sappi

Protection of Personal Information Policy for Sappi Limited and Sappi Southern Africa Limited

Document number	SPOL-030-SL	**Issue date**	01 July 2021
Originator	Maarten van Hoven		
Approved by	Maarten van Hoven Group Head Strategy and Legal Sappi Limited		
Revision number	02	**Revision date**	31 January 2022

Contents **Page**

1. Background to data privacy in South Africa

The Protection of Personal Information Act, 4 of 2013 ("POPIA") which came into force in South Africa on 1 July 2021, is a law which regulates the use and processing of a person and/or legal entity's personal information in order to protect and give effect to a person and/or legal entity's right to privacy, including the right not to have personal information and related data misused, abused or used for ulterior purposes.

POPIA applies to personal information which belongs to individuals and legal entities ("Data Subjects") which is processed in an automated or non-automated manner in South Africa by another ("Responsible Party") and places on any Responsible Party who is processing a Data Subject's personal information, a duty to use it lawfully and only for a specific and defined purpose.

Sappi Limited, Sappi Southern Africa Limited and all related South African subsidiaries and divisions ("Sappi") as a Responsible Party under POPIA are required to appoint an Information Officer ("IO") and Deputy Information Officers ("DIOs") to be responsible for establishing a POPIA Compliance Framework, in order to assess, analyse and understand what types of personal information Sappi is processing, and to thereafter develop processes and procedures, including a POPIA Policy to be followed.

A Personal Information Impact Assessment in terms of the Sappi POPIA Compliance Framework has been carried out, which has indicated that Sappi during the course of its business activities collects, stores and processes Personal Information about Sappi employees, customers, suppliers and other third parties.

Furthermore, the Personal Information Impact Assessment has revealed that Sappi processes a large amount of different types of Personal Information including names, addresses, opinions, financial details, medical details including biometric information and the like which pertain to current, past and prospective employees and customers, suppliers, and others with whom Sappi communicates.

Sappi also processes "Special Purpose Information" as defined under POPIA, from time to time for the purposes of recruitment, employment equity statistics, legal compliance and the facilitation of union fees and memberships.

Following the Personal Information Impact Assessment, Sappi is confident that the Personal Information (including the Special Personal Information) that it holds is stored subject to the prescribed legal safeguards as specified in POPIA and other regulations.

This Policy sets out how Sappi and its personnel are to go about processing and using another's Personal Information (including Special Personal Information) in accordance with the conditions for lawful processing as detailed in POPIA.

2. Statement from the Sappi board of directors

2.1. Sappi conducts business in accordance with the highest ethical standards and in compliance with all applicable laws, including the law known as the Protection of Personal Information Act, 4 of 2013, (POPIA) which regulates the lawful Processing of Personal Information.

2.2. This Protection of Personal Information Policy ("the/this Policy") has been developed at the direction of Sappi's Board of Directors in order to provide clear guidance to all directors, employees and those who Process Personal Information on behalf of Sappi to ensure that it is done in a lawful, transparent and consistent manner and in compliance with all applicable data protection laws, including POPIA and the General Data Protection Regulation 2016/679 (GDPR) applicable in the EU (hereinafter referred collectively as the "Data protection laws").

3. Terms and definitions used in this policy

POPIA makes use of certain definitions which are used in this Policy and which are explained below:

3.1. ***"Consent"*** means in relation to POPIA, any voluntary, specific and informed expression of will in terms of which permission is given by the Data Subject for the processing of Personal Information.

3.2. ***"Data Subject"*** means any individual or legal entity to whom Personal Information relates.

3.3. ***"Operator"*** means any person who Processes Personal Information on behalf of a Responsible Party as a contractor or sub-contractor, in terms of a contract or mandate, without coming under the direct authority of the Responsible Party.

3.4. ***"Personal Information"*** means Personal Information relating to any identifiable, living, natural person, and an identifiable, existing juristic person, including, but not limited to:

- name, address, contact details, date of birth, place of birth, identity number, passport number
- bank details
- qualifications, expertise, employment details
- tax number
- vehicle registration
- dietary preferences
- financial details including credit history
- next of kin/dependants
- education or employment history, and

- ***Special Personal Information*** means Personal Information as referred to in section 26 of POPIA, including religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information and criminal behaviour of a Data Subject to the extent that it relates to the alleged commission of an offence or any proceedings in respect of any offence allegedly committed.

