

MAHLE Behr South Africa

**PROTECTION OF PERSONAL INFORMATION ACT
(POPIA)**



INDEX

1. Important definitions and POPIA concepts
2. Introduction
3. Right to Privacy
4. Purpose of POPIA
5. Objectives of POPIA
6. Personal Information Impact Assessment
7. Application
8. Exclusions
9. Regulator's power to exempt processing
10. The 8 POPIA principles
11. Processing of special personal information
12. Prior Authorization
13. Protection aims and protection classes
14. Commissioned data processing by third-party operators
15. Selection and monitoring of third-party operators
16. Information Regulator
17. Codes of Conduct
18. Directories
19. Automated decision making
20. Trans border information flows
21. Enforcement and sanctions
22. Data breaches
23. Information officers
24. Policies and documentation in place
25. Processes and procedures
26. Document Approval.

1. IMPORTANT DEFINITIONS AND POPIA CONCEPTS

The Protection of Personal Information Act No. 4 of 2013 POPIA makes use of certain concepts and references, which are considered below, and which once unpacked will allow one to better understand the provisions and application of POPIA.

“Personal Information”

“Personal information” means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, which may be or which is processed, collected, and used by a Responsible Party, in this case Personal Information processed by the employees, and which will include any Personal Information related to or owned by either a private or public entity, such as a company, and/or natural individual, such as an employee, including but not limited to:

- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- (b) information relating to the education or the medical, financial, criminal or employment history of the person; this includes bank account numbers and credit card details.
- (c) any identifying number, symbol, e-mail address, physical address, IP address, telephone number or other assignment to the person;
- (d) the blood type or any other biometric information of the person;
- (e) the personal opinions, views or preferences of the person;
- (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- (g) the views or opinions of another individual of the person.
- (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person

All the details pertaining to THE COMPANY will be known as its Personal Information. In turn, all Personal Information provided to THE COMPANY will equally be referred to as Personal Information. Special Personal information requires extra protection and is defined below:

- Biometric Information such as one’s blood type and fingerprints; and

- Information such as a person's information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of a person.

“Processing”

The word **Processing** includes the collecting, receiving, storing, updating, modifying, disseminating and destruction of **Personal Information**. Importantly, **Processing** will include:

- the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as blocking, degradation, erasure or destruction of information;

“Responsible Party and Data Subject”

The person, legal entity, company or public body (i.e., THE COMPANY and its employee's) who process another's Personal Information is referred to as the **“Responsible Party”**, whereas the individual, legal entity, public body or company, whose information is being processed by THE COMPANY, is referred to as the **“Data Subject”**. **A Joint Responsible Party** exists where the Company and another organization jointly determine the means and purposes for processing personal information.

“Data Subject” therefore means the individual, legal entity, public body or company to whom the **Personal Information** relates.

Following this where THE COMPANY processes Personal Information belonging to a Data Subject, THE COMPANY will be referred to as the Responsible Party.

“Record”

A Record has been defined to mean any recorded Personal Information in any form that is in the possession or control of any Responsible Party (person, legal entity, individual, company or public body) and which pertains to a Data Subject, irrespective of whether the Responsible Party who holds such Records created it and regardless of when the Records came into existence. This means that all “records” housing Personal Information, which THE COMPANY intends to process in the future, will have to be brought in line with the provisions of POPIA.

All documents created by THE COMPANY containing Personal Information will be referred to as Records.

“Legal Basis of processing”

THE COMPANY may only process Personal Information if:

- The Data Subject (or competent person where the Data Subject is a child) has given its consent to the processing. **Consent** has been defined under POPIA to mean a voluntary, specific and informed expression of will in terms of which the Data Subject agrees to the processing of his/her or its Personal Information.
- Processing is necessary to carry out actions for the conclusion or performance of a contract with the Data Subject;
- Processing is necessary to comply with a legal obligation;
- Processing is necessary to protect the legitimate interests of a Data Subject;
- Processing is necessary to pursue the legitimate interests of a Responsible Party or third party;
- Processing is necessary for the proper performance of a public law duty by a public body;

The Responsible Party bears the burden of proof for consent.

“Information Officer” means in the case of a public body, the Information Officer or Deputy Information Officer who has been appointed in terms of POPIA or in the case of a private body, the head of a private body who has been appointed in terms of section 1 of PAIA. THE COMPANY must appoint such a person or person

2. INTRODUCTION

MAHLE Behr South Africa (Pty) Ltd (THE COMPANY) takes the protection of personal information extremely seriously. That is why we process the personal data of our employees, customers and business partners in accordance with the applicable statutory provisions on the protection of personal data and data security.

Effective data protection cannot be achieved through rules and regulations alone. It requires a strong awareness of data protection and security on the part of employees. One aim of this policy is therefore to raise awareness of data protection issues among our employees and

provide them with information and rules. These rules and information are intended to help employees understand the data protection provisions and implement them accordingly. The technical and organizational measures also play an important role in this regard, as they help to ensure that personal data is processed securely and may be subject to documentation obligations in certain countries.

The rules defined in this policy apply to all MAHLE Behr South Africa and all other group companies within the area of application of the South African Protection of Personal Information Act (POPIA) as well as the EU General Data Protection Regulation (GDPR).

Accordingly, these rules apply to the processing of personal data by a MAHLE company with a branch in the EU/EEA, irrespective of whether the processing takes place in the European Union.

These rules also apply to all processing of personal data carried out by MAHLE companies based in foreign countries which carry out these activities within the scope of commissioned data processing in cooperation with another controller/responsible party pursuant for a MAHLE company based in the EU/EEA or where data processing is contractually agreed with such a MAHLE company by means of EU Standard Contractual Clauses in accordance with the GDPR.

