First Arrow Consulting (Pty) Limited

Personal Data Retention Policy

1. Purpose

First Arrow Consulting (Pty) Limited has developed this Personal Data Retention Policy ("Policy") to guide employees in their obligations regarding the retention and disposal of Personal Data (as described below). This policy establishes general rules that are consistent with emerging trends in the law governing Personal Data, such as the EU General Data Protection Regulation ("GDPR") and South Africa's Protection of Personal Information Act ("POPI"). Where applicable local law or contract terms require stricter practices, those stricter practices shall apply.

Please check with your FIRST ARROW legal representative if you are unsure as to the laws or terms that apply to particular Personal Data.

All employees of FIRST ARROW whose positions may result in access to Personal Data are required to read and understand this Policy, comply with these and all other applicable policies and procedures, and ensure that all agents and contractors who may be provided access to Personal Data are aware of, understand, and adhere to this Policy. You should contact the Legal Department if you have any questions regarding this Policy. It is First Arrow's policy to investigate and address all circumstances in which there is a possibility that Personal Data entrusted to FIRST ARROW or its contractors by its customers is being retained in violation of this Policy, applicable regulations or applicable contractual terms.

FIRST ARROW is committed to continuously reviewing and updating its policies and procedures. Therefore, this Policy is subject to modification at First Arrow's discretion. In the event of conflicts between this Policy and future modifications, the latest modification will control. If you are unsure whether you are reviewing the latest version of this Policy, you should ask the Legal Department.

2. Introduction – What Is Personal Data?

Generally speaking, Personal Data is any information that FIRST ARROW obtains or creates that relates to a specific, individual living person, known frequently as a Data Subject. Personal Data includes identifiers such as: a name; an identification number, including government identification numbers and financial account identifiers; location data, including home or work addresses, phones numbers or e-mail addresses; an online identifier such as an IP address or a cookie string; or factors specific to the physical, genetic, physiological, mental, economic, cultural or social identity of a Data Subject. Some regulations refer to Personal Data as Personally Identifiable Information. Where Personal Data involves information arising from health care, it is sometimes referred to as Protected Health Information and is subject to heightened standards regarding its handling and use. The same holds true for other forms of sensitive Personal Data, such as data pertaining to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; sexual orientation or activities, genetic data and biometrics.

It is important to note that, even if FIRST ARROW is unable to identify the Data Subject from the piece(s) of Personal Data that are in its possession, this does not affect First Arrow's obligations for handling that data under the law. Unless the data that FIRST ARROW possesses about an individual has been irreversibly anonymized so that it is not possible to associate it back to the Data Subject, it remains Personal Data and is subject to this Policy. By way of example, although FIRST ARROW may not be able to identify an individual behind an IP address, possession of an IP address would still constitute Personal Data, as the internet service provider can trace the IP address back to a Data Subject.

Data need not be in electronic form to be Personal Data. Any data about individuals retained in a physical filing system (e.g., HR files) constitutes Personal Data for regulatory purposes and are subject to this Policy.

3. General Rule

Regulations such as POPIA place significant parameters around the retention of Personal Data. As an initial matter, Personal Data may only be collected and processed when the Data Subject has freely given informed, clear consent or, in very limited circumstances, where the law expressly allows the collection and processing of the Personal Data. The exception of allowable collection and processing under the law is generally inapplicable to FIRST ARROW; primarily, FIRST ARROW only will collect and process Personal Data in connection with entering into and performing contracts.

Assuming that proper consent was obtained and that there is a lawful purpose to process the Personal Data, the following principles control.

Personal Data must:

(1) only be collected and retained in an amount that is adequate, relevant and necessary for the processing being performed;

(2) be kept accurate, through updating where necessary;

(3) processed only for the purposes to which the Data Subject has explicitly consented as able to be demonstrated by FIRST ARROW;

(4) processed consistent with the Data Subject's rights to limit or bar processing, including the right to be forgotten (i.e. have all Personal Data deleted from the company's records); and

(5) not be retained longer than necessary to fulfil the processing for which consent was obtained.

Taken together, these controlling principles establish the following rules:

FIRST ARROW will only accept, collect or create, and shall only retain the minimum amount of Personal Data needed for meeting the purpose of the lawful processing that is being performed.

Where the Personal Data is no longer current or needed, that Personal Data shall be deleted in a manner consistent with Company policy within no more than ninety (90) days from the date of the determination of lack of need.

Where FIRST ARROW has been notified by a Data Subject that they have invoked their right to be forgotten, requested deletion or notified FIRST ARROW of the withdrawal of their consent, deletion of their Personal Data shall occur without undue delay.

For Personal Data that is no longer current or needed, the period of ninety days has been chosen to allow enough time to delete the Personal Data in an orderly fashion, without putting undue burdens on FIRST ARROW or allowing the data to reside on its systems for an excess amount of time.

Where a Data Subject has withdrawn consent for processing or has invoked the right to be forgotten, the burden is on FIRST ARROW to demonstrate that the amount of time that it took it to comply with the request was reasonable and did not constitute undue delay; therefore, it is essential in these situations that processing cease and deletion occur as soon as possible.

4. Exceptions

As with most rules, there are limited exceptions to the foregoing. Where FIRST ARROW has a legal obligation to retain a copy of the Personal Data (for example, regulatory requirements to maintain data on past or current employees), such laws control and archival copies of the Personal Data shall be retained to satisfy the separate legal obligation.

It also is unclear whether a Data Subject's invocation of the right to be forgotten mandates deleting all back-up copies of their data that may be in archival storage. FIRST ARROW assumes that enforcement of this requirement will be limited to live data repositories and locally backed-up copies.

Exceptions that increase the period of time that FIRST ARROW is retaining Personal Data should not be assumed, and must be first confirmed through the Legal Department.

5. Disposal or Deletion of Personal Data

Because of the sensitivity of the information it contains, Personal Data must be destroyed or deleted in a manner that ensures that it will not be accessible, retrievable or recoverable. Its disposal or deletion must be documented and performed in accordance with FIRST ARROW policies.

Physical (hard copy) documents containing Personal Data shall be destroyed either (1) by placing the documents into a secure, document destruction receptacle located in a FIRST ARROW office, or (2) by crosscut shredding the documents so as to render them incapable of being reconstructed. Where destruction shall occur through the use of a document destruction service, the service receptacle into which the Personal Data is placed must be locked so as to prevent removal or recovery of the data.

Destruction of electronic files shall be done using an industry-standard file destruction tool; such tool must be utilized in a manner approved by FIRST ARROW to ensure the complete destruction and non-recoverability of the electronic file(s).

6. Suspected Improper Retention of Personal Data

If you become aware of, or suspect that Personal Data is being retained in violation of this Policy, you are required to report it. Absent a concern of intentional management involvement, you should bring the suspected improper retention to the attention of your manager. If the matter continues to be unresolved, or if you prefer not to raise the issue directly with your manager, you may make a report to First Arrow's Legal Counsel or any of its directors. Regardless of the venue through which the concern is raised, the concerns should be raised without fear of reprisal, threats, retribution or reta