51 DURBAN STREET, CITY & SUBURBAN
JOHANNESBURG, 2001
TEL: +27 11 334-8744
gap@ftgap.co.za

PLASTIC INJECTION MOULDERS

PRODUCT DESIGN & TOOLROOM FACILITIES

POPIA MANUAL (including Procedures)

Subject: Data Protection and Information Sharing

Functional Area: GA Plastics (Pty) Ltd and Ferall Tools (Pty) Ltd, ("THE COMPANIES")

Purpose: To guide The Companies in ensuring confidentiality and security of information in compliance with the Protection of Personal Information Act, 2013 (POPIA)

Authority: Directors

Responsibility: Information Officer

Applicable to All Staff

Effective date: 30 June 2021

---

1. INTRODUCTION

This Manual should be read and used in conjunction with the Data Protection and Information Sharing Policy.

The Companies collects and uses (processes) different types of personal information of the individuals and entities (data subjects) with whom it engages in order to operate effectively. This includes employees, clients, contractors, suppliers and possibly other data subjects.

The Companies is committed to protecting the privacy of data subjects and ensuring that personal information is used appropriately, transparently, securely and in accordance with applicable laws.

2. PROCESSING OF PERSONAL INFORMATION

The Companies will only process Personal Information in accordance with the procedures as set out in ANNEXURE A hereof.

2.1 Purpose of Processing

The Companies uses the Personal Information it collects for the following purposes:

2.1.1 Administration of agreements
2.1.2 Staff administration
2.1.3 Keeping of accounts and records
2.1.4 Providing services to clients
2.1.5 Marketing and sales
2.1.6 Conducting financial checks and assessments of prospective clients

2.1.7 Complying with legal and regulatory requirements
2.1.8 In connection with legal proceedings
2.1.9 Detecting and prevention of fraud, crime, money laundering and other malpractice.

2.2 Conditions of Processing

The Companies acknowledges that personal information may only be processed if certain conditions are met, i.e. one of the following:

2.2.1 The data subject consents to the processing or there is a justifiable reason; or
2.2.2 The processing is necessary for concluding a contract or in terms of a contract; or
2.2.3 The processing complies with an obligation imposed by law on The Companies; or
2.2.4 The processing protects a legitimate interest of the data subject; or
2.2.5 The processing is necessary for pursuing the legitimate interests of The Companies or of a third party to whom information is supplied.

2.3 Personal information collected

Section 9 of POPIA states that "Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."

2.3.1 The Companies collects and processes personal information pertaining to the needs of its business activities and services. The type of information depends on the needs for which it is collected and will be processed for that purpose only. Whenever possible, The Companies will advise data subjects (see 2.4 below) as to the information required and the information deemed optional.
2.3.2 The Companies aims to have agreements in place with all contractors, suppliers, and third-party service providers to ensure a mutual understanding with regard to protection of the personal information of all data subjects.
2.3.3 The Companies may also supplement the information provided with the information that it receives over time via staff members if not directly from data subjects.

2.4 Categories of Data Subjects and their Personal Information

The Companies processes records relating to clients, contractors, suppliers, service providers, staff and consultants:

Data subjects / Entity Types	**Personal Information Processed**
Clients and Financiers (Natural Persons)	Names; date of birth; ID number; nationality; gender; contact details; physical and postal addresses; financial and tax-related information; confidential correspondence.
Financiers / Sureties / Medical Aid Schemes	Names of contact persons; name of legal entity; registration number; physical and postal address and contact details; financial information; tax-related information; authorized signatories; beneficiaries; ultimate beneficial owners; shareholding information

Contractors / Suppliers / Service Providers	Names of contact persons; name of legal entity; registration number; founding documents; physical and postal address and contact details; financial (banking) and tax-related information; authorized signatories
Staff / Consultants / Individual Contractors /	Names; date of birth; ID number; nationality; gender; marital status; race; disability; age; language; education information; financial (banking) and tax-related information; education; employment history; ID number; pregnancy*; well-being; physical and postal addresses; contact details; criminal record*

* Special personal information

2.5 Categories of Recipients for Processing the Personal Information

The Companies may share Personal Information with its agents, and contracted parties to whom The Companies may have assigned or transferred any of its rights or obligations under any agreement, to render the following services:

2.5.1 Sending of emails and other correspondence to clients and agents;
2.5.2 Storing of data; and
2.5.3 Sending of client information packs to financial institutions for deals to be discounted.