- This policy is aimed at all **employees** and concerns their obligations to comply with the regulations defined herein when handling personal data while carrying out their work. "Employees" also include interns, temporary staff and other external employees (consultants, etc.).
- This policy also addresses **managers**, who are required to ensure compliance with data protection within their area of responsibility.
- Under this data protection policy, **Mahle Data Controllers** are responsible for the compliance, implementation and adaptation of the processes for which they are responsible with respect to data protection. They must ensure that the process descriptions are data protection-compliant and are implemented accordingly.
- This policy applies to the **Board of Directors** with respect to its responsibility for the implementation of and compliance with data protection requirements in South Africa.
- The Information Officer and Deputy Information Officers work toward the implementation of the requirements/regulations defined and described in this policy in South Africa.

POPIA came into full force on 1 July 2021.

When looking at POPIA the requirements of other Acts should also be taken into consideration.

If there is a conflict between POPIA and another South African law, POPIA prevails. But if another South African law gives greater protection to personal information, the other law will prevail.

Below are some of the other laws that may impact the POPIA compliance process.

- The Constitution of the Republic of South Africa 1996 (The Constitution). The Constitution enshrines the right of privacy into our law and POPIA gives effect to this.
- King IV. This code requires that all governing bodies must ensure that their organisations are protecting the privacy of personal information.
- The Promotion of Access to Information Act 2 of 2000 (PAIA). POPIA and PAIA hold a special relationship. Both can be seen as "information" laws and are each on one end of a continuum. On the one end, PAIA is an "Access" law, all about freedom of information. POPIA on the other end, is about Privacy – “Prevention of exposure of information”. They shouldn't be seen as competing, both are there to help ensure that information is managed correctly.
- The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA). This regulates the monitoring and interception of communications including electronic communications in South Africa. See the separate IT, social media, Electronic Communication and Data Breach Policy.
- The EU General Data Protection Regulation (GDPR). This is legislation that is aimed at safeguarding a natural person's personal information when it is processed by public and private bodies in all European Union member states as well as entities that offer goods or services to EU citizens.

3. RIGHT TO PRIVACY

POPIA gives effect to the right to privacy, which is protected under section 14 of the Constitution, and which is a well-established concept and right under South African common law.

Section 14 of the **Constitution** states that:

*“Everyone has the right to privacy, which includes the right **not** to have:*

- *their person or home searched.*
- *their property searched.*
- *their possessions seized; or*
- *the privacy of their communications infringed.”*

This Constitution, however, is general and does not specifically apply in a holistic manner to “Personal Information”.

POPIA in contrast, is specifically aimed at protecting any person’s Personal Information from misuse and abuse by another.

4. PURPOSE OF POPIA

POPIA aims to regulate the Processing of Personal Information by both private and public bodies, including the State.

Following this, POPIA aims to regulate the processing of Personal Information by THE COMPANY, which it does daily during the course and scope of its business operations.

POPIA seeks to protect and prevent the abuse and misuse of Personal Information owned by individuals and companies in South Africa, which information is processed by these private and public sectors.

POPIA, however, must not be seen as a law which frustrates the operation of a business and to this end it seeks to create a careful balance between one’s Constitutional right to privacy and the needs and interests of commerce, government, and business.

Following this, when THE COMPANY processes the Personal Information of another, be it an individual or a company, it must ensure that these Personal details are processed for the

purpose for which they were collected, are not distributed to unauthorized parties, and that such information is kept safe and once used, permanently deleted, or destroyed.

5. OBJECTIVES OF POPIA

In essence then, the overarching objectives of POPIA are as follows:

- to give effect to the constitutional right of privacy by safeguarding **Personal Information** (see section 5 below for definitions) when it is processed by a **Responsible Party**, subject to certain limitations to balance the right of privacy against other rights, i.e., the right of access to information and the protection of important interests such as the free flow of trans-border information.
- to regulate the way **Personal Information** may be **Processed**.
- to provide persons with rights and remedies to protect their **Personal Information** from being processed that is not in line with POPIA and hence unlawful.
- to establish voluntary and compulsory measures, including the establishment of an **Information Regulator** (Regulator) to promote and enforce the rights protected by the POPIA.

6. PERSONAL INFORMATION IMPACT ASSESSMENT

POPIA requires a Personal Information Impact Assessment (PIIA) which focuses on situations where there is a high risk to the rights and freedoms of Data Subjects.

7. APPLICATION

POPIA regulates the Processing of Personal Information within South Africa, including the Processing of Personal Information that is entered in a record, by a company, or public body that is domiciled in South Africa, or a public body that is domiciled elsewhere but uses automated or non-automated means situated in South Africa.

POPIA does not distinguish between individuals and legal entities whereas the GDPR applies only to individual persons.

POPIA will therefore apply to various parties, including individuals, legal entities, such as a public and/or private body and to all information belonging to legal entities, including private and public bodies and/or individuals.

Following this, POPIA will apply to THE COMPANY when it and/or its employees process

Personal Information of Data Subjects, including its employees and third parties.

THE COMPANY must ensure that all such processing is done in accordance with the provisions of POPIA and the 8 core Data Privacy principles and conditions.

8. EXCLUSIONS

POPIA will not apply to the following types of processing and / or categories of Personal Information:

- Processing carried out by an individual during a purely personal or household activity.
- de-identified information.
- personal information held or used by or for the State or its various bodies, which is used for the purposes of achieving national security, defence, public safety, or the prevention of crime.
- personal information held or used by journalists and printed in the media so long as such information is used exclusively for journalistic purposes by media companies and which journalists are subject to a code of ethics that has safeguards for the protection of this personal information.
- personal information held or used by Cabinet, Provincial Executive Councils and Municipal Councils.
- personal information held or used by the judiciary if it relates to the exercise of judicial functions.
- personal information which has been specifically exempted under POPIA.
- personal information, which is protected and governed by other legislation, which to a higher standard regulates the Processing of personal information.

