

# MBA Incorporated Policies

---

**DESCRIPTION**

**PROTECTION OF PERSONAL INFORMATION &  
PRIVACY POLICY**

**Version 2**

**15 September 2025**

**DEPARTMENT:**

**OFFICE OF THE MANAGING DIRECTOR**

85 WESTERN SERVICE ROAD,  
WENDYWOOD, SANDTON,  
2090

**CONTACT PERSONS**

[coenie@mbaincorporated.co.za](mailto:coenie@mbaincorporated.co.za)

011 463 9401

# Index

COPYRIGHT NOTICE.....	2
DEFINITIONS.....	2
PURPOSE.....	5
POLICY STATEMENT.....	5
RESPONSIBILITY AND ACCOUNTABILITY .....	5
INFORMATION OFFICER:.....	6
PURPOSES OF PERSONAL INFORMATION:.....	6
PROCESSING OF PERSONAL INFORMATION:.....	8
PROCESSING SPECIAL PERSONAL INFORMATION:.....	9
DISCLOSURE: .....	10
COLLECTION, USE, PROTECTION AND DISCLOSURE OF PERSONAL AND/ OR CONFIDENTIAL INFORMATION (AN OVERVIEW): .....	11
RIGHTS OF DATA SUBJECTS: .....	13
GENERAL GUIDING PRINCIPLES: .....	15
STAFF TRAINING: .....	16
REFERENCES:.....	17
FORM 1: OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION .....	18
FORM 2: REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION .....	19

## COPYRIGHT NOTICE

This policy is the property of the company and may not be distributed without the consent of the managing partner. Any unauthorised copying, alteration, or distribution is strictly prohibited and may incur penalties in law.

For any enquiries related to this policy, please email [coenie@mbaincorporated.co.za](mailto:coenie@mbaincorporated.co.za).

## DEFINITIONS

**Biometrics** means a technique of personal identification that is based on physical, physiological, or behavioural characterisation, including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.

**Child** means a natural person under the age of 18 who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

**Company** means Motsoeneng Bill Attorneys Incorporated.

**Competent person** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

**Consent** means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.

**Constitution** means the Constitution of the Republic of South Africa, 1996.

**Data subject** means the person to whom personal information relates.

**Day** means business days, unless otherwise indicated.

**Deidentify**, in relation to personal information of a data subject, means to delete any information that:

- Identifies the data subject;
- Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- Can be linked by a reasonably foreseeable method to other information that identifies the data subject.

**Direct marketing** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply any goods or services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason.

**Electronic communication** means any text, voice, sound, or image message sent over an electronic communications network that is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

**Filing system** means any structured set of personal information, whether centralised, decentralised, or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

**Information officer**, in relation to a private body, means the head of a private body as contemplated in section 1 read with section 55 of the Act. This shall include a deputy information officer appointed in terms of section 56 of the Act.

**Operator** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

**Person** means a natural or juristic person.

**Personal information** means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including but not limited to:

- Information relating to 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.
- Information relating to the education, medical, financial, criminal, or employment history of the person.
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person.
- The biometric information of the person.
- The personal opinions, views, or preferences of the person.
- Correspondence sent by the person that is implicitly or explicitly private or confidential.
- The views or opinions of another individual about the person.
- The name of the person if it appears with other personal information or if the disclosure of the name itself would reveal information about the person.

**Processing** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

- The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use.
- Dissemination by means of transmission, distribution, or making available in any other form.
- Merging, linking, as well as restriction, degradation, erasure, or destruction of information.

**Public record** means a record that is accessible in the public domain and which is in the possession of or under the control of a public body.

**Record** means any recorded information:

- Regardless of form or medium, including:
  - Writing on any material.
  - Information produced, recorded, or stored electronically.
  - Labels, markings, or other writings identifying or describing anything.
  - Books, maps, plans, graphs, or drawings.
  - Photographs, films, negatives, tapes, or other visual images.
- In the possession or under the control of a responsible party.
- Whether or not it was created by a responsible party.
- Regardless of when it came into existence.