2.6 Retention of Personal Information Records

The Companies shall retain the Personal Information records to the extent permitted or required by law as per ANNEXURE B.

2.7 Disclosure of Personal Information

The Companies may

2.7.1 share personal information of employees, clients, contractors or suppliers or other data subjects with third parties as well as obtain information from such third parties for the reasons set out herein; and
2.7.2 disclose such personal information where there is a duty or a right to disclose in terms of applicable legislation, the law or where it may be necessary to protect The Companies's rights.

2.8 Objecting to processing of Personal Information

2.8.1 Where a data subject objects to The Companies processing their Personal Information, they must provide reasons for the objection.
2.8.2 The Companies must explain the consequences of non-processing of the Personal Information before the data subject confirms the objection for implementation.
2.8.3 Once an objection has been confirmed in writing, The Companies may no longer process said Personal Information.
2.8.4 In instances where non-performance in terms of any contract may result due to the non-processing of information, it might lead to the termination of the contract with the data subject.

To object, the data subject must use FORM 1 at the end of this manual and forward to the Information Officer (see contact details in item 3.1.2 below).

3. ACCESS AND CORRECTION OF PERSONAL INFORMATION

3.1 All data subjects have the right to request

3.1.1 access to any Personal Information that The Companies holds about them;
3.1.2 The Companies to update, correct or delete their personal information on reasonable grounds. Such requests should in the first instance be directed to The Companies' Information Officer (see details below).

Deputy Information Officer
Natalie Callaghan
Telephone number 011 334 8744
Postal address P.O. Box 751998 Johannesburg, 2000
Physical address 51 Durban Street, City and Suburban, 2001
Email address natalie@ftgap.co.za.co.za

To request any correction or deletion of information, the data subject must use FORM 2 at the end of this manual and forward it to the Information Officer.

4. GENERAL DESCRIPTION OF INFORMATION SECURITY MEASURES

4.1 The Companies shall ensure the safeguarding and protection of all personal information it processes.
4.2 The Companies (also through its service providers) employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information it processes. The measures The Companies uses include:

4.2.1 Physical access control, i.e. limited office access, lockable cabinets, passwords on computers;
4.2.2 Access to Personal Information is limited to authorized personnel only;
4.2.3 Firewalls for computer and network protection;
4.2.4 Virus protection software and update protocols;
4.2.5 Secure setup of hardware and software comprising the IT infrastructure;
4.2.6 Outsourced Service Providers who process Personal Information on behalf of The Companies are contractually bound to implement security controls;
4.2.7 All electronic files or data shall be backed up to a secure Nas Server.

4.3 The Companies must review its security controls and processes on a regular basis, at least annually to ensure that personal information is secure. For this purpose, it will use ANNEXURE C.

5. SECURITY BREACHES

5.1 Should The Companies become aware of a security breach on any of its systems that contain Personal Information, The Companies shall take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.
5.2 The Companies shall notify affected parties should it have reason to believe that their information has been compromised. This shall only be done where The Companies can identify the data subject to whose information has been compromised. Where it is not possible, it may be necessary to consider a website-based publication and whatever procedure the Information Regulator prescribes.

5.3 Notification will be provided in writing by means of either:

5.3.1 email;
5.3.2 registered mail;
5.3.3 Website notice.

5.4 The notification shall provide the following information where possible:

5.4.1 description of possible consequences of the breach:
5.4.2 measures taken to address the breach:
5.4.3 recommended actions to be taken by the data subject to mitigate adverse effects:
5.4.4 the identity of the party responsible for the breach, if available.

5.5 In addition to the above, The Companies shall notify the Regulator of any breach and/or compromise to Personal Information in its possession and work closely with and comply with any recommendations issued by the Regulator.

