

POPIA POLICY

1. Introduction

- 1.1. This Policy is implemented in compliance with the provisions of the Protection of *Personal Information* Act 4 of 2013 and its Regulations in order to give effect to the Constitutional right to privacy.
- 1.2. This Policy will regulate and protect *Personal Information* and the rights and interests of all *Data Subjects* who provide *Personal Information* to the Company.
- 1.3. The Company guarantees its commitment to protecting its Data Subject's privacy and ensuring that their *Personal Information* is used appropriately, transparently, securely and in accordance with applicable laws.

2. Scope

- 2.1. This Policy applies to all *Personal Information* processed by the Company in the exercise of its functions and obligations as a business entity, including the *Personal Information* of the Company's customers, employees and suppliers.

3. Definitions

- 3.1. "**Data Subject**" means the person to whom *Personal Information* relates, including Company employees;
- 3.2. "**Deputy Information Officer**" means any person(s) who have been designated by the Information Officer to perform certain delegated duties and responsibilities of the Information Officer;
- 3.3. "**Information Officer**" means the head of a private body being either the Chief Executive Officer, the acting Chief Executive Officer or an equivalent officer or any person duly authorized by that officer;
- 3.4. "**Operator**" means a person who processes *Personal Information* for a *Responsible Party* in terms of a contract of mandate, without coming under the direct authority of that party;
- 3.5. "**Personal Information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: -
 - 3.5.1. 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;
- 3.5.2. information relating to the education or the medical, financial, criminal or employment history of the person;
- 3.5.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- 3.5.4. the biometric information of the person;
- 3.5.5. the personal opinions, views or preferences of the person;
- 3.5.6. 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;
- 3.5.7. the views or opinions of another individual about the person;
- 3.5.8. 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;
- 3.6. **“POPIA”** means the Protection of *Personal Information* Act 4 of 2013;
- 3.7. **“Processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning *Personal Information*, including: -
- 3.7.1. the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- 3.7.2. dissemination by means of transmission, distribution or making available in any other form; or
- 3.7.3. merging, linking as well as restriction, degradation, erasure or destruction of information;
- 3.8. **“Process”** and **“Processed”** will have the same meaning;
- 3.9. **“Regulator”** means the Information Regulator established in terms of section 39 of *POPIA*;
- 3.10. **“Responsible Party”** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing *Personal Information*;
- 3.11. **“Special Personal Information”** means the *Personal Information* referred to in section 26 of *POPIA*, namely *Personal Information* concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a *Data Subject* or the criminal behaviour of a *Data Subject* to the extent that such information relates to the alleged commission of any offence by the *Data Subject* or any proceedings in

	POPIA POLICY	DRAFT 1
		Page 3/17

respect of any offence allegedly committed by a *Data Subject* or the disposal of such proceedings.

4. **Lawful Processing of Personal Information**

- 4.1. The Company is required, in the normal exercise of its functions and obligations as a juristic business entity, to process the *Personal Information* of *Data Subjects* from time to time.
- 4.2. In order to process such *Personal Information*, the Company as a *Responsible Party*, is required to comply with the eight conditions for lawful processing of *Personal Information*, as contained in *POPIA*, namely: -
 - 4.2.1. Accountability;
 - 4.2.2. Processing Limitation;
 - 4.2.3. Purpose Specification;
 - 4.2.4. Further Processing Limitation;
 - 4.2.5. Information Quality;
 - 4.2.6. Openness;
 - 4.2.7. Security Safeguards; and
 - 4.2.8. *Data Subject* Participation.
- 4.3. The Company's *Data Subjects* must ensure that they understand and are familiar with the conditions set out above as well as the other provisions of *POPIA* in order to ensure lawful processing of *Personal Information* at all times.
- 4.4. In the event that the Company's *Data Subjects* are unsure of any issues related to *POPIA* or the handling, collection or Processing of *Personal Information*, they must contact the Company's Deputy Information Officer and/or any other person designated by the Company to obtain clarification.

5. **Conditions for Lawful Processing**

Accountability

- 5.1. The Company must ensure that the conditions set out above are complied with: -
 - 5.1.1. at the time that the purpose for which the *Personal Information* is being Processed is determined;
 - 5.1.2. at the time that the method of Processing such *Personal Information* is determined; and
 - 5.1.3. during the Processing of the *Personal Information*.