None of the abovementioned exclusions will apply to THE COMPANY, save where it has been granted an exemption from the Act.

9. REGULATOR'S POWER TO EXEMPT PROCESSING

In terms of section 37 of POPIA, the Information Regulator (Regulator) appointed under POPIA may on application grant any person an exemption from the Act which exemption authorizes a Responsible Party to process Personal Information even where it would be in breach of any condition housed under POPIA. The exemption however will only be granted

when the Regulator is satisfied that in the circumstances the public interest outweighs, to a substantial degree, any possible interference with privacy or such processing Involves a clear benefit to the Data Subject or third party that substantially outweighs any interference with privacy.

The “public interest” includes:

- the interests of State security.
- the prevention, detection and prosecution of criminal offences.
- important economic and financial interests of the State and other public bodies; or
- scientific research and government statistics.

The Regulator must publish any exemption in the Government Gazette.

10. THE 8 POPIA PRINCIPLES

PRINCIPLE 1: ACCOUNTABILITY

When THE COMPANY processes any Personal Information, it must ensure that all the provisions housed under POPIA are always complied with. This means in a lawful and reasonable manner that does not infringe the privacy of the Data Subject.

These provisions may not be waived or contracted out of. Accountability compliance with POPIA will commence from the time when the Personal Information is received or requested by THE COMPANY, the purpose for the processing determined and will thereafter apply throughout the lifecycle of the processing, including whilst being processed by third party operators until the record housing the Personal Information has been de-identified so that it can never be re-identified.

EXAMPLE: There is a data breach by a Third -Party Operator who processes PI on behalf of THE COMPANY. Who is accountable and what actions having the COMPANY taken to prevent or mitigate the effects of such breaches?

ACTION TAKEN: (EXAMPLE)

The CEO is **accountable** to the Regulator and the relevant Data Subject for compliance from “cradle to grave”. He/she is also the Information Officer as laid down by POPIA. Accountability can never be delegated but day-to-day responsibility for POPIA has been delegated to the Deputy Information Officer.

All Third-Party Operators have signed or have had their attention drawn to the Third-Party Operator Agreement which requires the latter to have in place legal, technical and organizational measures as required by POPIA and which also indemnifies THE COMPANY for any damage suffered by it because of a commission or omission by the Third-Party Operator. The CEO remains accountable, but the Agreement requires a comparable level of protection from the Third Party and transfers responsibility to them allowing for a right of redress.

The Company POPIA Notice is available via the website, email disclaimers and in various documentation used or sent to staff, third party operators and customers.

A data breach response plan has been drawn up.

PRINCIPLE 2: PROCESSING LIMITATION

POPIA contains several conditions and limitations on how Personal Information may be processed which are set out under the subject headings below.

Processing must be lawful, purpose specific and not excessive

Lawful

THE COMPANY may only process Personal Information lawfully and in a reasonable manner which does not infringe on the Data Subject’s rights to privacy.

Not excessive

THE COMPANY may only process Personal Information, **if given the purpose**; it is adequate, relevant and not excessive.

Permission

THE COMPANY may only process Personal Information if:

- the Data Subject (or competent person where the Data Subject is a child) has given its **consent** to the processing.
- in the **absence of consent**, processing is necessary to carry out actions for the conclusion or performance of a contract with the Data Subject.
- Processing is necessary to comply with a legal obligation.
- Processing is necessary to protect the legitimate interests of a Data Subject.
- Processing is necessary to pursue the legitimate interests of a Responsible Party or third party.
- Processing is necessary for the proper performance of a public law duty by a public body.

The Responsible Party bears the burden of proof for consent.

Withdrawal of permission

The Data Subject can withdraw his/her or its consent at any time; however, such withdrawal will not affect the lawfulness of the processing of the Personal Information that has been processed before the withdrawal.

Right to object

The Data Subject can object at any time to the processing of Personal Information unless legislation provides for the processing.

Manner of collection

Personal Information must be collected **directly** from the Data Subject, unless:

- the information is obtained from a public record or has deliberately been made public by the Data Subject.
- the Data Subject consented or allowed the Personal Information to be collected from another person.
- the processing and collection by a 3rd party does not prejudice the legitimate interest of the Data Subject.

- the collection is necessary to comply with a legal obligation.
- collection from another source is necessary to avoid prejudice to the maintenance of the law or comply with an obligation imposed by law.
- for the conduct of proceedings in a court or tribunal that have commenced or are reasonably contemplated.
- in the interests of national security.
- to maintain the legitimate interests of the responsible party or of a third party to whom information is supplied.
- compliance with this principle would prejudice a lawful purpose of the collection.
- compliance with this principle is not reasonably practical in the circumstances of a particular case.

EXAMPLE: Image- and Video recordings of Employees. The purpose of the data processing is an HR campaign by MAHLE on the topic of "Diversity in the workplace".

ACTION TAKEN: The Controller (MAHLE) has to inform the data subjects before the image- and video recordings are started. The Controller (MAHLE) must ask every employee for consent before the image- and video recordings are started.

PRINCIPLE 3: PURPOSE SPECIFICATION

Personal Information must be collected for a specific, explicitly defined and lawful purpose which purpose must be related to a function or activity of the Responsible Party.

The Data Subject must be made aware/informed of the purpose for the processing and/or why the Personal Information is required.

Subject to certain exceptions, the retention of Personal Information must not be for a period longer than necessary to achieve the purpose for which such Personal Information was collected or processed. Thereafter it must be de-identified so that it can never be re-identified.

Notwithstanding the above, the retention of processed Personal Information can be retained for a period longer than the actual purposes provided that the following conditions can be shown:

- that the required retention period is prescribed and/or authorized by law.

- prolonged retention is reasonably required for a specific lawful purpose.
- prolonged retention is required due to contractual requirements as between the parties.
- the Data Subject (or competent person on behalf of a child) has consented to the further retention of the record.

