DATA QUALITY POLICY

"DATA POLICY"

July 2021

TVR LAW

TINEKE VAN ROOYEN

Situated at:

1 Mimosa Street

Jeffreys Bay

DATA QUALITY POLICY

BACKGROUND

TVR LAW, as collator and custodian of sensitive personal information, have become increasingly dependent on information for decision taking. In terms of Section 16 of the Protection of Personal Information Act ("POPIA"), a reasonable party must take all reasonable steps to ensure that all personal information is complete, accurate, not misleading and updated where necessary.

Ensuring that information is of the highest possible quality is essential to both quality of care and effective decision-making. Data must be as relevant as possible, easily accessible and easy to understand. Data must be accurate, comparable, timely and usable to be effectively used in the taking and implementation of decisions. Only once Data has complied with all of these characteristics, then it can be used to effectively and efficiently take and manage decisions. This Data Quality Policy aims to improve and maintain the quality of the data held by TVR LAW.

PURPOSE

The purpose of this Data Quality Policy is to ensure that data collected by TVR LAW is of high quality and able to support it intended uses. This is achieved by allocating accountability and responsibility for the quality of the data collected by TVR LAW.

In terms of Section 16(b) of POPIA, there must be a purpose for the collection of data. Therefore, to comply with this provision, TVR LAW must indicate the purpose of collection of certain data as well as the role and function the data will play within the company's different policies.

With specific regards to this policy, data will be collected and evaluated to determine whether or not the data will assist and enable TVR LAW to effectively and efficiently take decisions with the data available. This policy also aims to address the method and manner in which data may be stored, updated and destroyed

SCOPE

The scope of this policy includes data held by TVR LAW on all of its systems and any data collected from these systems and any other data collections provided for by statute.

The scope of this policy includes both paper-based and electronically collected data and any data obtained in any other manner relating to identity, race, gender, age, identity number, e-mail address, telephone number etc.

Therefore, this policy may be seen as an overarching policy with regard to information held by TVR LAW and supported by a framework regulating the quality thereof.

DEFINITIONS

These important concepts are defined in terms of the Protection of Personal Information Act (POPIA):

"data subject" means the person to whom personal information relates;

"de-identify" means to delete any information that identifies the subject or reasonably foresees a possibility to identify data subject whether it be linked to other information or manipulated;

"electronic communication" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"information officer" an employee within the company who will assume the duties of an Information Protection Officer who must appoint information officers whose responsibilities are defined in the act and includes the encouragement of compliance, by the body, with the information protection principles and dealing with requests made to the body pursuant to this POPIA including any investigations;

"person" means a natural or a juristic person.;

"personal information" means information about a person's race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language, education, medical information, financial information, criminal or employment history, an identifying number, e-mail address, physical address, telephone number, blood type, biometric information, personal opinions, views or preferences of a person., correspondence of a private or confidential nature and the name of the person if it appears with other personal information relating to the person;

"POPIA" Protection of Personal Information Act 4 of 2013;

"prescribed" means prescribed by regulation or by code of conduct;

"processing" means any operation or activity or any set of operations, whether or not it be an automatic, concerning personal information and includes collection, receipt, recording, organization, collation, storage, updating, modifying, retrieving, altering, consulting or using by means of transmission, distribution or making available in any form or merging, linking, restricting, degrading, erasing or destructing of information;

"record" means any recorded information regardless of form or medium and includes the writing on any material, any information produced, recorded or stored by means of a tape recorder, computer equipment (hardware/software or both) or any other device resulting in information being produced, recorded or stored; any label, marking or other writing that identifies or

describes anything that forms part thereof; any book, map, plan, graph, drawing, photograph, film, negative, tape or other device in which one or more images are embodied which can be reproduced (with or without equipment) which is in the possession or control of a responsible party regardless of whether it was created by responsible party or when it came into existence;

"responsible party" means a public or private body or any other person in conjunction with others who determines the purpose and means of processing personal information.

POLICY STATEMENTS

1. Duration of keeping records

Records of personal information may not be kept longer than reasonably necessary for achieving the initial purpose for which it was obtained, unless authorized or required by statute. Other lawful exclusions include retaining a record due to contract between parties or a data subject consents to retention.

Whenever data is kept for a period longer that was reasonably necessary or the initial purpose has been achieved, the responsible party must provide for appropriate and effective safeguarding of such records.

However, if there is no reasonable, lawful or statutory reason for retaining records, it must be destroyed (or de-identified) as soon as reasonably possible. Destruction (or de-identification) must be done to such an extent that reconstruction will not be possible in intelligible form.

Time retention is statutorily prescribed and strictly adhered to in the following scenario's:

STATUTE	WHAT IS RETAINED	RETENTION PERIOD
Companies Act	Business records	15 years
Income Tax Act	Tax records	5 years
Value Added Tax (VAT) Act	VAT records	5 years
Basic Conditions of Employment Act	Employee records	3 years
National Credit Act	Credit agreement records	3 years
Electronic Communications and Transactions Act	Any record containing electronic communications or records of electronic transactions (excluding e-mail)	1 year
No statute but good practice that is enforced	E-mails	3 years

2. Updating of records

The further processing of records is limited insofar the initial purpose has been achieved. Therefore, in introductory terms, records may only be updated if the initial purpose of the collection has changed or the initial data collection does not satisfy the purpose (it was originally collected for) anymore. The data subject must, however, always consent to further processing of data.