**Regulator** means the Information Regulator established in terms of section 39 of the Act.

**Re-identify**, in relation to personal information of a data subject, means to resurrect any information that has been de-identified.

**Responsible party** means a public or private body or any other person which determines the purpose of and means for processing personal information.

**Restriction** means to withhold from circulation, use, or publication any personal information but not delete or destroy such information.

**Special personal information**, refers to personal information that is more sensitive in nature and is subject to stricter processing conditions under POPIA. Based on the provision you provided, it includes:

- Religious or philosophical beliefs
- Race or ethnic origin
- Trade union membership
- Political persuasion

- Health or sex life
- Biometric information
- Criminal behaviour, specifically - the alleged commission of an offence by the data subject; or legal proceedings related to such offence or the outcome of those proceedings. This type of information may not be processed unless specific exceptions under section 27 apply.

**Unique identifier** means any identifier assigned to a data subject that uniquely identifies that data subject in relation to a responsible party.

## **PURPOSE**

1. The purpose of this policy is to ensure compliance with the Protection of Personal Information Act 4 of 2013 (POPIA), safeguarding personal information in line with the Constitutional right to privacy. This policy aims to regulate the lawful processing of personal information within the company by setting minimum threshold requirements, balancing privacy rights with access to information, and protecting key interests such as the free flow of information. In addition, it provides for the monitoring of compliance and the reporting of breaches to the Information Regulator.

## **POLICY STATEMENT**

2. The company is committed to safeguarding the privacy of its employees, clients, and website visitors. The company takes the maintenance and protection of privacy and confidentiality very seriously, including but not limited to, commercial information, personal information, and intellectual property.

## **RESPONSIBILITY AND ACCOUNTABILITY**

3. The director/s, together with its appointed information officer retain the accountability to ensure that the company remains compliant with the provisions of this policy.
4. Every director and employee will be responsible for observing and complying with the provisions of this policy.
5. Every director and employee will be responsible to report any activity that construes non-compliance with the policy.

## INFORMATION OFFICER:

6. The information officer is:

**Michael Motsoeneng Bill**

Email: [info@mbaincorporated.co.za](mailto:info@mbaincorporated.co.za)

Tel: 011 463 9401

7. The deputy information officer is:

**Coenie Bezuidenhout**

Email: [coenie@mbaincorporated.co.za](mailto:coenie@mbaincorporated.co.za)

Tel: 011 463 9401

8. Duties of the information officer include:

- 8.1. Monitoring compliance with this policy.
- 8.2. Enforcing compliance with this policy.
- 8.3. Developing, implementing and enforcing any additional procedures, standards and processes, as he or she may deem necessary and appropriate, to effectuate this policy.
- 8.4. Working with and engaging with the Regulator as may be required.
- 8.5. Assigning duties to the deputy information officer/s.

## PURPOSES OF PERSONAL INFORMATION:

9. The company will collect data for the purposes below:

- 9.1. Billing and invoicing for legal services provided.
- 9.2. Client communication and updates (progress reports, case updates, requesting further information, etc.)
- 9.3. Client identification and verification as required in terms of the Financial Intelligence Centre Act 38 of 2001.