Furthermore, records of Personal Information may not be kept more than a period longer than necessary to achieve the purpose for which it was collected or processed, or if it is for historical, statistical or research purposes, and the Responsible Party has established appropriate safeguards.

This should all be set out under a **consent document**.

EXAMPLE: Retention of Past Employees Medical and Safety Records.

ACTION TAKEN: Retention of Past Employee’s Medical and Safety Records is legal requirement. The controller (MAHLE) must define the purpose of this processing activity concretely according to the legal requirement. A processing of the Past Employee Medical and Safety Records for another purpose like e.g. performance evaluation of employees is not allowed.

PRINCIPLE 4: FURTHER PROCESSING LIMITATION

If Personal Information or a record must be used or processed further such ***further processing*** must be in accordance with or be compatible with the original purpose for which the Personal Information was collected. Examples of situations where Personal information may be disclosed in compliance with this principle include the following:

- any supervisory or complaints body to whom a complaint has been made.

An example of where further processing is not permitted without consent is where THE COMPANY wishes to pass on personal information to another of its customers. e.g., to facilitate further business activities.

Where *further processing* of Personal Information takes place, which is not compatible with the original purpose, it will only be allowed where:

- the Data Subject has given his, her or its consent to such incompatible further processing.

- the Personal Information which is subject to any such further processing was derived from a public record or which was deliberately made public by the Data Subject.
- further processing is necessary to comply with a legal obligation or legislation.
- further processing is necessary to avoid serious harm or imminent threat to public health or safety.
- the Personal Data is to be used for historical, statistical or research purposes, and the Responsible Party can ensure that the further Processing will be carried out solely for this purpose and that it will not publish the information in an identified form; or
- further processing is in accordance with an exemption granted by the Regulator.

EXAMPLE: THE Company wants to share the Data subject's information with other Retirement fund organizations in South Africa.

ACTION TAKEN: That processing isn't permitted without the explicit consent of the client as the purpose isn't compatible with the original purpose for which the information was processed.

PRINCIPLE 5: INFORMATION QUALITY

THE COMPANY must ensure that the Personal Information processed is correct, accurate, not misleading and reliable and must ensure that such data is kept complete and up to date in accordance with the provisions of the Protection of Personal Information Act.

- THE COMPANY must correct any factually inaccurate personal information including where this is identified by the data subject to be the case in a verifiable way.

THE COMPANY must have appropriate procedures in place to check the accuracy of information following its entry.

EXAMPLE: A customer changes his contact details and does not advise THE COMPANY.

ACTION TAKEN: PI that is subject to change (addresses etc.) must be verified with the Data Subject. E.g., a via a regular PI update request.

TP operator contracts require them to advise THE COMPANY of any changes.

Staff are required, in terms of the Staff Privacy to Policy advise HR when their OPI changes

Data Subjects are told that he/she /it has a right to update and or correct their Personal Information.

This is all set out in the consent document which is provided to the Data Subject when THE COMPANY is processing the Personal Information.

Duplication of collection of data is minimized and it is stored in a secure database.

PRINCIPLE 6: OPENNESS

Any processing of Personal Information must be done in a transparent and open manner.

THE COMPANY in this regard must take reasonable steps to ensure that the Data Subject is made aware of the type of Personal Information being collected, the purpose for which it is being collected, and if not collected directly from the Data Subject the source from where the Personal Information is or will be collected.

Information which must be disclosed

When processing Personal Information, THE COMPANY must record and provide the following details to the Data Subject:

- its name and address.
- the purpose of the collection and what the Personal Information will be used for.
- whether the supply of the Personal Information by the Data Subject is voluntary or mandatory.
- the consequences of any failure to provide Personal Information.
- if there is any law that requires or authorizes the requirement of Personal Information.
- if the Personal Information is to be transferred to another country.

- nature or category, recipient of the Personal Information.
- whether subsequent processing will occur.

This is set out under a “Section 18 Consent Document” which is attached as an annexure.

Time of notification

This action must be performed before collection of the Personal Information unless the Data Subject is already aware of these details and in any other case, as soon as reasonably practicable after the Personal Information has been collected.

Subsequent and repeated Processing

If Personal Information of the same type for a similar or the same purpose is subsequently collected, it will be taken that the Responsible Party has complied with the above requirements. In other words, the above steps will not have to be repeated where the same Personal Information is collected on a subsequent occasion.

Exceptions

It will not be necessary to comply with the above disclosure provisions and requirements were

- Data Subject has agreed that THE COMPANY does not have to comply- i.e., Data Subject has provided his/her or its consent for non-compliance.
- Non-compliance with the provisions will not prejudice the Data Subject.
- Non-compliance with the provisions is necessary to comply with an obligation in terms of the law.

EXAMPLE: An employee wants to know exactly how his/her PI is being used.

ACTION TAKEN: This is contained in the Staff Privacy Policy. (TO BE DRAFTED).

PRINCIPLE 7: SECURITY SAFEGUARDS

Safe and secure

All records housing Personal Information and held by THE COMPANY must be kept safe and secure.

Following this THE COMPANY must ensure the integrity and confidentiality of all Personal Information under its control, by taking appropriate and reasonable technological measures. These measures will be employed to prevent loss, damage, destruction and /or unlawful access to said data.