3.5. ***"Personnel"*** means Sappi directors, employees and any other person who may Process Personal Information on behalf of Sappi.

3.6. ***"Processing, Process, Processed"*** means in relation to Personal Information, the collection, receipt, recording, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; merging, linking, as well as restriction, degradation, erasure or destruction of information; or sharing with, transfer and further Processing, including physical, manual and automatic and in relation thereto which may be held in a ***"Record"*** which means any recorded information housing Personal Information Processed by Sappi, or its Personnel, regardless of form or medium.

3.7. ***"Processing Notices"*** means a notice setting out the prescribed information that must be provided to Data Subjects before Processing their Personal Information (also referred to as "Section 18 Notices", "Privacy Notices" or "Data Protection Notices").

3.8. ***"Purpose"*** means the underlying reason why a Responsible Party or Operator needs to Process a Data Subject's Personal Information.

3.9. ***"Record(s)"*** means any recorded information housing Personal Information Processed by Sappi or its Personnel, regardless of form or medium.

3.10. ***"Responsible Party"*** means, in relation to POPIA, the person or legal entity who is Processing a Data Subject's Personal Information.

4. Scope and application

This Policy applies to any person who Process Personal Information on behalf of Sappi, including Sappi directors, employees and Operators, who are referred to collectively as "Personnel" in this Policy.

5. Lawful basis for processing

In terms of POPIA, where Personal Information is Processed such Processing must be done lawfully and in a reasonable manner that does not infringe on the privacy of the Data Subject. In order to discharge this obligation, Personnel must comply with the Conditions for Lawful processing of Personal Information as detailed in Chapter 3 of POPIA and as summarised in this Policy.

6. Consent

6.1. A Data Subject does not have to Consent to the Processing of his/her/its Personal Information where there is a lawful basis for such Processing. A lawful basis for Processing in terms of the applicable Data Protection Laws is:

- Where the Processing is **necessary to conclude a contract** to which the Data Subject is a party and to perform contractual obligations or give effect to contractual rights
- Where the Processing is **necessary in order to comply with a law** or to comply with certain legal obligations imposed by a law
- Where the Processing is **necessary to protect a Data Subject's legitimate interests or rights, the Data Subject's legitimate interests or rights or a third party's legitimate interests or rights**, unless there is a good reason to protect the Data Subject's Personal Information which overrides those legitimate interests, and
- Where the Processing is **necessary in order to perform a public duty** or to perform tasks carried out in the public interest or the exercise of official authority.

6.2. Where there is no lawful basis for the Processing, then the Data Subject is required to Consent to the Processing.

6.3. Personnel must ensure that prior to Processing a Data Subject's Personal Information, that there is a lawful basis for the Processing (which lawful reason will be described in the relevant Processing Notice) alternatively that the Data Subject has consented to such Processing.

6.4. A Data Subject may withdraw his/her/its Consent by providing Sappi with a "Withdrawal of Consent Notice" available on Sappi's website. Such notification will be handled directly by Sappi's Information Officer or Deputy Information Officer, which outcome will be relayed to the Data Subject concerned.

6.5. A Data Subject may not withdraw Consent where no Consent was in fact required, ie where Sappi can show that there is a lawful basis for the Processing. In such a case the Data Subject must rather provide Sappi with an "Objection Notice", available on the Sappi's website. Such notification will be handled directly by Sappi's Information Officer, which outcome will be relayed to the Data Subject concerned and relevant Personnel if appropriate.

6.6. Where a Data Subject withdraws Consent or objects to the Processing of certain Personal Information, the relevant Personnel in such a case must refrain from Processing the Personal Information concerned, unless Sappi can show compelling legitimate grounds which overrides the interests, rights and freedoms of the Data Subject concerned or the Processing is necessary for the establishment, exercise or defence of legal claims.

6.7. Sappi's Information Officer will at the time of the withdrawal or objection referred to above, explain to the Data Subject the effects and consequences of any withdrawal or objection and relay the outcome to the Data Subject concerned.

6.8. The Processing of Special Personal Information is generally prohibited under POPIA unless the prior consent of the Data Subject has been obtained **or** any of the following conditions are met:
- Processing is necessary for the establishment, exercise, or defence of a right or obligation in law
- Processing is necessary to comply with an obligation under international public law
- Processing is for historical, statistical or research purposes to the extent that i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or ii) it is impossible or would involve a disproportionate effort to ask for consent and sufficient guarantees are in place to ensure the privacy of the Data Subject, or
- Information has deliberately been made public by the Data Subject or the provisions of POPIA have been complied with.

