PAIA/POPI MANUAL

CRS TECHNOLOGIES (PTY) LTD AND AFFILIATED COMPANIES

PREPARED IN ACCORDANCE WITH THE PROVISIONS OF THE

PROTECTION OF PERSONAL INFORMATION ACT, NO 4 OF 2013

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

PROMOTION OF ACCESS TO INFORMATION ACT, NO 2 OF 2000

VERSION: 1.0
DATE OF VERSION: 01/07/2021
CREATED BY: NICOL MYBURGH
REVIEWED BY: _____
POLICY REVIEW DATE: 01/07/2022

CRS Technologies (RF) (Pty) Ltd - 2000/009010/07
+27 11 259 4700 (t) • +27 11 259 4750 (f) • info@crs.co.za • crs.co.za
Centric House, Mellis Court, Mellis Road, Rivonia, 2128 • PO Box 2712, Rivonia, Gauteng, 2128
Director: M. Moodle

Contents

1. DEFINITIONS

Consent means the voluntary, specific and informed expression of will.

Data subject means the natural or juristic person to whom the personal information relates.

Direct marketing means approaching a data subject personally for the purpose of selling them a product or service, or requesting a donation.

Personal Information means information relating to an unidentifiable, living, natural person, or an identifiable, existing juristic person, as defined in POPIA.

Processing means an operation or activity, whether or not by automatic means, concerning personal information.

Responsible party means the party who determines the purpose of and means for processing personal information. This decision may be made alone or in conjunction with another party.

Operator means a person who processes personal information for a responsible party in terms of a contract or mandate, but does not come under the direct authority or control of the responsible party;

CRS/the company means CRS Technologies (Pty) Ltd and affiliated companies, including CRS Human Capital (Pty) Ltd, CRS Recruitment Outsourcing Solutions (Pty) Ltd, CRS Konsult (Pty) Ltd, CRS Outsourcing (Pty) Ltd, Centric Solutions (Pty) Ltd and Adfinserv (Pty) Ltd.

POPIA refers to the Protection of Personal Information Act, Act 4 of 2013 and, where applicable, any reference to the Regulations under POPIA refers to regulations issued by the provisions of Section 112(2) of the Act.

PAIA means the Promotion of Access to Information Act, Act 2 of 2000.

Information officer in relation to a public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17, or in relation to a private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act.

2. INTRODUCTION

This Promotion of Access to Information Manual (manual) provides an outline of the type of records and personal information it holds, and explains how to submit requests for access to these records in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA). In addition, it explains how to access or object to personal information held by the company, or request correction of the personal information, in terms of paragraphs 23 and 24 of the Protection of Personal Information Act 4 of 2013 (POPI Act).

The PAIA and POPI Acts give effect to everyone's constitutional right of access to information held by private sector or public bodies, if the record or personal information is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

Requests shall be made in accordance with the prescribed procedures.

This manual must be read in conjunction with the following policy documents:

- CRS Application Data
- CRS Password Policy
- CRS Supplier Data Security
- Data Code of Conduct
- Supplier Compliance
- Confidential Information Policy V2
- Data Protection Policy

2.1. PAIA Manual Availability

This manual is published on the CRS website at www.crs.co.za. Alternatively, a copy can be requested from the **Information Officer** (see contact details in Section 2).

2.2. Availability of Guides to the PAIA and POPIA

Guides to PAIA and POPIA can be obtained and queries directed to:

The South African Human Rights Commission:

PAIA Unit (Research and Documentation Department)

Postal address:
Private Bag 2700
Houghton
Johannesburg

Street address:
Corner York and St Andrews Street
Parktown
Johannesburg

2041 2193

Telephone number: +27 11 484-8300
Fax number: +27 11 484-7146
Website: www.sahrc.org.za
E-mail: PAIA@sahrc.org.za

The Information Regulator (South Africa):

Postal address:
PO Box 31533
Braamfontein
Johannesburg
2017

Street address:
JD House
27 Stiemens Street
Braamfontein
Johannesburg
2001

Ms Mmamoroke Mphelo

Telephone number: +27 12 406 4818
Fax number: +27 86 500 3351
Website: www.justice.gov.za/inforeg/
E-mail: inforeg@justice.gov.za

3. COMPANY CONTACT DETAILS

3.1. CRS contact details in terms of PAIA Section 51:

Postal address:
PO Box 31045
Kyalami
1684

Street address:
Centric House
Mellis Court
Mellis Road
Rivonia
2191

Tel: +27 11 259 4700
Fax: +27 11 259 4750
Email: info@crs.co.za
Website: www.crs.co.za