Measures to secure

THE COMPANY is obliged to take the following reasonable measures to ensure the safety and integrity of Personal Information under its control:

- identify all reasonably foreseeable internal and external risks.
- establish appropriate safeguards.
- regularly verify that safeguards are effectively implemented; and
- ensure that the safeguards are continually updated.
- THE COMPANY, when implementing these safeguards, must have due regard for generally accepted information security practices and procedures. Ensure that:
 - Appropriate procedures are in place in relation to back-up of data.
- Focus is placed on the security of personal data held on portable devices, with appropriate security measures such as encryption applied.
- Robust procedures for limiting access to personal data are in place and that staff are aware of these limits.
- An appropriate procedure is in place to ensure that only the data subject or their clearly chosen representative has access to their personal data.
- A confidentiality policy is in place pertaining to the collection, processing, keeping and use of health and other special personal Information.
- Access to special personal information sensitive data is restricted to authorised staff. It is expected that access to sensitive personal information should be restricted to HR staff needing to access a particular file as part of their role.
- An appropriate IT, social media, Electronic Communications and Data Breach policy is in place.

Duties of service providers and third-party operators

Where THE COMPANY uses the services of a third party known as an “**Operator**” to process Personal Information, on its behalf, THE COMPANY must conclude a written contract with the

Operator which gives the Operator a clear mandate on what it is required to do with the data, and which sets out that such Operator must before such processing:

- ensure that it has established and maintains the security measures required under POPIA.
- inform the Data Subject that it is processing the Data Subject's Personal Information on behalf of THE COMPANY.
- treat the Personal Information as confidential and not disclose it unless required by law or during the proper performance of its duties.

In addition, although not required expressly by POPIA, any contract between THE COMPANY and its Operator should include

- an undertaking by the Operator that will comply with all the provisions pertaining to the processing of Personal Information as housed under POPIA.
- a suitably worded indemnity in favor of THE COMPANY, in the event of a breach by the Operator.

Notification of security compromises

THE COMPANY has a duty to notify the Regulator and the Data Subject, unless the identity of the Data Subject cannot be established when it becomes aware of, or where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by an unauthorized person.

Time of notification

Notification must take place, as soon as reasonably possible, unless a public body is responsible for the prevention, detection or investigation of offences, or the Regulator determines that notification will impede a criminal investigation.

Manner

THE COMPANY must notify the Data Subject in writing of the compromise, which document must be either.

- mailed,

- e-mailed,
- placed on a prominent position on THE COMPANY website; or
- published in the media.

The written notice must provide sufficient information to allow the Data Subject to take protective measures against any potential consequences of the leak or infringement.

In addition to the above, under certain circumstances, the Regulator may issue a directive to THE COMPANY compelling it to publicize in a public manner any such compromise or security leak and/ or breach.

EXAMPLE: A data breach occurs resulting in the contact details belonging to a senior member of staff of a customer being compromised. The customer wants to know how this happened and what measures are being put into place to prevent a re-occurrence.

ACTION TAKEN: (EXAMPLE ONLY)

Procedures where PI is processed have been mapped to understand how, where, what, when, who by and why it is used.

A risk assessment has been completed and remedial action has been taken or is underway.

There is a Data Breach policy in place, and this has been/will be activated to find out what happened.

Where THE COMPANY uses Service Providers (Operators) to process a Data Subject's Personal Information, it has concluded written contracts with these Operators, which ensures that they establish and maintain the security measures required under POPIA. and which contract houses, in the event of a breach by the Operator, a suitably worded indemnity in favour of THE COMPANY.

Legal, technical and organizational measures are in place or are being put into place to prevent loss, damage or destruction or unlawful access to these records. These will include the correct identification of the records and their classification.

PRINCIPLE 8: DATA SUBJECT PARTICIPATION

PI is effectively on loan to THE COMPANY. An individual has a right to find out, free of charge, if an organization holds personal information about them. The individual also has a right to be given a description of the information held about them and to be told the

purpose(s) for holding their information.

Manner of Request

The application must be done by contacting the Deputy Information Officer as per the standard process used for access to company information as provided by the Promotion of Personal Information Act (PAIA).

The Data subject must provide adequate proof of is, her or its identity, and provided such request is made using the process set out under THE COMPANY's PAIA Manual, enquire, free of charge:

- whether his, her or its Personal Information is being or has been processed by THE COMPANY.
- where the Personal Information or any records pertaining thereto are being safely held; and
- what has been done with the Personal Information, and who has been given access thereto.

This request and any request for a copy of the record or description of the Personal Information being held must be provided:

- within a reasonable time.
- at a prescribed fee, where copies of the documents have been requested.
- in a reasonable manner and format; and
- in a form that is generally understandable.

In other words, any request for access to a record or related Personal Information must be made by the Data Subject in the manner provided for under sections 18 and 53 of PAIA, read together with and as set out under THE COMPANY's PAIA Manual.

Processing Fee

If a processing fee is requested by THE COMPANY for it to respond to a request, then the Data Subject must be given a written estimate of the fees and where applicable any required deposit.

Request Refusal

Where a Data Subject has requested access to information which the Responsible Party does not have to release, due to the defenses or rights to refuse access to data, as housed under PAIA, then in such an event, where applicable, the Responsible Party must refuse access to the record on such grounds.

If only parts of a record are subject to grounds for refusal, then the remainder of the record must be provided.

Correction of personal information

At any time after the Processing of Personal Information has taken place, a Data Subject may, in the prescribed manner, request the Responsible Party to:

- correct or delete any of his/her or its Personal Information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
- destroy or delete a Record that the Responsible Party is no longer authorized to obtain.

Upon receipt of such a request the responsible party must:

- correct the information
- destroy or delete the information
- provide credible evidence in support of the information, to the satisfaction of the Data Subject; or
- where agreement cannot be reached, attach a notification to the information that a correction was requested but not made.

On receipt of a request for changes and after they have been affected, the Responsible Party must inform where reasonably practicable all applicable persons or bodies of the especially where the amendments will have an impact on decisions taken in respect of the Data Subject.

EXAMPLE: A Data Subject (staff, supplier or customer) requests details of all her/his PI in the possession of THE COMPANY.