- 9.4. Compliance with regulatory and legal obligations (tax related requirements, legal filings, etc.)
- 9.5. Conducting legal research and case preparation.
- 9.6. Employment-related purposes (HR records, payroll, etc.)
- 9.7. Ensuring security and confidentiality of client information.
- 9.8. Handling complaints or disputes.
- 9.9. Handling requests for access to personal information.
- 9.10. Maintaining records of legal transactions and agreements.
- 9.11. Management of client trust accounts.
- 9.12. Managing client matters (legal advice, litigation, contract drafting, drafting Wills and other legal documents, etc.)
- 9.13. Managing relationships with external service providers (sheriffs, advocates, experts, consultants, court staff, deeds offices etc.)
- 9.14. Marketing and business development, subject to consent (newsletters, client engagement, etc.)
- 9.15. Our services are not directed at or designed for children. However, we may need to process a child's personal information when providing legal services in certain private matters (such as advising on inheritance tax, children's court matters, divorces, etc.). This will only occur where required for the specific legal service and always on behalf of the parent or guardian. If the reason for needing a child's personal information is unclear, please contact our information officer for further clarification.
- 9.16. When it is necessary for us to process your special personal information, we will do so as part of our standard business operations, for a legitimate and lawful purpose, and in compliance with all applicable legal requirements, including POPIA.



## PROCESSING OF PERSONAL INFORMATION:

10. For the purposes stated above, the company may collect and process personal information in various way, including but not limited to:
- 10.1. Billing and invoicing: personal and case-related data is processed to generate invoices, track payment status, and manage client accounts.
  - 10.2. Communication: client information is processed to communicate with clients about case progress, court dates, meetings, and billing. This may involve email, phone calls, letters, or secure portals.
  - 10.3. Data analysis: information is analysed to assess legal matters, prepare for cases, draft documents, or provide legal advice/ services. This includes reviewing client histories, legal documents, and applicable laws.
  - 10.4. Data collection: information collected through various means, such as client intake forms, email correspondence, phone calls, meetings, and documents provided by clients.
  - 10.5. Data sharing: information may be shared with external parties such as courts, opposing counsel, experts, or government agencies to further a case, comply with legal obligations, or obtain required documentation.
  - 10.6. Data storage: collected information is stored securely, usually in electronic databases (back up servers, shared network drives within the firm, and local hard drives), case management software, or physical files. This policy must be read in conjunction with the company's policy on Cyber Security.
  - 10.7. Document preparation: client information is used to draft legal documents such as contracts, pleadings, agreements, and other transactional documents. Personal and case details are processed to create accurate legal content.
  - 10.8. Record keeping: records of client data, legal documents, and communication are maintained for compliance with legal, regulatory, and professional standards. **In terms of FICA, client information is retained for 5 years, whereas the Legal Practice Counsel requires client information to be retained for 7 years.**

After expiry of the mandatory record keeping period above, the records must be destroyed.

Public records may be disposed of in the ordinary manner, but all financial records, and/ or records that are confidential in nature will be shredded or destroyed in an equivalent fashion as directed by the industry standards at the time.

- 10.9. Security: MBA has implemented data protection measures, including encryption, access controls, and audits to secure sensitive client information from unauthorised access, theft, or loss.

## **PROCESSING SPECIAL PERSONAL INFORMATION:**

- 11. The company may process special personal information under the following circumstances:

- 11.1. With the data subject's consent – when explicit consent has been given for the processing of such information.
- 11.2. To establish, exercise or defend legal rights – when necessary for litigation, legal advice, or compliance with legal obligations.
- 11.3. To comply with international public law obligations – if processing is required under international legal standards.
- 11.4. For public interest research, statistics or history – when the purpose serves the public interest, consent is impractical, and safeguards are in place.
- 11.5. When the data subject has made the information public – voluntarily and knowingly.
- 11.6. If authorised by the regulator – where the regulator grants permission based on public interest and adequate safeguards.

- 12. Additional authorisations apply for specific categories:

- 12.1. Religious or philosophical beliefs – we do not collect information about your religious or philosophical beliefs, where such information is required for the execution of our mandate, we will advise you and seek consent.
- 12.2. Race or ethnic origin – for identification when essential, or to advance legitimate interests under the law.