3.2. Information Officer:

Name: Nicol Myburgh
Email: Nicolm@crs.co.za
Office: +27 11 259 4700

Cell: +27 83 465 5972

4. RECORDS AVAILABLE IN TERMS OF ANY OTHER LEGISLATION

- Basic Conditions of Employment Act No. 75 of 1997
- Broad-Based Black Economic Empowerment Act No. 53 of 2003
- Companies Act No. 61 of 1973
- Compensation for Occupational Injuries and Health Diseases Act No. 130 of 1993
- Copyright Act No. 98 of 1978
- Electronic Communications and Transactions Act No. 25 of 2002
- Employment Equity Act No. 55 of 1998
- Financial Intelligence Centre Act No. 38 of 2001
- Income Tax Act No. 95 of 1967
- Labour Relations Act No. 66 of 1995
- Occupational Health and Safety Act No. 85 of 1993
- Promotion of Access to Information Act No. 2 of 2000
- Skills Development Levies Act No. 9 of 1999
- Skills Development Act No. 97 of 1998
- Unemployment Contributions Act No. 4 of 2002
- Unemployment Insurance Act No. 63 of 2001
- Value Added Tax Act No. 89 of 1991

5. ACCESS TO THE RECORDS

5.1. Information Readily Available

Applicable information is readily available and accessible by means described in **the CRS Information Security Policy** and various **operations agreements**.

5.2. Records that may be requested and held at the offices of the business:

5.2.1. Administration

- Correspondence
- Minutes of management meetings
- Minutes of employee meetings

5.2.2. Companies Act Records

- Documents of incorporation
- Memorandum of incorporation
- List of directors
- Records relating to the appointment of directors/auditor/secretary/public officer and other officers

- Minute books and resolutions
- Power of attorney agreements
- Share register
- Shareholders agreements
- Statutory registers

5.2.3. Financial Records

- Audited annual financial statements
- Accounting records
- Assets register
- Banking records
- Banking details
- Bank statements
- Stock records
- Financial agreements
- Supplier records
- Utility bills
- Invoices
- VAT

5.2.4. Payroll

- PAYE records, internal and clients
- Documents issued to employees and client employees for income tax purpose (IRP5s)
- Records of payments to SARS on behalf of employees and client employees (IT88)
- Employee and client employee-related details sent to third parties, i.e. pension/provident fund, medical aid, etc.
- All statutory requirements
    - Skills development levies
    - Unemployment insurance fund
    - Workmen's Compensation

5.2.5. Human Resources

The below relates to internal employees and client employees:

- Disciplinary records and documentation pertaining to disciplinary proceedings
- Employee code of conduct
- Employment contracts
- Employment equity plan
- Personnel files
- Remuneration records and policies
- Employee recruitment policies
- Training records

- Recruitment records
- CVs

5.2.6. Information Technology

- Computer software support and maintenance agreements
- Software licence agreements
- Agreements in respect of computer hardware
- Agreements with internet service providers
- Agreements in respect of hosting

5.2.7. Operations

- Register of clients
- Sales records
- Specific types of work done, and records related to it
- Service level agreements

5.2.8. Policy Documents

6. ACCESS TO PERSONAL INFORMATION

All individuals and entities may request access, amendment, or deletion of their own personal information held by CRS. Any requests should be directed to the information officer on the prescribed form (Annexure A).

6.1. Remedies Available if Request for Access to Personal Information is Refused

6.1.1. Internal Remedies

CRS does not have internal appeal procedures. As such, the decision made by the information officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the information officer.

6.1.2. External Remedies

A requestor who is dissatisfied with the information officer's refusal to disclose information may, within 30 days of notification of the decision, apply to a court for relief. Likewise, a third party dissatisfied with the information officer's decision to grant a request for information may, within 30 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status.

6.2. Grounds for Refusal

CRS may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which CRS may refuse access include:

- Protecting personal information that CRS holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
- Protecting commercial information that CRS holds about a third party or CRS (for example, a trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the organisation or the third party);
- If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
- If disclosure of the record would endanger the life or physical safety of an individual;
- If disclosure of the record would prejudice or impair the security of property or means of transport;
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- If disclosure of the record would prejudice or impair the protection of the safety of the public;
- The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
- Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of CRS;
- Disclosure of the record would put CRS at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- The record is a computer programme;
- The record contains information about research being carried out or about to be carried out on behalf of a third party or CRS;
- Records that cannot be found or do not exist.