PROCEDURE: PERSONAL INFORMATION of an EMPLOYEE

6. For the purposes of this Manual, employees include potential, past and existing employees, Temporary and Casual employees. The Companies will use and process such employee information, as set out in its Data Protection and Information Sharing Manual (Manual) for, but not limited to, its employment records and to make lawful decisions in respect of that employee and The Companies' business.

2. Collection

The Companies will, when recruiting and appointing new employees, require information, including, but not limited to that listed in the Manual, from the prospective employee in order to process the information on The Companies' systems. Such information is reasonably necessary for The Companies to ascertain if the prospective employee meets the requirements for the position which he or she is being considered for or appointed to, and is suitable for appointment, and also for record purposes.

The information is processed by the Deputy Information Officer or her nominated staff member.

3. Use

Employees' personal information will only be used for the purpose for which it was collected and intended. This would include, but is not limited to:

• for purposes of
- considering an applicant for employment
- contracting with a successful applicant
- Record keeping

• in connection with
- legal proceedings
- legal and regulatory requirements
- disciplinary action or action in respect of employee's conduct or capacity
- administrative functions of The Companies
- employment benefits, including pension fund
- pre and post-employment checks and screening

• submissions to

- Department of Labour
- South African Revenue Service

• any other relevant purpose.

4. Store

Employees

Format	Where	Post-employment	Where
Hard Copies	Admin Office	Archive	On site
Electronic info	Pastel Payroll	Archive	Iron Tree/Nas Server

Directors

Format	Where	Post-employment	Where
Hard Copies	Admin Office	Archive	On site
Electronic info	Pastel Payroll	Archive	Iron Tree/Nas Server

Volunteers/Temps

Format	Where	Post-employment	Where
Hard Copies	Admin Office	Archive	On site
Electronic info	Pastel Payroll	Archive	Iron Tree/Nas Server

5. Delete

Hard copies must be shredded and electronic copies deleted post the period stipulated in ANNEXURE B.

ANNEXURE A2

PROCEDURE: PERSONAL INFORMATION of a CONSULTANT, CONTRACTOR or SUPPLIER

1. For the purposes of this Manual, Consultants, Contractors and Suppliers include potential, past and existing Consultants, Contractors and Suppliers of The Companies. The Companies will use and process information of Consultants, Contractors and Suppliers, as set out in Data Protection and Information Sharing Manual (Manual) for, but not limited to, its administrative and accounting records and to make lawful decisions in respect of the Consultants, Contractors and Suppliers for The Companies' business.

2. Collection

The Companies will, when proposing to and when contracting with Consultants, Contractors and Suppliers, require information, including, but not limited to that listed in its Manual, from prospective Consultants, Contractors and Suppliers. The information is reasonably necessary for The Companies' assessment as well as to ascertain if the prospective Consultants, Contractors and Suppliers meet the requirements for the services and or products required by The Companies. It will further be used on The Companies' systems as stated below and for record purposes.

The information is processed by the Information Officer or her nominated staff member.

3. Use:

Personal Information of Consultants, Contractors and Suppliers will only be used for the purpose for which it was collected and intended. This would include, but is not limited to:

• for purposes of
- opportunities to quote
- Contracting
- administration
- Record-keeping
- remittance and communication

• in connection with
- administrative functions of The Companies
- accounting functions of The Companies
- legal proceedings
- legal and regulatory requirements
- pre and post-contracting checks and screening

• submissions to
- South African Revenue Service

• any other relevant purpose.

4. Store

Format	Where	Post contract	Where
Hard Copies	Admin Office	Archive	On site
Electronic info	Pastel Evolution	Archive	Iron Tree/Nas Server

5. Delete

Hard copies must be shredded and electronic copies deleted post the period stipulated in ANNEXURE B.