- 12.3. Trade union membership – as required for the execution of our mandate, particularly in relation to labour law matters.
  - 12.4. Political persuasion – we do not collect information about your political beliefs and persuasions, but we may collect information about political affiliations to the extent that it may affect the execution of our mandate.
  - 12.5. Health or sex life – when necessary for the purposes of executing our lawful mandate.
  - 12.6. Criminal behaviour or biometric information – when necessary for the purposes of executing our mandate, especially when it relates to criminal law matters, on information required for the purposes of human resources records.
13. The company may process children's personal information under these conditions:
- 13.1. With prior consent from a competent person – typically a parent or legal guardian.
  - 13.2. To establish, exercise or defend legal rights – in legal proceedings or advisory services involving children.
  - 13.3. To comply with international public law obligations – where necessary under international law.
  - 13.4. For public interest research, statistics or history – where consent is impractical, provided safeguards protect the child's privacy.
  - 13.5. Where the child, with competent person's consent, made the information public – the child has willingly disclosed the information.
  - 13.6. Additionally, the Regulator may authorise such processing if it serves the public interest and adequate safeguards are in place. The company will provide transparency, allow parental oversight, avoid over-collection, and implement protective measures to ensure the integrity and confidentiality of the child's data.

## **DISCLOSURE:**

14. The company may disclose personal information to a third party under specific lawful circumstances. These include where:
- 14.1. The data subject has given voluntary, specific, and informed consent.

- 14.2. The disclosure is necessary to conclude or perform a contract to which the data subject is a party; or where required by law, regulation, or a court order.
- 14.3. When necessary to protect the legitimate interests of the data subject, the company, or a third party, provided these do not override the data subject's rights.
- 14.4. It is required for the performance of a public duty or where the data subject has deliberately made the information public.
- 14.5. In the case of cross-border disclosures, information may be transferred if the recipient is subject to laws or agreements offering similar protection to POPIA, or if the data subject consents.

## **COLLECTION, USE, PROTECTION AND DISCLOSURE OF PERSONAL AND/ OR CONFIDENTIAL INFORMATION (AN OVERVIEW):**

<b>Collected from</b>	<b>Type of data collected</b>	<b>Application of information</b>	<b>Protection</b>	<b>Disclosure</b>
<b>Prospective employees</b>	Personal and demographic information (mode: CVs; application forms; interviews)	Consideration of prospective employees Building of prospective employee data base.	Prospective employees are asked whether the firm may retain their information. All information is stored on password protected computers, or in lockable cabinets behind a lockable door (when not under direct control of the responsible person.	Where legally required to do so; when in public interest; when in the best interests of the firm; with consent of the prospective employee.
<b>Employees</b>	Personal and demographic information (mode: employee information forms; employee	General employee administration, payroll processing, employee related statistics and reports.	All information is stored on password protected computers, or in lockable cabinets behind a lockable door (when not	Where legally required to do so; when in public interest; when in the best interests of the firm; with consent of the employee.

	discussions and correspondence)		under direct control of the responsible person.	
<b>Prospective clients</b>	Limited personal and demographic information (mode: website submission forms; consultations etc.)	To establish contact with prospective clients and/ or to assess client needs; elected correspondence eg: newsletters.	All information is stored on password protected computers, or in lockable cabinets behind a lockable door (when not under direct control of the responsible person. Secured website with SSL security certificate. Users can unsubscribe from electronic communication.	Where legally required to do so; when in public interest; when in the best interests of the firm; with consent of the prospective client.
<b>Clients</b>	Personal and demographic information (mode: mandate; FICA documents; consultations; documentary evidence; correspondence; website etc.)	Case management; billing of clients; correspondence with clients etc.	All information is stored on password protected computers, or in lockable cabinets behind a lockable door (when not under direct control of the responsible person. Secured website with SSL security certificate. Users can unsubscribe from electronic communication. Password protected login interface + Encryption.	Where legally required to do so; when in public interest; when in the best interests of the firm; with consent of the employee.

## RIGHTS OF DATA SUBJECTS:

15. The rights of data subjects under POPIA include the right to:

15.1. Be notified when personal information is collected or accessed by an unauthorised person.

In the event of a breach, The company will promptly notify the Regulator and affected data subjects.