7. Purpose specific

7.1. Personal Information:
- May only be collected for a specified, explicit and legitimate purpose
- May only be used for the purpose for which it was collected and for no other purpose, unless the Data Subject has been informed of the other purposes, and
- May not be further Processed or used for any subsequent purpose unless that Personal Information is required for a similar purpose and such Processing is compatible with the initial purpose.

7.2. Sappi Processes Personal Information belonging to a vast range of Data Subjects for business purposes, including visitors to its sites, employees and staff, prospective employees and job applicants, students and interns, service providers and contractors, vendors, clients, customers, and other third parties.

7.3. Examples of these purposes and the lawful basis for Processing under POPIA are described below:
- To access Sappi's sites – legitimate interest
- To recruit and employ – employment
- To sell or purchase goods and services – procurement and supply chain
- Concluding and managing a contract or business transaction – contract
- Conducting criminal reference checks – legitimate interest
- Risk assessments – legitimate interest
- Insurance and underwriting purposes – legitimate interest
- Assessing and Processing queries, enquiries, complaints, and/or claims – legitimate interest
- Conducting credit checks – legitimate interest
- Confirming, verifying and updating personal details – legitimate interest
- Detection and prevention of fraud, crime, money laundering or other malpractices – legitimate interest
- Conducting market or customer satisfaction research – legitimate interest
- Direct marketing – legitimate interest
- Audit and record keeping purposes – laws

- Managing debtor and creditors – legitimate interest
- Complying with laws and regulations – laws
- Dealing with regulators – laws
- Paying taxes – laws
- Collecting debts or legal proceedings – legitimate interest
- Communications – legitimate interest, and
- Managing employees – laws.

7.4. Personnel must accordingly:

- Ensure that before Personal Information is Processed, there is a lawful basis for such Processing, and
- Advise Data Subjects why their Personal Information is being Processed, which purpose will be described under the Processing Notices housed on Sappi's website.

8. Accuracy

8.1. All Personal Information Processed by Sappi must be accurate and, where necessary, be kept updated.

8.2. In order to ensure that Personal Information is accurate and is up to date, Personnel must:

- Take reasonable steps to ensure that the Personal Information which they Process is accurate and updated
- Implement procedures to allow Data Subjects to update their Personal Information
- Send out communications to Data Subjects requesting that details are updated
- Ensure that any inaccurate or out-of-date records are updated, and that redundant information is deleted, and
- Take note of the rights of the Data Subjects in relation to updates and rectifications of Personal Information and give effect thereto.

9. Data minimisation

9.1. Sappi may not Process Personal Information which is not necessary for the Purpose for which the Personal Information is initially collected or Processed.

9.2. Personnel must accordingly:

- Ensure that when they process Personal Information on behalf of Sappi, that it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed, and
- Revisit all Records which are currently used to collect Personal Information and consider the purpose for the collection and if no longer needed for the defined purpose then delete such Personal Information.

10. Transparency and Processing Notices

10.1. Sappi has a duty to show that it has dealt with a Data Subject in a transparent manner.

10.2. In order to demonstrate transparency, Sappi must refer Data Subjects to a Processing Notice at the time when Sappi Processes a Data Subject's Personal Information or within a reasonable period thereafter, which Processing Notice must set out:

- The types of Personal Information Processed and the purpose or reason for the Processing
- The lawful basis relied upon for such Processing or whether Consent is required for the Processing
- The period for which the Personal Information will be retained
- Who the Personal Information will be shared with, including external or cross border transfers and the mechanism(s) relied upon for such transfer
- The security measures which are in place to protect the Personal Information, and
- The respective rights of the Data Subject and how these rights may be exercised.

