Key operative definition of the Protection of Personal Information Act 2013 (POPIA)

What are the operative components to POPIA ?

POPIA applies to the PROCESSING of PERSONAL INFORMATION [of the "DATA SUBJECT"] and according to Section 3(1)(a) and Section 3(1)(b), PERSONAL INFORMATION entered in a RECORD by or for a RESPONSIBLE PARTY by making use of automated or non-automated means, provided that when the RECORD of PERSONAL INFORMATION IS PROCESSED by non-automated means (e.g. paper and text, photographs, x-rays), it forms part of a FILING SYSTEM or is intended to form part of a FILING SYSTEM and in terms of Section 3 (1)(b)(i), the RESPONSIBLE PARTY is domiciled in the Republic OR in terms of Section 3(1)(b)(ii) the RESPONSIBLE PARTY is not domiciled in the Republic, but makes use of automated or non-automated means, unless the PROCESSING relates only to the FORWARDING OF PERSONAL INFORMATION.

What is meant by processing?

PROCESSING means any activity, whether or not by automatic means relating to PERSONAL INFORMATION, including OBTAINING according to Section 1(a), the following concerning PERSONAL INFORMATION:

- Collection
- Receipt
- Recording
- Organization
- Collation
- Storage
- Updating
- Modification
- Retrieval
- Alteration
- Consultation
- Use in general

PROCESSING further means any activity, whether or not by automatic means relating to PERSONAL INFORMATION, including DISSEMINATION according to Section 1(b)means the Dissemination of Personal Information by means of:

- Transmission
- Distribution

Processing also pertains to what is described as Dissemination, which includes all activities in respect of DATA SUBJECT's PERSONAL INFORMATION.

PROCESSING means any activity, whether or not by automatic means relating to PERSONAL INFORMATION, including **DESTROYING according to** Section 1(c) means the following concerning personal information.

- Merging – Departments
- Linking
- Restriction
- Degradation
- Erasure
- Destruction

PROCESSING SUBJECT TO PRIOR AUTHORISATION means that a RESPONSIBLE PARTY must obtain prior authorization from the Information Regulator if the RESPONSIBLE PARTY plans to PROCESS INFORMATION in terms of Section 57(1)(a), which contains any unique identifiers of Data Subjects for a purpose other than the one specifically intended at collection and with the aim of linking the Personal Information being processed, with information processed by a Responsible Party and also in terms of Section 57(1)(b) in respect of criminal or unlawful conduct, also Section 57(1)(c) for the purpose of credit reporting and Section 57(1)(d) which is defined as Special Personal Information or is the Information of a child which is being transferred to a foreign country that does not provide an adequate level of protection in its Law.

Access: the right, the opportunity, or the means of finding, using, or retrieving information
Accountability: the condition that individuals, organisations, and the community are responsible for their actions and may be required to explain them to others

Anonymous information which does not relate to an identified or identifiable natural person or to personal information rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Anonymous information: information which does not relate to an identified or identifiable natural person or to personal information rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Anti-malware: software that is designed to identify and prevent malicious software, or malware, from infecting computer systems or electronic devices.

Anti-virus: software designed to detect and destroy computer viruses.
Automated decision making: Decisions made by machine (computers), without human intervention. For example, to automatically accept or deny an online credit application or the automated processing of CVs that evaluates (profiles) personal aspects of individuals to determine if they will qualify for a position.

Availability: The guarantee of reliable access to information by authorised people

Binding corporate rules: Personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country.

Biometric data: Personal information resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Child: 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

Children
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.

Classification: the process of assigning an appropriate level of classification to an information asset to ensure it receives an adequate level of protection

Confidentiality: is managed by the set of rules that limits access to information

Consent: Of the data subject means, any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information

Continuity: encompasses planning and preparation to ensure that an organisation can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period

Core activities: the core activities of a Responsible Party relate to primary activities and do not relate to the processing of personal information as ancillary activities. An example of an ancillary activity would be a organisation paying the salaries of its workers. However, the core activity of a hospital is to provide health care and it could not provide healthcare safely and effectively without processing health data, such as patients' health records. Those activities cannot be considered ancillary and must be considered as core.