Notifications will be issued in writing via mail, email, website, media, or as directed by the Regulator.

The notice will outline the nature of the breach, corrective actions taken, recommended protective measures, and, if known, the identity of the unauthorised party.

If necessary, The company will publicly disclose the breach to ensure data subjects are informed and protected, always prioritising transparency and compliance with regulatory requirements.

15.2. Establish whether a responsible party holds personal information and request access.

A previous, current, or prospective client (data subject), upon proving their identity, may request confirmation (free of charge) on whether The company holds their personal information. They may also request access to that information, including details of third-party access, within a reasonable time, format, and fee structure. The company will provide a fee estimate and may request a deposit. The data subject must be informed of their right to request correction. Access may be refused if valid grounds under the Promotion of Access to Information Act apply, but non-exempt information will still be disclosed.

15.3. Request correction, destruction, or deletion of personal information.

A data subject may request the correction or deletion of their personal information if it is inaccurate, outdated, irrelevant, or unlawfully obtained, or request its destruction if the The company is no longer authorised to retain it. Upon request, The company will act promptly by correcting, deleting, or justifying the information, or noting the unresolved dispute. If changes affect past or future decisions, affected third parties will be informed where practicable/ applicable. The company will also notify you of the action taken in response to the request.

The above may be requested by completing and submitting **form 2**, to the information officer.

- 15.4. Object to the processing of personal information on reasonable grounds.
- 15.5. Object to the processing of personal information for direct marketing purposes.
- 15.6. Not have personal information processed for direct marketing via unsolicited electronic communications.

A data subject has the right to object to the processing of their personal information on reasonable grounds relating to their specific situation.

This objection applies when processing is based on the The company's or a third party's legitimate interests, or when used for purposes like direct marketing. The objection must be made in the prescribed manner. Once an objection is lodged, The company will no longer process the information unless legislation permits it, or compelling legitimate grounds can be demonstrated that override the interests, rights, and freedoms of the data subject.

It must be understood that an objection to processing of certain information may result in The company being unable to execute its mandate, which may result in termination of the mandate by the responsible attorney.

The above may be requested by completing and submitting **form 1**, to the information officer.

- 15.7. Not be subject to decisions based solely on automated processing of personal information.

A data subject may not be subject to decisions with legal or significant effects based solely on automated processing, such as profiling for work performance, creditworthiness, or health. Exceptions apply if the decision is linked to a contract and protects the data subject's interests, or if governed by law or a code of conduct with safeguards. In such cases, The company will allow the data subject to make representations and provide enough information on the logic behind the automated decision to enable an informed response.

- 15.8. Submit complaints to the Information Regulator.

Any person may submit a written complaint to the Information Regulator, in the prescribed manner and form, if they believe their personal information has been interfered with or unlawfully processed. Additionally, a responsible party or data subject may lodge a complaint if aggrieved by an adjudicator's decision under section 63(3). The Regulator must provide reasonable assistance to individuals who require help in submitting their complaint.

For more information on how to lodge a complaint with the Regulator, please visit their website on <https://inforegulator.org.za/complaints/>.

- 15.9. Institute civil proceedings for interference with the protection of personal information.

A data subject, or the Regulator on their behalf, may institute civil action for damages against a responsible party for breach of POPIA, regardless of intent or negligence. Defences include vis major, plaintiff's consent or fault, impracticality, or exemption by the Regulator. Courts may award compensation for patrimonial and non-patrimonial loss, aggravated damages, interest, and legal costs. If the Regulator brings the action, awarded amounts are deposited into a trust, with expenses deducted and the remainder distributed to the data subject. Undistributed funds after three years revert to the Regulator. All court orders must be published. Settlements require court approval.

