statutory provisions, such as where they are in a foreign jurisdiction. Concern may also arise in the case of organisations within South Africa which are subsidiaries of organisations headquartered outside SA.

This document is based on work on Privacy Impact assessments completed by the UK Information commissioner’s Office ([www.ico.org.uk](http://www.ico.org.uk)).