10.3. In order to meet its obligations under 10.2 above Sappi has developed the following Processing Notices:

- A **Human Resources Processing Notice**, which applies to employees (prospective and actual) and bursary or learnership beneficiaries (prospective and actual)
- A **Procurement or Supply Chain Processing Notice**, which applies to participants in Sappi's supply chain, including persons who provide goods and services to Sappi (service providers), persons or entities who purchase goods or services from Sappi (customers), and other parties with whom Sappi engages with and who make up the Sappi procurement and supply chain, including applicable regulators
- A **Company Secretarial Processing Notice**, which applies to all Data Subjects who deal with Sappi from a company secretarial perspective, including directors, trustees, investors, Regulators, shareholders, stakeholders and/or other parties who Sappi may engage with
- A **Security Processing Notice**, which applies to any persons who come onto Sappi sites, facilities and offices and who Sappi may engage with, and
- A **Website Privacy Notice**, which applies to any persons who make use of Sappi's website, social media websites, emails, and other IT related communications facilities and platforms.

10.4. In order to give effect to the above Personnel must:

- Familiarise themselves with the Processing Notices and any others implemented from time to time
- Familiarise themselves with Sappi's Binding Corporate Rules, Personal Information Transfer Agreement and/or its Operator Agreement.

- Ensure that Company documents and forms and Records which house or call for Personal Information contain the following Data Processing details:

  "Please note that in order for Sappi to engage with you it will have to Process certain Personal Information which belongs to you and which Processing is described and explained under the Processing Notices on Sappi's website which we ask that you read. By providing us with the required Personal Information, such act will be taken as an indication that you have read and agree with the provisions described under the Processing Notice and where applicable that you consent to the processing by us of your Personal Information."

- At the time of Processing, direct the Data Subjects to the relevant Processing Notice.

11. General duties: confidentiality, integrity and security of personal information

11.1. In order to safeguard, secure and ensure the confidentiality and integrity of Personal Information held or under the control of Sappi, Sappi together with its Personnel must:

- Identify reasonably foreseeable internal and external risks to Personal Information in its possession or under its control
- Document the identified risks
- Establish, in response to the identified risks, reasonable technical and organisational measures across areas where Personal Information is held or stored
- Implement and maintain measures across areas where Personal Information is held or stored, including electronic and physical measures, designed to minimise the risk of loss, damage, unauthorised destruction and/or unlawful access of Personal Information
- Verify that these measures are effectively implemented which may include the following:
  - The pseudonymisation and encryption of Personal Information
  - ongoing efforts to ensure the long-term confidentiality, integrity, availability and resilience of Personal Information housed within the Sappi environment
  - applications and processes which have the ability to rapidly restore the availability of and access to Personal Information in the event of a tangible or technical incident, and
  - procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organisational measures taken to ensure the security of Processing, including IT Security Audits.

11.2. The duty to ensure data privacy, confidentiality and integrity of Personal Information commences when Sappi initially interacts with a Data Subject and continues until the purpose for the Processing of the Personal Information comes to an end.

12. Records management duties: Confidentiality, integrity and security of personal information

12.1. In order to ensure the confidentiality and integrity of Records, Personnel must ensure that:

12.1.1. All Processing of Personal Information activities and communications are reduced to writing and retained in a Record, which Record may either be electronic, or paper based

12.1.2. Where possible and if necessary, each Record created should be classified and then housed in a folder ("Folder")

12.1.3. Records and Folders should be named in a consistent and logical manner so they can be easily located, identified and retrieved

12.1.4. Folders and Records must be stored and saved in a way that the contents are safeguarded and are identifiable as per the agreed Sappi naming convention and classification, and

12.1.5. Each department must review their Records Register annually and provide a copy to the Information Officer on request.

12.2. Upon termination of employment, or change of job roles or responsibilities of Personnel, the line manager responsible must ensure that any access rights to Folders or Records are terminated and that physical access rights to Sappi's premises and facilities are also terminated.

13. Records management duties: Storage of records housing personal information

13.1. In order to ensure the confidentiality and integrity of paper-based Records which house Personal Information, Personnel must ensure that paper-based Records:

- Which are housed in physical storage areas are labelled and the details recorded
- When in use, are not left around for others to access, and are not left in places where persons can view the contents e.g., on a printer or on unmanned desks
- Are stored securely in Folders when not in use which in turn are placed in locked boxes, drawers, cabinets, or similar structures or containers
- That only Personnel who are required, on an operational and need to know basis, are given access to such Records and/or Folders, and
- Such Records and/or Folders are only removed from Sappi premises if such removal is recorded in the Department Records Management Register and when removed off site, such Records are safeguarded and kept confidential.