7. PROCESSING OF PERSONAL INFORMATION

7.1. Purpose of Processing

The company uses the personal information under its care in the following ways:

- To provide or manage any information, products and/or services requested by data subjects and/or a responsible party;
- To help us identify data subjects and responsible parties when they contact us;
- To maintain client records;
- For rendering services according to instructions given by clients;
- For recruitment processes;
- For employee administration;

- For keeping of accounts and records;
- For complying with tax laws;
- For legal or contractual purposes;
- For health and safety purposes;
- To help us improve the quality of our products and services;
- To help us detect and prevent fraud and money laundering;
- To help us recover debts;
- To carry out analysis and client profiling (benchmarking);
- To identify other products and services which might be of interest to data subjects and/or responsible parties; and to
- Inform them about our products and services.

7.2. Categories of Data Subjects and Their Personal Information

The company may possess records relating to suppliers, shareholders, contractors, service providers, employees and clients:

Entity Type	Personal Information Processed
Clients – juristic persons/entities	• Names of contact persons; • Name of legal entity; • Physical and postal address and contact details; • Financial information; • Registration number; • Founding documents; • Tax-related information; • Authorised signatories, beneficiaries, ultimate beneficial owners • Employee ID number • Employee income tax number • Employee bank details • Name • Surname • Sex • Marital status • Age • Health • Language • Date of birth • Education • Medical aid • Salary • Employment • Email address

	• Physical address • Telephone number **Special Personal Information** • Race • Gender • Pregnancy • Nationality • Physical or mental health • Disability • Criminal history • Membership of a trade union • Biometric information
Intermediary/advisor	• Names of contact persons • Name of legal entity • Physical and postal address and contact details • Financial information • Registration number • Founding documents • Tax-related information • Authorised signatories, beneficiaries, ultimate beneficial owners
Contracted service providers	• Names of contact persons • Name of legal entity • Physical and postal address and contact details • Financial information • Registration number • Founding documents • Tax-related information • • Authorised signatories, beneficiaries, ultimate beneficial owners
Employees/directors /shareholders	• Employee ID number • Employee income tax number • Employee bank details • Name • Surname • Sex • Marital status • Age • Health • Language

	• Date of birth • Education • Medical aid • Salary • Employment • Email address • Physical address • Telephone number **Special Personal Information** • Race • Gender • Pregnancy • Nationality • Physical or mental health • Disability • Criminal history • Membership of a trade union • Biometric information
Recruitment	• CV and application forms • Criminal checks • Background checks

7.3. Categories of Recipients for Processing the Personal Information

CRS may supply the personal information to service providers who render the following services:

- Capturing and organising of data;
- Storing of data;
- Sending of emails and other correspondence to clients;
- Conducting due diligence checks;
- Administration of the collective investment schemes;
- Administration of employee benefit schemes.

7.4. General Description of Information Security Measures

Refer to the following policy documents:

- CRS Application Data
- CRS Password Policy
- CRS Supplier Data Security
- Data Code of Conduct
- Supplier Compliance

- Confidential Information Policy V2
- Data Protection Policy

We will send our data subjects notifications or communications if we are obliged to do so by law, or in terms of our contractual relationship with them.

We will only disclose personal information to government authorities if we are required to do so by law.

8. ACTUAL OR PLANNED TRANSBORDER FLOWS OF PERSONAL INFORMATION

- The company may transfer data transborder in order to store data with third party cloud storage providers.

- The company will ensure that its affiliates and sub-contractors shall not transfer personal information transborder, except where:

    - There is a decision in force that the countries or territories to which the personal information transfer is to be made ensures an adequate level of protection for the processing of personal information; and
    - On written approval of the responsible party and then subject to any additional restrictions reasonably required by the responsible party for compliance with applicable law, which may include obtaining the prior consent of the applicable regulator, where such is required.

- If the appropriate safeguards demonstrated or implemented by CRS in accordance with this clause are deemed at any time not to provide an adequate level of protection in relation to personal information, the company will implement such alternative measures as may be required by the responsible party to ensure that the relevant cross-border personal information transfer and all resulting processing are compliant with the applicable law.

9. EIGHT PROCESSING CONDITIONS

POPIA is implemented by abiding by eight processing conditions. CRS shall abide by these principles in all its possessing activities.

9.1. Accountability

CRS shall ensure that all processing conditions, as set out in POPIA, are complied with when determining the purpose and means of processing personal information and during the processing itself. CRS shall remain liable for compliance with these conditions, even if it has outsourced its processing activities.

9.2. Processing Limitation

9.2.1. Lawful Grounds

The processing of personal information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive.