ACTION TAKEN: The PAIA Manual held by THE COMPANY and published on the website makes specific mention to the rights of a Data Subject to request his or her Personal Information and related records, and sets out the procedure, which should be followed by such Data Subject, should he, she or it require access to this information.

11. PROCESSING OF SPECIAL PERSONAL INFORMATION

There is a general section housed under POPIA, which prohibits the processing of “Special Personal Information”, save where special circumstances can be shown which justifies the need to process this Special Personal Information.

Types of Special Personal Information

The processing of the following **Special Personal Information** is prohibited, subject to certain exceptions. SPI processed is highlighted below and consent is obtained therefore:

- religious or philosophical beliefs.
- **race or ethnic origin, (Employment Equity returns);**
- trade union membership.
- political persuasion.
- **health or sex life; (medical aid purposes).**
- **biometric information; (entry to Company premises).**
- **criminal behavior. (Employment purposes).**

Exceptions

Notwithstanding the above prohibition, POPIA will allow THE COMPANY to process Special Personal Information if:

- it is carried out with consent of the Data Subject.
- is necessary for the establishment, exercise or defense of a right or obligation in terms of a law.

- is necessary to comply with an obligation of international public law.
- is for historical, statistical or research purposes and THE COMPANY can guarantee that it is for public interest and will be safeguarded.
- the information has been deliberately made public; and/or
- specific reasons for the processing can be shown.

Note: The last point concerns specific justifications which are addressed and detailed under certain sections of POPIA, and which will not be discussed for the purpose of this manual.

EXAMPLE: The processing of Biometric information (e.g., fingerprint mapping) for a specific purpose - i.e., to facilitate the wages /salaries payroll process.

ACTION TAKEN: Provide the Data Subjects with reasons for processing of Biometric information to obtain the necessary consent for processing the Data Subjects S.P.I.

12. PRIOR AUTHORIZATION AND NOTIFICATION TO THE REGULATOR

Where certain special Personal Information is processed, and before the processing takes place, THE COMPANY must notify and obtain permission from the Regulator to legally process such information.

In this regard THE COMPANY must obtain prior authorization from the Regulator prior to any processing if THE COMPANY plans to—

- Process any unique identifiers of Data Subjects for a purpose other than the one for which the identifier was specifically intended at collection; and with the aim of linking the information together with information processed by other Responsible Parties. This applies to such as Credit Bureaux. It is unlikely that this section of the Act will ever apply to THE COMPANY.
- Process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties.
- Transfer special Personal Information to a third party in a foreign country that does not provide an adequate level of protection for the processing of Personal Information; or

- Transfer the Personal Information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

The provisions above may be applied by the Regulator to other types of information processing by law or regulation if such processing carries a particular risk for the legitimate interests of the Data Subject.

A Responsible Party must obtain prior authorization as referred to above only once and not each time that Personal Information is received or processed, except where the processing departs from that which has been authorised.

The reader should note that this requirement to notify will not apply if a Code of Conduct has been issued and has come into force in a specific sector or sector of society. No such code is in existence for the sector.

ACTION TAKEN

This task forms part of the duties of the Information Officer or Deputy Information Officer's and details are contained in the duties of the DIO.

13. PROTECTION AIMS AND PROTECTION CLASSES

The most important protection aims are confidentiality, integrity and availability.

- Confidentiality: Data must be protected against unauthorized access. Data is made accessible only to selected groups of persons. It must therefore be ensured through various protective measures that unauthorized third parties are not able to gain access to this data.
- Integrity: Data must remain intact, complete and up to date during processing. The loss of integrity can have serious consequences, such as a disruption to operations. To prevent this, various procedures/precautions must be implemented (e.g., password protection, authorization system). The integrity of the data must be verifiable.
- Availability: Data must be available and able to be duly always processed.

The classification of data processing procedures is based on the data being processed. The sensitivity of personal **data** in terms of data protection is determined by assessing the extent to which a personal data breach would, or may, violate or restrict the data subject's personal rights or harm their personal or professional reputation (**assessment criterion**). The MAHLE Group uses the following classification levels (CL):

- CL1 – MAHLE public:

This level is to be used for freely accessible data. This data may be viewed without the person accessing the data having to assert a legitimate interest, e.g., data that the controller publishes online or in brochures or in publicly accessible records.

- _CL2 – MAHLE internal:

This level is to be used for personal data that, if misused, is not anticipated to have any negative consequences, but access is nevertheless tied to a legitimate interest on the part of the person viewing the data, e.g., internal direct dial numbers, internal responsibilities.

- _CL3 – MAHLE confidential:

This level is to be used for personal data that, if misused, may have a negative impact on the data subject's social status or financial situation (keyword: damage to reputation), e.g., data about contractual relationships, amount of income, any social benefits, administrative offenses.

- _CL4 – MAHLE strictly confidential:

This level is to be used for personal data that, if misused, may have a (significant) negative impact on the data subject's social status, financial situation (keyword: social existence) or health, life or freedom (keyword: physical existence), e.g., institutionalization, criminality, professional assessments, psychological/medical examination results, debt, seizure, insolvency, addresses of people who could be a possible victim of a crime.

14. COMMISSIONED DATA PROCESSING BY THIRD-PARTY OPERATORS

If external service providers are to be commissioned to carry out the processing of personal data, individual processing steps (e.g., collection, erasure = disposal) or activities (e.g., maintenance, repair) during which they have an opportunity to process personal data, data protection advice must be sought prior to the assignment being made, supported by the draft contract and the criteria of the contract control measures taken or planned. In the case of data transmission to a third country, the provisions of the section "Data transmission and processing in the group and/or third countries" must be observed.

15. SELECTION AND MONITORING OF THIRD-PARTY OPERATORS

When selecting contractors for commissioned data processing, it is critical to conclude a Third-Party Operator Agreement and to check whether the Operator provides sufficient guarantees

for the protection of the rights of data subjects by means of technical and organizational measures. Appropriate steps must be taken to check the technical and organizational measures implemented.