13.2. In order to ensure the confidentiality and integrity of electronic Records which house or contain Personal Information, which are held by Sappi, and in order to safeguard and secure these Records, Personnel must ensure that:

- They comply with all applicable Sappi IT Policies and Procedures
- All electronic Records are stored and housed on Sappi servers which are protected by approved security software and one or more firewalls under the direction of Sappi's IT department and where uploaded to cloud computing services, that these services have been approved by the Sappi's IT department
- All devices where electronic Folders and/ or Records are stored are password protected and that passwords are not written down or shared
- All network devices and drives where electronic Folders and Records are stored have access control measures in place
- Electronic Folders and Records are not stored on mobile devices and removable media, which includes, but is not limited to: smart phones, tablets and Ipads, Digital media, USB sticks, external hard drives, CDs, DVDs, memory cards, tapes, unless the device is password protected
- Electronic Records are regularly backed up using the Sappi's provided systems and applications and in accordance with backup protocols
- Device screens are locked when not in use and are password protected, and
- Electronic Records are only transmitted over secure networks, including wireless and wired networks.

14. Records management duties: Retention and disposal of records housing personal information

14.1. Records housing Personal Information must not be retained for a period longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless the longer retention of the Folder or Records:

- Is required or authorised by law
- Is required by Sappi for lawful purposes related to its business activities
- Is required pursuant to a contract between the parties thereto, or
- Consent is received from the Data Subject who owns the Personal Information.

14.2. Records housing Personal Information can be retained indefinitely for business, historical, statistical or research purposes if Sappi has established appropriate safeguards.

14.3. Each Sappi department will be responsible for the correct management of their Folders and Records, including their closing and archiving when they are no longer needed.

14.4. To ensure that the above duties are discharged, Personnel must ensure that:

- The life cycles of Folders and Records under their control are managed
- The relevant record retention periods are adhered to as detailed in Sappi's Records Retention Policy
- The record retention periods, and related requirements are recorded in a relevant register
- A Folder and Record is formally closed when the matter housed in the Folder or Record comes to an end

- A closed Folder or Record is moved to a dedicated archive storage area where the Folder or Record is retained for the required retention period
- Folders and Records are only archived in secure storage area
- Only authorised personnel are granted physical and system-based access to archived Folders and Records
- Folders and Records in archived in areas are regularly backed up
- Once the prescribed retention period in respect of an archived Folder or Record has expired, the Folder or Record is marked "for deletion or disposal"
- Any legal/PAIA hold status is indicated on the relevant Folder or Record or in the relevant register
- During a legal/PAIA hold procedure, the affected Folder or Record is not destroyed, even if the retention period has expired, and
- The destruction of any Folder or Record is recorded under the relevant register.

15. Operators

15.1. Where Sappi makes use of an Operator to process Personal Information, it must ensure that an Operator Agreement/Addendum (hereinafter referred to as the "Operator Agreement/Addendum") is concluded between the parties to ensure that the Operator establishes and maintains the security measures detailed in section 19 of POPIA.

15.2. All Personnel must:

- Familiarise themselves with the Operator Agreement/Addendum
- Ascertain who they use as Operators and ensure that all such Operators sign the Operator Agreement/Addendum or a similar agreement approved by Sappi's legal department, and
- Ensure compliance by the Operator with the provisions of the Operator Agreement/Addendum.

16. Sharing personal information with third parties

16.1. Sappi may not share Personal Information with third parties unless:

- There is a legitimate business need to share the Personal Information, or
- The Data Subject has been made aware and consented to such sharing, or
- The person receiving the Personal Information has agreed to keep the Personal Information confidential and to use it only for the purpose for which it was shared under an appropriate agreement with Sappi.

17. Cross border transfers of personal information

17.1. Sappi may not transfer Personal Information to another party who is situated outside South Africa, unless:

- The Data Subject has consented thereto, or
- The transfer is necessary in order to perform a contract between Sappi and a Data Subject, or for reasons of public interest, or to establish, exercise or defend legal claims or to protect the vital or legitimate interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent, or

- The country where the Personal Information is being transferred to provides the Data Subject with the same level of protection under the data processing laws applicable in South Africa, or alternatively,
- Sappi has concluded a Personal Information data transfer agreement with the recipient of the Personal Information, which sets out the rules which apply to the receipt and the subsequent Processing of that Personal Information.