CRS may only process personal information if one of the following grounds of lawful processing exists:

- The data subject consents to the processing;
- Processing is necessary for the conclusion or performance of a contract with the data subject/responsible party;
- Processing complies with a legal responsibility imposed on CRS;
- Processing protects a legitimate interest of the data subject;
- Processing is necessary for pursuance of a legitimate interest of CRS, or a third party to whom the information is supplied;

Special personal information includes:

- Religious, philosophical, or political beliefs;
- Race or ethnic origin;
- Health or sex life;
- Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
- Criminal behaviour;
- Information concerning a child.

CRS may only process special personal information under the following circumstances:

- The data subject/responsible party has consented to such processing;
- The special personal information was deliberately made public by the data subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical or research reasons;
- Processing of race or ethnic origin is in order to comply with affirmative action laws.

All data subjects have the right to refuse or withdraw their consent to the processing of their personal information, and a data subject may object at any time to the processing of their personal information on any of the above grounds, unless legislation provides for such processing. If the data subject withdraws consent or objects to processing, CRS shall forthwith refrain from processing the personal information.

9.2.2. Collection Directly from the Data Subject

Personal information must be collected directly from the data subject, unless:

- Personal information is contained in a public record;
- Personal information has been deliberately made public by the data subject;
- Personal information is collected from another source with the data subject's consent;
- Collection of personal information from another source would not prejudice the data subject;
- Collection of personal information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the data subject would prejudice the lawful purpose of collection;
- Collection from the data subject is not reasonably practicable.

9.3. Purpose Specification

CRS shall only process personal information for the specific purposes as set out and defined in Section 7 of this manual.

9.4. Further Processing

New processing activity must be compatible with the original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

- The data subject has consented to the further processing;
- Personal information is contained in a public record;
- Personal information has been deliberately made public by the data subject;
- Further processing is necessary to maintain, comply with or exercise any law or legal right;
- Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the data subject or a third party.

9.5. Information Quality

CRS shall take reasonable steps to ensure that personal information is complete, accurate, not misleading and updated. CRS shall periodically review data subject records to ensure that the personal information of which it is the responsible party is still valid and correct.

Employees should, as far as is reasonably practicable, follow the following guidance when collecting personal information:

- Personal information should be dated when received;
- A record should be kept of where the personal information was obtained;

- Changes to information records should be dated;
- Irrelevant or unneeded personal information should be deleted or destroyed;
- Personal information should be stored securely, either on a secure electronic database or in a secure physical filing system.

9.6. Openness

CRS shall take reasonable steps to ensure that the data subject/responsible parties is/are made aware of:

- What personal information is collected, and the source of the information;
- The purpose of collection and processing;
- Where the supply of personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;
- Whether collection is in terms of any law requiring such collection;
- Whether the personal information shall be shared with any third party.

9.7. Data Subject Participation

A data subject has the right to request access to the amendment or deletion of their personal information.

All such requests must be submitted in writing to the information officer. Unless there are grounds for refusal, CRS shall disclose the requested personal information:

- On receipt of adequate proof of identity from the data subject or requestor;
- Within a reasonable time;
- On receipt of the prescribed fee, if any;
- In a reasonable format.

CRS shall not disclose any personal information to any party unless the identity of the requestor has been verified.

9.8. Security Safeguards

CRS shall ensure the integrity and confidentiality of all personal information in its possession by taking reasonable steps to:

- Identify all reasonably foreseeable risks to information security;
- Establish and maintain appropriate safeguards against such risks;

Refer to the following policy documents for further information:

- CRS Application Data

- CRS Password Policy
- CRS Supplier Data Security
- Data Code of Conduct
- Supplier Compliance
- Confidential Information Policy V2
- Data Protection Policy

10. DIRECT MARKETING

All direct marketing communications shall contain the company's details, and an address or method for the customer to opt out of receiving further marketing communication.

10.1. Existing Customers

Direct marketing by electronic means to existing customers is only permitted:

- If the customer's details were obtained in the context of a sale or service; and
- For the purpose of marketing the same or similar products.

The customer must be given the opportunity to opt out of receiving direct marketing on each occasion of direct marketing.

10.2. Consent

CRS may send electronic direct marketing communication to data subjects who have consented to receiving it. CRS may only approach a data subject for consent once.

10.3. Record Keeping

CRS shall keep record of:

- Date of consent;
- Wording of the consent;
- Who obtained the consent;
- Proof of opportunity to opt out on each marketing contact;
- Record of opt-outs.

11. DESTRUCTION OF DOCUMENTS

- Documents may be destroyed after the termination of the retention period specified herein, or as determined by CRS from time to time.
- Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked to

make sure that they may be destroyed and also to ascertain if there are important original documents in the file.