## GENERAL GUIDING PRINCIPLES:

16. The company is guided by the following 8 conditions/ guiding principles for the lawful processing of personal information:

### **Accountability:**

17. The company will take full responsibility for ensuring that all personal information is processed lawfully and in accordance with POPIA. This includes putting policies, procedures, and training in place to monitor and enforce compliance throughout the information lifecycle.

### **Processing limitation:**

18. We will only process personal information lawfully and for legitimate purposes. Processing will be minimal, relevant, and limited to what is necessary. Consent will always be obtained where required, and data will be collected directly from the data subjects unless otherwise justified.

### **Purpose specification:**

19. All personal information collected will be for a specific, explicitly defined, and lawful purposes. Records will not be kept longer than necessary unless required by law or for lawful retention. Retention and destruction practices will be clearly documented and enforced.

### **Further processing limitation:**

20. Further use of personal information will be compatible with the original purpose for which it was collected. If not, new justification or consent will be sought. We will evaluate compatibility based on the relationship between the purposes, the nature of the information, and its consequences.



**Information quality:**

21. Personal information must be complete, accurate, and kept up to date. The company will take reasonable steps to ensure the integrity of data at the time of collection and during use, especially when decisions are made based on that information.

**Openness:**

22. We will maintain documented processing activities and inform data subjects when collecting their personal information. Notification will include the purpose, source (if not direct), recipients, and the subject's rights, ensuring transparency and informed participation.

**Security safeguards:**

23. The company has implemented appropriate technical and organisational measures to secure personal information against loss, unauthorised access, or damage. Contracts with operators will ensure compliance, and we will notify affected parties and the Regulator of any security compromise.

**Data subject participation:**

24. Data subjects have the right to access their personal information and request correction or deletion where appropriate. Requests will be handled fairly, efficiently, and in the prescribed manner, ensuring transparency, responsiveness, and respect for data subject rights.

**STAFF TRAINING:**

25. All director/s, associates, managers and employees will be provided with a copy of this policy upon engagement, alternatively employment, and this policy will be prominently available at the firm's offices, and/ or on each director and employee's computer; save were in the latter instance the policy may also be availed on the firm's local intranet or network.
26. All director/s, associates, managers, and employees will receive in-service training, as applicable to their job function, in respect of the application of this policy.
27. Training will be provided on an ongoing informal basis, as well as on a more formal basis (by structured in-service training) at least once every two years or more frequently, subject to changes made to the Act.
28. Any amendments to this policy will be brought to the attention of each director/s, associate, manager and employee by distributing a copy thereof to the aforesaid persons and by prominently pointing out the material changes.

## REFERENCES:

Destroying Records – the legal effect, Michalson L <https://www.michalsons.com/blog/destroying-records-the-legal-effect/1093> (accessed November 2018).

Financial Intelligence Centre Act 38 of 2001.

Information Regulator (South Africa) <https://inforegulator.org.za/> (accessed: September 2025).

Protection of Information Act 84 of 1982.

Protection of Personal Information Act 4 of 2013, and regulations.

Rules made under section 95(1) of the Legal Practice Act 28 of 2014.

## FORM 1: OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

*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.*

<b>(A) DETAILS OF DATA SUBJECT</b>	
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
Contact number(s):	
Email address:	
<b>(B) DETAILS OF RESPONSIBLE PARTY</b>	
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
Contact number(s):	
Email address:	
<b>(C) REASONS FOR OBJECTION IN TERMS OF SECTION 11 (1) (d)</b>	
<b><i>(Please provide detailed reasons for the objection) – attach more pages if required</i></b>	

Signed on \_\_\_\_ of \_\_\_\_\_.

---

*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

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.

Mark with "X":

	<i>Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.</i>
	<i>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.</i>

(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):	
Email address:	
(B) DETAILS OF RESPONSIBLE PARTY	
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
Contact number(s):	
Email address:	
(C) INFORMATION TO BE CORRECTED/DELETED/ DESTROYED/ DESTROYED	
Attach more pages if required	