17.2. In order to ensure that the above is complied with, Personnel may not transfer Personal Information to areas outside South Africa, unless one of the following controls are in place:

- The Personal Information Regulator has issued an "adequacy decision" confirming that the territory/country where Sappi proposes transferring the Personal Information to has adequate Data Protection laws in place which will afford the Data Subject with the same level of protection as that under POPIA
- The standard Sappi Personal Information data transfer agreement or Operator Agreement/Addendum has been concluded with the recipient of the Personal Information
- The Data Subject has consented to the proposed transfer, having been informed of any potential risks, or
- The transfer is necessary in order to perform a contract between Sappi and a Data Subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject in circumstances where the Data Subject is incapable of giving consent.

18. Direct marketing

18.1. Direct marketing by means of unsolicited electronic communication as detailed in section 69 of POPA is prohibited unless the Data Subject has consented to the receipt of marketing material.

18.2. In order to ensure that direct marketing is undertaken by Sappi in terms of POPIA, Personnel must ensure that:

- Sappi customers, when approached or dealt with for the first time, are given the opportunity to agree or disagree to the receipt of any Sappi direct marketing material and that where consent is granted that the details of the customer are set out under a "consented to " direct marketing data base, and when marketing material is sent to these Data Subjects, that the material houses an "Opt-Out" form, allowing the Data Subject to opt out of any further marketing material should it so elect
- Before direct marketing is sent to a non-customer that such person provides consent thereto in the form of the prescribed "Opt-In" form, available on the Sappi's website
- When marketing material is sent to Data Subjects, who have opted in that the marketing material houses an "Opt-Out" form allowing the Data Subject to opt out of any further marketing material, and
- When a Data Subject exercises their right not to receive direct marketing, in the form of an "Opt-Out" form that such opt out is recorded and given effect to.

19. Reporting personal information breaches

19.1. In the event of a Personal Information breach, Sappi has a duty to give notice of such breach to the POPIA Information Regulator and to the Data Subject(s) whose Personal Information has been compromised or affected as a result of such breach.

19.2. Sappi has put in place appropriate procedures to deal with any Personal Information breach under POPIA and will notify the Information Regulator and/or the Data Subjects, as the case may be, when legally required to do so.

19.3. Personnel have a duty to:

19.3.1. Immediately report through to the Information Officer, any suspected or known Personal Information breach which report must contain the following details:

- Details of the Data Subjects concerned
- Details of the Personal Information records concerned
- The likely cause of and the consequences of the breach, or
- Details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

19.3.2. Keep such information strictly private and confidential, and

19.3.3. Ensure that they do not deal with any persons in relation to the Personal Information breach, noting that only the Information Officer has the right to report any Personal Information breach to the Information Regulator and/or the affected Data Subjects.

20. Data subject rights and requests

20.1. A Data Subject has a number of rights under POPIA in relation to the Processing of his/her/its Personal Information, including the right to:

- Withdraw Consent
- Object to Processing
- Obtain confirmation of Processing and/or access to Personal Information
- Amend, update and delete Personal Information
- Object to direct marketing
- Be notified of a personal information breach, and
- To complain.

20.2. Sappi has developed, implemented certain processes and related forms to give effect to these rights contained in the Processing Notices which can be found on Sappi's website at: https://www.sappi.com/legal-notices.

20.3. Personnel must:

- Familiarise themselves with the Data Subjects' rights, and the related processes and forms which need to be completed in order to give effect to rights, and
- Note that where a Data Subject seeks advice on what Personal Information Sappi holds pertaining to that Data Subject or where the Data Subject is desirous of accessing this Personal Information, that such right be exercised pursuant to the Promotion of Access to Information Act, 2000 ("PAIA") and which request procedure is set out under Sappi's PAIA Manual available on the website.

21. The right to complain

21.1. A Data Subject has to right lodge a complaint with regards to the Processing of Personal Information.

21.2. Should a Data Subject wish to submit a complaint, the Data Subject should complete the prescribed "Personal Information Complaint Form" housed on the Sappi website and thereafter to submit same to the Information Officer.

21.3. On receipt of the complaint, the Information Officer will attempt to resolve the matter, internally and failing resolution will provide the Data Subject with a non-resolution notice.

21.4. If the Information Officer and Data Subject are able to resolve the matter, a record setting out the solution will be compiled, and signed by the parties and any other affected persons provided with details of the resolution.