- The documents must be shredded.
- Deletion of electronic records must be done in consultation with the IT department to ensure that deleted information is incapable of being reconstructed and/or recovered.

12. STATUTORY RETENTION PERIODS

Legislation	Document Type	Period
Companies Act	• Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act; • Notice and minutes of all shareholders meetings, including resolutions adopted and documents made available to holders of securities; • Copies of reports presented at the company's annual general meeting; • Copies of annual financial statements as required by the Act; • Copies of accounting records as required by the Act; • Record of directors and past directors, after the director has retired from the company; • Written communication to holders ofsecurities; • Minutes and resolutions of directors meetings, audit committees and directors committees.	7 years
	• Registration certificate; • Memorandum of Incorporation and alterations and amendments; • Rules; • Securities register and uncertified securities register; • Register of company secretary and auditors; • Regulated companies (companies to which Chapter 5, Part B, C and takeover regulations apply) • Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.	Indefinitely

Consumer Protection Act	• Full names, physical address, postal address and contact details; • ID number and registration number; • Contact details of public officer in case of a juristic person; • Service rendered; • Cost to be recovered from the consumer; • Frequency of accounting to the consumer; • Amounts, sums, values, charges, fees, remuneration specified in monetary terms; • Conducting a promotional competition (refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions);	3 years
Financial Intelligence Centre Act	• Whenever a reportable transaction is concluded with a customer, the institution 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; • The nature of that business relationship or transaction; • In the case of a transaction, the amount involved and the parties to that transaction; • All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; • The name of the person who obtained the identity of the person transacting on behalf of the accountable institution; • Any document or copy of a document obtained by the accountable institution;	5 years

Compensation for Occupational Injuries and Diseases Act	• 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
	• 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.	3 years
	• Asbestos Regulations, 2001, regulation 16(1): • Records of assessment and air monitoring, and the asbestos inventory; • Medical surveillance records; • Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): • Records of risk assessments and air monitoring; • Medical surveillance records. • Lead Regulations, 2001, Regulation 10: • Records of assessments and air monitoring; • Medical surveillance records • Noise - induced Hearing Loss Regulations, 2003, Regulation 11: • All records of assessment and noise monitoring; • All medical surveillance records, including the baseline audiogram of every employee.	40 years
	• Hazardous Chemical Substance Regulations, 1995, Regulation 9: • Records of assessments and air monitoring; • Medical surveillance records	30 years

Basic Conditions of Employment Act	Section 29(4): • Written particulars of an employee after termination of employment; Section 31: • Employee's name and occupation; • Time worked by each employee; • Remuneration paid to each employee; • Date of birth of any employee under the age of 18 years.	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 to be retained by the employer are the collective agreements and arbitration awards.	3 years
	• An employer must retain prescribed details of any strike, lockout or protest action involving its employees; • 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 by the public notice; • Will enable SARS to be satisfied that the person has observed these requirements.	5 years
Income Tax Act	• Amount of remuneration paid or due by him to the employee; • The amount of the 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	• Where a vendor's basis of accounting is changed 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

ANNEXURE A: REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR TRANSFER 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 objection may be attached.
2. If the space provided for in the form is inadequate, submit information as an annexure to this form and sign each page.
3. Complete as is applicable.

Request for: (mark the appropriate box with an "X")

☐ 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 authorised to retain the record of information.

SECTION A	DETAILS OF DATA SUBJECT
Name(s) and surname/registered name of data subject	
Unique identifier/identity number:	
Residential, postal or business address:	
Contact number(s):	
Fax number/email address:	
SECTION B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname/registered name of responsible party:	
Residential, postal or business address:	
Contact number(s):	
Fax number /email address:	
SECTION C	INFORMATION TO BE CORRECTED/DELETED/DESTROYED

SECTION D (Please provide detailed reasons for the request)	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 AUTHORTISED TO RETAIN

ANNEXURE B: 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 the form is inadequate, submit information as an annexure to this form and sign each page.
3. Complete as is applicable.

SECTION A	DETAILS OF DATA SUBJECT
Name(s) and surname/registered name of data subject	
Unique identifier/identity number:	
Residential, postal or business address:	
Contact number(s):	
Fax number/email address:	
SECTION B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/registered name of responsible party:	
Residential, postal or business address:	
Contact number(s):	
Fax number/email address:	
SECTION C (Please provide detailed reasons for the objection)	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) TO (f)**
Signed at……..on this……day of……20….. _____ Signature of data subject/designated person	