16. INFORMATION REGULATOR

POPIA makes provision for the appointment of an Information Regulator who will be responsible for the administration of POPIA. This person has been appointed.

17. CODES OF CONDUCT

The Regulator and or any Industry may of its own volition issue a code of conduct, which will set out how it processes and deals with Personal Information, and any disputes relating thereto

18. DIRECTORIES

A Data Subject who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his, her or its Personal Information is included must be informed, free of charge and before the information is included in the directory:

- about the purpose of the directory; and
- the various uses of such directory.

The Data Subject must be given a reasonable opportunity to object, free of charge, in a manner which is free of unnecessary formality to the use of his/her Personal Information in such directories.

ACTION:

Published for interest.

19. AUTOMATED DECISION MAKING

A Data Subject may not be subject to a decision which results in legal consequences for him/her, or which affects him/her or it to a substantial degree, and which decision is based solely since the automated Processing of Personal Information, and which is intended to provide a profile of such person on his/ her or its:

- performance at work.
- credit worthiness.
- reliability.
- location.
- health.
- personal preference and conduct.

Exclusions

The above provisions will not however apply if the decision has been taken in connection with the conclusion of a contract, and the request of the Data Subject in terms of the contract has been met or appropriate measures have been taken to protect the Data Subject's legitimate interest or the decision is governed by a law or a code of conduct.

In this regard, before any decision or conclusion or agreement is made or reached, appropriate measures must be in place allowing the Data Subject with:

- an opportunity to make representations about the decision; and/or
- sufficient information about the underlying logic of the automated processing to enable representations to be made.

EXAMPLE: The Data subject has just been employed within the Finance Department, hence the necessary check for credit credentials will be executed. The results of the Data Subject's credit report were unfavorable.

ACTION TAKEN: Data Subject has the right to be informed about the negative results and an opportunity to make representation before any conclusion is reached by the employer.

20. TRANS BORDER INFORMATION FLOWS

- POPIA will apply to any Personal Information processed in South Africa and to any such Personal Information or Record, which is then, is conveyed across our borders to another country for storage and/or for further processing purposes. Before Personal Information is transferred to a third party in a foreign country, one of the following conditions must be met:

- the third party who is the recipient of the Personal Information must have in place in such country where he or she or it is located, similar Personal Information protection laws or principles, or binding corporate rules, binding agreements or a memorandum of understandings which have been entered into between two or more public bodies, in such country and which provide for an adequate level of protection, as housed under POPIA.
- where this protection is not possible, then in such case.
 - the Data Subject must have consented to the transfer of the Personal Information and Records.
 - The transfer is necessary for the performance of a contract between Data Subject and THE COMPANY.
 - The transfer is necessary for performance of pre-contractual measures at Data Subject's request.
 - The transfer must be necessary and for the benefit of the Data Subject and it is not reasonably practicable to obtain consent, or if it were the Data Subject would most likely grant consent.

The European General Data Protection Regulation (GDPR) came into force in May 2018. The primary objective of the GDPR is to protect data subjects' fundamental rights in their data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Other statutes apply in various countries.

This will apply worldwide to any processing of the Personal Information of data subjects in the EU, where that processing is either related to the offering of goods or services (including those that are free) to the data subjects in the EU, or where the behaviour of the EU data subjects is monitored. This extended territorial reach affects every entity and individual doing business with the EU, even if they operate from a non-EU country. This includes everyone who operates a website accessible from the EU, as this is considered as a free electronic service. The collection of IP addresses in access logs, or the tracking of visitors using cookies, java script or similar technologies also triggers the application of the GDPR law. The same situation applies in reverse. POPIA not only regulates information held in South Africa. It also seeks to regulate the transfer of Personal Information to parties situated outside South Africa.

GDPR is a 'principles'-based regulation. The GDPR outlines a broad set of principles of conduct. If applicable, companies must decide on how to implement them.

The legislation stipulates a new approach for organisations (data controllers or processor) based upon 'data privacy by design'. This means that each service or business process that makes use of personal data should take the protection of that data into consideration upon the design thereof. The use or consumption of personal data should only be used when necessary to facilitate a specific purpose.

In addition to the above, GDPR includes a concept of "data portability" which provides data subjects with the right to request that their data be made available electronically so it can be transported from one organization to another. This data needs to comply with an open standard electronic format to facilitate the transfer of the information.

The GDPR authorizes the imposition of potentially very large penalties for violations. Sanctions that could be imposed include a warning in writing for the first infringement, regular data protection audits and lastly a fine of up to 20 000 000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.

EXAMPLE: A customer asks if any of his\her personal information is transferred offshore for storage purposes.

ACTION: In such an event this is permitted if there is a suitable contract between MAHLE Behr and the third-party operator.

21. ENFORCEMENT AND SANCTIONS

The Regulator is tasked with ensuring that POPIA is complied with, including receiving reports of non-compliance and conducting investigations.

Reports and Investigation

On receipt of information regarding non-compliance, the Regulator will then:

1. Conduct a pre-investigation.
2. Act as conciliator.
3. Dismiss the complaint.
4. Conduct full investigation.
5. Refer the matter to an enforcement process.

Enforcement notice

The Regulator has the right to issue and serve on a person who is not complying with POPIA, an enforcement notice requiring the Responsible Party to:

- take specified steps to comply with POPIA; or
- to stop Processing Personal Information specified in the notice.

In the event of the party not complying with the notice, the Regulator will issue an infringement notice with required information including a request that the Tribunal hands down and levies a penalty.

Penalties

Where a person does not comply with an infringement notice, he may be issued with an administrative penalty of up to R10 million.

Criminal liability

Certain criminal offences have been created under POPIA, such as refusing to comply with an order, such as a search warrant, giving incorrect or refusing to give information and breach of confidence.