21.5. Where the parties are unable to resolve the matter, the Data Subject on receipt of the non-resolution notice, will have the right to refer the complaint to the Information Regulator.

22. Governance

22.1. Sappi's appointed Information Officer and Deputy Information Officers are responsible for the following:

- Developing, implementing and overseeing a POPIA Compliance Framework
- Monitoring compliance with this Policy, the various Personal Information Processing procedures and the Data Processing laws
- Providing training and ongoing guidance and advice on Personal Information Processing
- Conducting Personal Information impact assessments when required, including base line risk assessments of all Sappi's Personal Information Processing activities
- Ensuring that all operational and technological Personal Information and data protection standards are in place and are complied with
- Working closely with IT in order to ensure that appropriate technological and operational measures have been implemented to ensure the safety and security of Personal Information stored electronically
- Receiving and considering reports about compliance with all technological and operational data protection standards and protocols
- Be entitled and have authorisation in conjunction with the Sappi HR function, to initiate disciplinary proceedings against Personnel who breach any technological and/or organisational and/or operational data protection standard, rule, custom, instruction, policy, practice and/or protocol (verbal, in writing or otherwise), including this Policy
- Reviewing and approving any contracts or agreements which deviate from the standard documentation
- Attending to requests and queries from Data Subjects, including requests for access to their Personal Information, and
- Liaising with and/or co-operating with any regulators or investigators or officials who may be investigating a Personal Information matter.

22.2. All queries and concerns in relation to the Processing of Personal Information within Sappi operations must be referred to the Information or Deputy Information Officers.

22.3. Sappi's IT department will be responsible for the following:

- Conducting cyber security risk assessments including base line risk assessments on all of Sappi's information technology activities
- Ensuring that adequate and effective IT operational and technological data protection procedures and standards are in place in order to address all IT security risks
- Ensuring that all systems, services and equipment used for Processing and/or storing data adhere to internationally acceptable standards of security and data safeguarding
- Issuing appropriate, clear, and regular rules and directives, whether for Sappi as a whole or a particular part of it, department, person or level of person in relation to any aspect of the Sappi work, including password protocols, data access protocols, levels of persons who enjoy access to certain data sign-on procedures, password safeguarding protocols, sign-on and sign-off procedures, log-on and log-off procedures; the description of accessories, applications and equipment that will or may be used, and/or that may not be used under any circumstances, and the like, and
- Evaluating any third-party services which Sappi is considering or may acquire to Process or store data, eg cloud computing services and ensuring that appropriate and effective operational and technological data protection procedures and standards are in place in order to address all IT security risks which may present themselves in respect of these external service providers.

23. Training

23.1. Sappi will conduct training on this Policy from time to time.

23.2. Personnel must:

- Attend the scheduled and offered training
- Familiarise themselves with this Policy and e Sappi Personal Information Processing policies, procedures and prescribed forms, and
- Ensure that they Process Personal Information in accordance with the Data Processing laws, this Policy, the training, the related policies and procedures and/or any guidelines issued by Sappi from time to time.

24. Non-compliance

24.1. Compliance with this Policy and any related procedures and policies is mandatory.

24.2. Material transgression of this Policy, and related procedures and policies, will be investigated.

24.3. Further information on the relevant Data Protection Laws including POPIA and practical guidance can be found on Sappi's website: https://www.sappi.com/legal-notices.

25. Revision control sheet

Document number	SPOL-030-SL	
Subject	Protection of Personal Information Policy for Sappi Limited and Sappi Southern Africa Limited	
Revision number	**Date**	**Reason for revision**
00	Unknown	Approved and issued.
01	01 July 2021	Approved and issued.
02	31 January 2022	General review.

26. Annexure A: Documents in support of the POPIA Policy

26.1. POPIA Compliance Framework/Manual
26.2. Appointment of Information Officer and Deputy Information Officers
26.3. Personal Information Impact Assessments and data maps (if applicable)
26.4. Processing Notices required under Section 18 of POPIA
26.5. Standard Operator Agreement
26.6. Data Transfer Agreement
26.7. Binding Corporate Rules
26.8. Opt-out and opt-in form
26.9. Withdrawal of consent notice
26.10. Objection notice
26.11. Complaint form
26.12. Update to or correction of Personal Information
26.13. PAIA Manual