Information may only be processed insofar the processing thereof is lawful and reasonable while not infringing on the privacy of the data subject. This policy statement is regulated in terms of Section 9 of POPIA. When obtaining data from a data subject, the data collector may only collect data that is lawfully required and legally permissable. Therefore, any information that is not relevant or justifiable may not be collected to form part of data. This specifically includes any collection of data when updating the data.

Further processing will be allowed (even if incompatible with the initial purpose of the collection of data):

- The data subject expressly agrees thereto;
- The data forms part of information records that has been made public by the data subject self or the data is derived from any public record;
- Data is required to prevent or mitigate a serious or imminent threat either against the data subject or another;
- Data may also be further processed if it is required to prevent legal prejudice.

Data must be stored in such a manner that a data subject is able to request such information at any time.

3. Destruction of records

Once data retention is no longer compatible with the purpose it was obtained for or no longer satisfies a statutory or reasonable cause, TVR LAW will destroy such records to such an extent that recovery or re-identification is no longer possible in an intelligible sense.

4. Training of staff

Any staff member who has access to personal data and/or who is the responsible party for capturing of data must undergo basic training of the POPIA. Such training will, at the very least, consist of an in-depth discussion with the company's Information Protection Officer who must seek to address the following outcomes:

- Inform the employee(s) of the POPIA;
- Have a discussion with the employee(s) on the workings and legal consequences that POPIA pose on a company as well as any individual WHO has access to personal data;
- Supply the employee(s) with all the implemented Policies on Personal Information Protection;
- Ensure to cover the aim, scope and provisions relating to implemented policies;
- Provide every employee with this policy together with the Protection of Personal Information Policy.

Only employees, who have completed the above-mentioned outcomes to the satisfaction of the Information Protection Officer, shall be allowed to access and capture personal information held by TVR LAW.

5. Limiting access control to records

Access control will be implemented as per the Protection of Personal Information Policy. This includes (but is not limited to):

- Encryption of data messages;
- Strong and secure passwords on personal computers, servers and documents;
- Non-disclosure agreements, in writing, with third parties whenever a data transfer takes place;
- Access to databases, server rooms or data centers be strictly limited to only those who have the necessary authority to do so;
- Strong regulation by the Protection Information Officer to ensure that any retired, retrenched, transferred or previous employees do not retain access to data;
- Any contractors/temporary staff/consultants or external service providers must be subjected to stricter regulation and monitoring, when accessing data, while also adhering to all Information Protection Policies (including this one).

IMPLEMENTATION

This Data Quality Policy must be implemented with the necessary care, skill and knowledge reasonably expected from an Information Protection Officer.

It must, furthermore, seek to comply with all other Personal Information Policies adopted by TVR LAW. The Information Protection Officer must aim to implement all adopted policies concurrently including the POPIA. Should a discrepancy arise between any policy and/or the POPIA, the POPIA will prevail.

When applying this Data Quality Policy, the following checklist must be considered to determine whether the minimum requirements have been met:

Audit the Data process with specific regard to:	
➢ The collection of data; ➢ The recording of data; ➢ The storing of data; ➢ The integrity and safeguarding of data; ➢ The destruction of data no longer compatible with purpose it was obtained for or data that has become irrelevant.	

Audit the initial purpose the data was collected for: ➢ Is the purpose still compatible at this stage? ➢ Is there a legally reasonable reason for still storing the data?	
Audit the limitation of further data processing: ➢ Further processing must be lawful, reasonably necessary and not excessive; ➢ **Further processing should commence at the approval of the data subject unless extraordinary circumstances are at play.**	
Audit the steps taken to notify data subject of further processing ➢ Any individual whose personal information is being processed has a right to know why it is being done, why and by who; ➢ It should also be stated whether or not the processing is voluntary or mandatory;	
Audit the reasoning behind further processing;	
Ensure that information obtained is adequate, up to date, complete and not misleading;	
Allow the data subject to make requests: ➢ Data subjects are allowed to make requests to companies in possession of personal information about them; ➢ These requests must be made free of charge; ➢ A data subject is entitled to request the complete record of data available.	
Audit retaining process: ➢ Ensure that certain types of documents are retained for the prescribed period of time required; ➢ Once this period of time has lapsed, destroy or de-identify to data to such an extent that intelligible recovery will not be possible.	
Audit cross border transfer ➢ Always determine whether or not cross border transfer occurred and whether all the relevant and applicable statutes and processes were duly followed.	

CONCLUSION

Poor quality data can have extreme consequences for an institution. With specific regard to TVR LAW, poor quality data will result in reputational damage throughout the sector. _____ (PTY) LTD hold and controls personal data, as collator and custodian, of a vast spectrum of people within the general public.

Therefore, by implementing the above Policy Statements, TVR LAW ensures that data collected is of a high quality and enables them to effectively and efficiently take the necessary decisions. It furthermore provides for a safe and confidential environment wherein their data subjects feel secure and respected which ensures client satisfaction.