Processing Limitation

- 5.2. The Processing of the *Personal Information* must be lawful and conducted in a reasonable manner that does not infringe on the privacy of the *Data Subject*. The *Personal Information* Processed must, in light of the purpose for the Processing of the *Personal Information*, be adequate, relevant and not excessive.
- 5.3. The Company collects and processes a Data Subject's Personal Information pertaining to the Data Subject's needs. The type of information will depend on the need for which it is collected and will be processed for that purpose only, subject to the provisions of POPIA. Whenever possible, the Company will inform the Data Subject of the information required and the information deemed optional. Examples of personal information collected includes:-
- 5.3.1. Payment particulars;
 - 5.3.2. Description of the Data Subject's residence, contact information;
 - 5.3.3. Email particulars;
 - 5.3.4. Web address;
 - 5.3.5. Telephone and mobile phone numbers;
 - 5.3.6. Banking details, etc.,
 - 5.3.7. For purposes of this Policy, data subjects include potential and existing data subjects.
- 5.4. The Company will seek to obtain the consent of all *Data Subjects* prior to the Processing of their *Personal Information*. This informed consent requires that the *Data Subject* should understand the purpose of Processing of the *Personal Information*. Such consent must be obtained in writing.
- 5.5. In obtaining consent from a *Data Subject*, the *Data Subject* must be aware that the Company will be responsible for proving that the *Data Subject's* consent was obtained. Notwithstanding this, failure to obtain such consent will not preclude the Company from Processing the *Personal Information* of *Data Subjects* in certain circumstances where it is permitted in accordance with the provisions of *POPIA*.
- 5.6. Any consent provided by a *Data Subject* may be withdrawn by that *Data Subject* at any time after such consent was obtained by the Company.
- 5.7. A *Data Subject* may object to the Processing of *Personal Information* at any time, should such information not be utilized for the purposes it was intended for, and should such withdrawal of consent not be in contravention of any legislative requirements and shall not interfere with the ability of the Company to continue to

	POPIA POLICY	DRAFT 1
		Page 5/17

manage the employment relationship.

- 5.8. A request to withdraw or object to the Processing of the *Personal Information* must be brought to the attention of a responsible person at the Company in writing and in accordance with **Annexure A**, in order to ensure that the matter is handled appropriately. Any such request for withdrawal of consent must also fully disclose the reason for the request to withdraw consent. In circumstances where the consent is withdrawn, the Company may no longer process the *Personal Information*, unless otherwise permitted in terms of the provisions of POPIA.

Purpose Specification

- 5.9. The Company may only Process *Personal Information* for a specific, explicitly defined and lawful purpose related to the exercise of its functions and obligations as a business entity. Such purpose must be identified and explained to the *Data Subject* and must be recorded in the applicable consent forms (where applicable). This may include:-
- 5.9.1. providing products or services to data subjects and to carry out the transactions requested;
 - 5.9.2. for sharing with other third parties, if necessary;
 - 5.9.3. conducting credit reference searches or verification;
 - 5.9.4. confirming, verifying and updating data subject details;
 - 5.9.5. for purposes of claims history;
 - 5.9.6. for the detection and prevention of fraud, crime, money laundering or other illegal acts
 - 5.9.7. for audit and record-keeping purposes;
 - 5.9.8. in connection with legal proceedings;
 - 5.9.9. providing services to data subjects, to render the services requested and to maintain and constantly improve the relationship;
 - 5.9.10. providing communication in respect of the Company and regulatory matters that may affect data subjects; and
 - 5.9.11. in connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.
- 5.10. Subject to the provisions of *POPIA*, records of *Personal Information* must not be retained by the Company any longer than is necessary for achieving the purpose for which the *Personal Information* was processed.