Data mapping: the process used to identify what personal information you use, why you use it, how sensitive it is, how long you may retain it, where you process it and where you collect it.

Data subject: the person to whom personal information relates.

De-identified: information which does not relate to an identified or identifiable natural person or to personal information rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Delete
the process of eliminating or deleting records beyond any possible reconstruction.

Deletion
the process of eliminating or deleting records beyond any possible reconstruction.

Destroy
the process of eliminating or deleting records beyond any possible reconstruction.

Disaster recovery
the process or actions for an organisation to minimise the effects of a disruptive incident, to continue to operate or quickly resume mission-critical functions.

Encryption
the process of converting information or data into a code, especially to prevent unauthorised access

Erasure
the process of eliminating or deleting records beyond any possible reconstruction.
Filing system: any structured set of personal information which are accessible according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis

Genetic: personal information relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular DNA or RNA analysis

Genetic data: personal information relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Group of undertakings: a controlling undertaking and its controlled undertakings

Health: personal information related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status

Health: personal information concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject

High-risk: activities including, but not limited to, large scale data processing which could affect a large number of individuals; regular and systematic monitoring; the transfer of personal information to countries which don't have adequate privacy

Information officer: in relation to a private body means the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act or in relation to a public body means an information officer or deputy information officer as contemplated in terms of sections 1 or 17 of the Promotion of Access to Information Act

Integrity: the assurance that information is trustworthy and accurate

International organisation
an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

Large-scale data processing: examples include - patient data in the regular course of business by a hospital; travel data of individuals using a city's public transport system (e.g. tracking via travel cards); real time geo-location data of customers of an international fast food chain for statistical purposes by an Operator specialised in these activities; customer data in the regular course of business by an insurance organisation or a bank; personal information for behavioural advertising by a search engine; data (content, traffic, location) by telephone or internet service providers. Examples that do NOT constitute large-scale processing include - processing of patient data by a single physician; processing of personal information relating to criminal convictions and offences by an individual lawyer.

Operator: a natural or legal person, public authority, agency or other body which processes personal information on behalf of the Responsible Party

Personal information: information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

Personal information impact assessment: a systematic process for evaluating the potential impact of information processing risks that are likely to affect the privacy rights of individuals.

Policies: clear and measurable statements of preferred direction and behaviour to condition the decisions made within an organisation

Policy: clear and measurable statements of preferred direction and behaviour to condition the decisions made within an organisation

Process: a set of interrelated or interacting activities that transforms inputs into outputs

Processing: any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Profiling: any form of automated processing of personal information consisting of the use of personal information to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

Regular and systematic monitoring: examples include - operating a telecommunications network; providing telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment (e.g. credit scoring, fraud prevention or detection); location tracking (for example, by mobile apps); loyalty programs; behavioural advertising; fitness and health data via wearable devices; CCTV; connected devices.

Responsible Party: a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

Restriction: to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information - for example - temporarily moving the data to another processing system, making the data unavailable to users, or temporarily removing published data from a website.

Risk: a threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided or mitigated through pre-emptive action.

Security compromise: a security compromise means a security compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information transmitted, stored or otherwise processed.

Security compromise: a compromise of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed.

Special personal information: personal information including religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information.

Technical and organisational measures: internal policies as well as measures which meet the conditions of privacy, inter alia - minimising the processing of personal information; de-identifying personal information as soon as possible; transparency with regard to the functions and processing of personal information; enabling the data subject to monitor the data processing; using Operators who provide the appropriate guarantees; ensuring the appropriate security measures, including confidentiality; maintaining data quality; conducting privacy impact assessments; on-going training and awareness of staff.

Technical or organisational measures: internal policies as well as measures which meet the conditions of privacy, inter alia - minimising the processing of personal information; de-identifying personal information as soon as possible; transparency with regard to the functions and processing of personal information; enabling the data subject to monitor the data processing; using Operators who provide the appropriate guarantees; ensuring the appropriate security measures, including confidentiality; maintaining data quality; conducting privacy impact assessments; on-going training and awareness of staff.

The Regulator: The Information Regulator established in terms of section 39 of POPIA