ANNEXURE B

RETENTION PERIODS

Basic Conditions of Employment Act
Section 29(4):
-Written particulars of an employee after termination of employment
3 YEARS

Section 31:
-Employee's name and occupation;
-Time worked by each employee;
-Remuneration paid to each employee;
-Date of birth of any employee
3 years

Employment Equity Act
Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act;

Section 21 report which is sent to the Director General
3 YEARS

Labour Relations Act

Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions
INDEFINITE

Unemployment Insurance Act

Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed
5 YEARS

Tax Administration Act

Section 29 documents which:
-Enable a person to observe the requirements of the Act;
-Are specifically required under a Tax Act by the Commissioner;
5 YEARS

Income Tax Act
-Amount of remuneration paid or due by him to the employee;
-The amount of employee's tax deducted or withheld from the remuneration paid or due;
-The income tax reference number of that employee;
-Any further prescribed information; Employer Reconciliation return.
5 YEARS

Value Added Tax Act
-The vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period;
-Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS;

-Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques;
-Documentary proof substantiating the zero rating of supplies;
-Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.
5 YEARS

Occupational Health and Safety Act, and Compensation for Occupational Injuries and Diseases Act
-A Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.
4 YEARS

General Administrative Regulations, 2003

Section 20(2) documents
-Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation;
-Records of incidents reported at work.
10 YEARS

Financial Intelligence Centre Act

-Whenever a reportable transaction is concluded with a customer, the Company must keep record of the identity of the customer;
-If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person;
-If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer;

-The manner in which the identity of the persons referred to above was established;
-In the case of a transaction, the amount involved and the parties to that transaction;
Any document or copy of a document obtained by the accountable institution.
5 YEARS

Electronic Communications and Transactions Act 25 of 2002
E-Invoices
5 YEARS

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT No. 4 of 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 2]
Note:

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

A. DETAILS OF DATA SUBJECT

Name(s) and surname/ registered name of data subject:……..
Company/ Identity Number :……..
Residential, postal or business address :……..
Code :……..
Contact number(s): :……..
Fax number / E-mail address: :……..

B. DETAILS OF RESPONSIBLE PARTY

Name(s) and surname :……..
Residential, postal or business address :……..
Code :……..
Contact number(s) :……..
Fax number/ E-mail address :……..

C. REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)

……
……
……
……
……
……..

Signed at ..... this ..... day of .....20……..

.....
Signature of data subject/designated person

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT No. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 3]

Note:
1. Affidavits or other documentary evidence as applicable in support of the request may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

Mark the appropriate box with an "x".
Request for:
Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorized to retain the record of information.

A. DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject:……..
Company/ Identity Number :……..
Residential, postal or business address :……..
Code :……..
Contact number(s): :……..
Fax number / E-mail address: :……..

B. DETAILS OF RESPONSIBLE PARTY
Name(s) and surname :……..
Residential, postal or business address :……..
Code :……..
Contact number(s) :……..
Fax number/ E-mail address :……..

C. INFORMATION TO BE CORRECTED/ DELETED/ DESTRUCTED/ DESTROYED
……
……
……
……
……

D. REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or

REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORIZED TO RETAIN.

(Please provide detailed reasons for the request)

……
……
……
……
……

Signed at ..... this ..... day of .....20…….....

.....

Signature of data subject/ designated person

MONITORING AND EVALUATION

	DATE	COMMENT	RECOMMENDATION	FOLLOW-UP
PREMISES				
Inspection of physical security & access				
Access control and biometrics				
Burglar bars				
Alarm and deactivation codes				
Armed response				
No-go areas – demarcated				
Risk analysis of security issues				
FILING AND PHYSICAL RECORD KEEPING				
Locked offices & cabinets				
No-go areas				
Proper disposal of records/files/hard copies - policy				
Work/document flow - data remains secure				
File integrity & lockup				
STAFF				
Keys to authorised staff only				
Alarm codes				
Area specific access				
Staff awareness re POPI obligations				
Confidentiality declaration and undertaking				
THIRD PARTY PROCESSING				
External operators all have written contracts				
External operators are aware of data usage security and limitations				
External operations Confidentiality requirements				
IT & DATA				
Computers physically secured				
Password policy				
Encryption of data				
Back-up policy & schedule				
Person appointed to manage backups				
Off-site storage				
Proper disposal of damaged devices / data drivers				
Network, Internet & www security				
MOBILE DEVICES				
No flash drives / removable media in restricted areas				
Private devices not permitted to sync on networks				
Laptop - data encrypted				
Laptop - password secured				
Theft prevention strategy				
SECURITY BREACHES				
Any loss of data / security breach - Information Regulator				
Any loss of data / security breach - Data subjects				