Conviction could lead to Imprisonment for a period not exceeding 10 years or to a fine or both fine and imprisonment.

Civil remedies

The Data Subject or the Regulator, upon request of the Data Subject, may institute a civil claim for damages where non-compliance with POPIA can be shown and regardless of intention or negligence on the part of the person who has not complied with the Act.

22. DATA BREACHES

In the event of a potential personal data breach, particularly in the event of a loss of confidentiality due to unauthorized disclosure or data transmission, unauthorized access or processing, or the loss, destruction or falsification of data, the person responsible for data protection must be informed immediately. Corporate Data Privacy must also be informed in the event of reportable data breaches. Regarding the procedure for handling data breaches, the Policy for Information Technology social media, Electronic Communications and Data Breaches must be accessed, and the relevant section utilized.

23. INFORMATION OFFICERS

To ensure that POPIA is being complied with, THE COMPANY Information Officer, by default the CEO, will oversee and will ensure that THE COMPANY complies in all respects with the Act, which duties will include:

- providing training and advice.
- dealing with requests made in terms of POPIA and/or PAIA; and
- working with the Regulator in terms of investigation.

In turn the Information Officer may, if required, appoint Deputy Information Officer(s).

The Information Officers must be registered with the Regulator.

ACTION TAKEN

THE COMPANY will appoint 2 Deputy Information Officers to monitor and control compliance with POPIA and PAIA.

24. POLICIES AND DOCUMENTATION IN PLACE (SAMPLE ONLY)

The following policies and documents relating to the implementation of POPIA exist:

- POPIA Notice
- Compliance Risk Management Plan (CRMP).
- Protection of Personal Information and Privacy Notice.
- Policy for Information Technology, social media, Electronic Communications and Data Breaches.
- Policy for Document Retention and Records Management.
- Personal Data Classification Schedule.
- Data Flow Audit Report:
- Physical Access Control Policy.
- Policy for Complaints Management.
- The Promotion of Access to Information Act Manual.
- Policy for Customers: Informed Consent.
- Contract for Operators who Process Personal Information. Short and long formats.
- Joint Responsible Party Contract.
- Privacy Policy and Consent Declaration for Employees.
- Addendum of Service Agreement for Employees

Summaries of each policy and document are set out below.

POPIA Notice

This sets out the General principles of POPIA and is available on the Company website and other places

Compliance Risk Management Plan (CRMP)

The CRMP contains a register of legal and other requirements. It lists the regulator in charge of POPIA, a summary of the law and related requirements, those policies and controls which should be in place, the actual policies and controls that are in place, which department or person within THE COMPANY is responsible for POPIA and the status and due date of any corrective action that might be required.

Protection of Personal Information and Privacy Notice

This policy is to be posted on THE COMPANY website and must be referenced in any communication to customers. Its purpose is to advise customers and potential customers of THE COMPANY of the principles surrounding POPIA relating to the definition of personal information and what is done with such information. It also touches on the security measures in place and the customer's rights to access their personal information.

Policy for Information Technology social media, Electronic Communications and Data Breaches.

This document is central to POPIA and controls various other issues such as overall IT governance including the security of passwords, the usage of social media and the internet, a data recovery and recall procedure, the email policy and email disclaimers as well as the methodology surrounding the use of phones faxes and the like. This policy needs to be tailored to suit Company needs.

It is recommended that all employees study this policy carefully as compliance therewith will form part of their employment contracts.

Policy for Document Retention and Records Management

In terms of POPIA THE COMPANY has a duty to retain personal information for no longer than is necessary. Some instances relating to the retention of personal information are subject to various laws and this policy sets out the framework for this. It also provides a schedule of statutory retention periods.

Personal Data Classification Schedule

Following on from the above this sheet contains details of each type of document kept by THE COMPANY and which contains personal information. It lists by department the purpose of each document and how the information contained therein is used and managed.

Physical Control Access Policy

To monitor and control visitors to Company Offices.

Policy for Complaints Management.

POPIA requires data subjects to be able to complain if they believe their personal information is not being handled correctly. The complaints policy has been developed to cater not only for this but also to all other complaints that THE COMPANY may receive regarding its services.

Promotion of Access to Information Act Policy

This policy must be read in conjunction with the complaints policy. It provides procedures for third parties to apply for access to information held by THE COMPANY.

Policy for Customers: Informed Consent

This covers situations where consent is required to process the personal information of customers.

Contract for Operators who Process Personal Information (short form and long form contracts exist).

Third party operators such as accountants and service providers such as benefits administrators who handle personal information on behalf of THE COMPANY are required to enter into an agreement with THE COMPANY whereby, they contract to adhere to POPIA principles.

Joint Responsible Party Contract

This is used where both PFK and another party jointly process personal information.

Privacy Policy and Consent Declaration for Employees

Employees are also protected by POPIA and this policy notes how their personal information

is used by THE COMPANY and what rights are available to staff members. Prospective employees are covered, and it applies to previous employees insofar as their personal information is kept by THE COMPANY after them leaving. For example, payrolls are required by law to be kept for 7 years.

Addendum of Service Agreement for Employees

This agreement incorporates the provisions of POPIA into the staff conditions of service.


25. PROCESSES AND PROCEDURES

To comply with POPIA as well as general internal efficiencies, internal processes and procedures to ensure that all the rights and obligations of THE COMPANY, its staff, customers and third-party operators have been reviewed and incorporated in a Data Classification and Identification Schedule and in Data Flow Audit Reports.

26. DOCUMENT APPROVAL



Alex Holmes.
Managing Director.



Dashani Pillay.
Head Of Human Resources.

Checked by:	Janine Naidoo	Data Protection Coordination MBZA
Checked by:	Marven Wurm	Corporate Data Privacy
Authored by:	Dashani Pillay	Naresh Maharaj