- 5.11. The Processing of *Personal Information* must be restricted in certain instances as set out in *POPIA*. Where the Processing of *Personal Information* is restricted, the Company must inform the *Data Subjects* before lifting the restriction on Processing. The Company will restrict processing of *Personal Information* where:-
- 5.11.1. the accuracy of the *Personal Information* is contested by the *Data Subject* for a period enabling the Company to verify the accuracy of the *Personal Information*;
 - 5.11.2. The Company no longer needs the *Personal Information* for achieving the purpose for which the *Personal Information* was collected (but it has to be maintained for purposes of proof);
 - 5.11.3. the Processing is unlawful and the *Data Subject* opposes the destruction or deletion of the *Personal Information* and requests the restriction of its use or the return of the information instead; or
 - 5.11.4. the *Data Subject* requests to transmit the *Personal Information* into another automated Processing System.
- 5.12. *Personal Information* must be destroyed, deleted or de-identified, in a manner that prevents its reconstruction in an intelligible form, as soon as reasonably practicable once the purpose of its use is met or as soon as the Company is no longer authorised to retain the *Personal Information*, subject to the provisions of *POPIA*.

Further processing limitation

- 5.13. The Company may from time to time be required to perform further Processing of *Personal Information*.
- 5.14. In instances where further Processing of *Personal Information* is required after the initial Processing of the *Personal Information* and the further Processing of *Personal Information* is not compatible with the initial purpose of the Processing of the *Personal Information*, as identified and explained to the *Data Subject*, the Company shall seek to obtain the consent of the *Data Subject* for purposes of such further Processing.
- 5.15. Notwithstanding this, failure to obtain such consent will not preclude the Company from further Processing of the *Personal Information* of *Data Subjects* in certain circumstances where it is permitted to do so as set out in *POPIA*.

Information Quality

- 5.16. The Company's Employees must take reasonably practicable steps to ensure that all *Personal Information* is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the *Personal Information* of *Data Subjects* is being collected or further processed.

	POPIA POLICY	DRAFT 1
		Page 7/17

Openness

- 5.17. Having regard to the specific circumstances in which the *Personal Information* is or is not to be Processed, and in accordance with *POPIA*, the Company's employees must ensure that the *Data Subjects* are aware of the following before the *Personal Information* is collected or, if collected from any source other than directly from the *Data Subjects*, as soon as reasonably practicable after it has been collected: -
- 5.17.1. the information being collected and where the *Personal Information* is not collected from the *Data Subject*, the source from which it is collected;
 - 5.17.2. the name and address of the Company, as the Responsible Party;
 - 5.17.3. the purpose for which the *Personal Information* is being collected;
 - 5.17.4. whether or not the supply of the *Personal Information* by that *Data Subject* is voluntary or mandatory;
 - 5.17.5. the consequences of failure to provide the *Personal Information*;
 - 5.17.6. any particular law authorising or requiring the collection of the *Personal Information*;
 - 5.17.7. the fact that, where applicable, the Company intends to transfer the information to a third country or international organisation and the level of protection afforded to the *Personal Information* by that third country or international organisation;
 - 5.17.8. Any further information such as the: -
 - 5.17.8.1. recipient or category of recipients of the *Personal Information*;
 - 5.17.8.2. nature or category of the *Personal Information*;
 - 5.17.8.3. existence of the right of access to and the right to rectify the *Personal Information* collected;
 - 5.17.8.4. the existence of the right to object to the Processing of *Personal Information*; and
 - 5.17.8.5. the right to lodge a complaint to the Regulator and the contact details of the Regulator.
- 5.18. The Company has prepared a consent form in terms of which it sets out the above information. Notwithstanding the consent form, it is the responsibility of the Company's employees to ensure that the information is communicated to the *Data Subject* (where seeking their *Personal Information*) in accordance with *POPIA*.

Security Safeguards

- 5.19. The Company's employees must treat any and all *Personal Information* collected

	POPIA POLICY	DRAFT 1
		Page 8/17

and/or Processed by it as confidential and must not disclose it to any other party and must make every effort to secure the integrity and confidentiality of the *Personal Information* collected by following appropriate procedures regarding security of *Personal Information*.

- 5.20. Appropriate, reasonable technical and organisational measures must be taken to prevent loss of, damage to or unauthorised destruction of *Personal Information* and unlawful access to or Processing of *Personal Information*
- 5.21. The Company will continuously review its security controls and processes to ensure that personal information is secure.
- 5.22. The Company is a wholly owned subsidiary within the EDF Group.
- 5.23. The EDF Group and its shareholders expect from all its directors, officers, and employees strict adherence to the principle of legality, but also - except if a local country law or regulation provides explicitly otherwise - strict adherence to the corporate governance framework of the EDF Group.
- 5.24. The EDF Group has drafted specific documents, applicable worldwide as mentioned earlier, regulating our IT security and the protection of personal information, including a data retention policy and personal information breach policy.
- 5.25. Any internal or external risks to the *Personal Information* must be reported by the Company's Employees to one of the Company's Deputy Information Officers or any other person designated by the Company.
- 5.26. The Company may appoint Operators to Process *Personal Information* and to establish and maintain security measures to safeguard against any risks identified. Such Operator will only process such information with the knowledge and authorisation of the Company and must treat the *Personal Information* as confidential and not disclose it. Such Operator will notify the Company where there are reasonable grounds to believe that the *Personal Information* of *Data Subjects* has been accessed or acquired by an unauthorised person.
- 5.27. Should the confidentiality of the *Personal Information* be compromised, this must be reported as soon as reasonably possible to The Company's Deputy Information Officer and/or any other designated person at the Company. The Regulator must be notified and the *Data Subject* must be notified in writing informing the *Data Subject* of any protective measures the Company intends to take.

Data Subject Participation

- 5.28. The *Data Subject* may, after providing adequate proof of their identity, request access to relevant *Personal Information*, which must then be provided to the *Data Subject*.

- 5.29. The Company may refuse access where the provisions of the Promotion of Access to Information Act are applicable.
- 5.30. The *Data Subject* must be advised of the right to correct the *Personal Information*.
- 5.31. The *Data Subject* may request that their *Personal Information* be corrected or deleted or that a record containing *Personal Information* of the *Data Subject* be destroyed or deleted if the *Data Subject* believes that the *Personal Information* or record of the *Personal Information* is:-
- 5.31.1. inaccurate;
 - 5.31.2. irrelevant;
 - 5.31.3. excessive;
 - 5.31.4. out of date;
 - 5.31.5. incomplete;
 - 5.31.6. misleading; or
 - 5.31.7. has been obtained unlawfully.
- 5.32. If the Company receives such a request it must, as soon as reasonably practicable, and in compliance with *POPIA*:-
- 5.32.1. correct the *Personal Information*;
 - 5.32.2. destroy or delete the *Personal Information*;
 - 5.32.3. provide the *Data Subject*, to his or her satisfaction, with credible evidence in support of the *Personal Information*; or
 - 5.32.4. where agreement cannot be reached between the Company and the *Data Subject*, and if the *Data Subject* so requests, take such steps as are reasonable in the circumstances to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

6. Processing of Special *Personal Information*

- 6.1. The Company will seek to obtain the specific consent of all *Data Subjects* to the Processing of their Special *Personal Information*. Notwithstanding this, failure to obtain such consent will not preclude the Company from Processing the Special *Personal Information* in certain circumstances where it is expressly permitted to do so in accordance with the provisions of *POPIA*.

7. *Personal Information* of Employees and Job Applicants

- 7.1. In addition to what has been set out above, the following principles are particularly

important in respect of the *Personal Information* of the Company's Employees and job applicants.

Recruitment and Appointment

- 7.2. The Company may, from time to time, need to Process various *Personal Information* about a job applicant in connection with the recruitment process. The Company will ensure that when processing a job applicant's *Personal Information*, it will adhere to its obligations in accordance with the provisions of *POPIA*.
- 7.3. In addition, and as a consequence of the employment relationship entered into between the Company and its employees, the Company will Process various *Personal Information* about an Employee in connection with the employment relationship. The Company will ensure that in processing an Employee's *Personal Information*, it will adhere to its obligations in accordance with the provisions of *POPIA*.
- 7.4. The Company will take reasonably practicable steps to ensure that the job applicant or the Employee understands the purpose for the Processing of their *Personal Information* and that informed consent is obtained from the Job Applicant or the Employee prior to processing any of their *Personal Information*.
- 7.5. Notwithstanding this, failure to obtain such consent will not preclude the Company from Processing the *Personal Information* in certain circumstances where it is permitted to do so in accordance with the provisions of *POPIA*.
- 7.6. The Company must collect *Personal Information* from the job applicant or the employee directly unless the information is derived from a public record or has been deliberately made public by the job applicant or the employee.
- 7.7. The Company will take all reasonable steps to ensure that the job applicant's *Personal Information* will only be used for purposes connected to recruitment and marketing purposes related to recruitment and the employment relationship.

8. Storage of Personal Information of Employees

- 8.1. In instances where further Processing is required after the initial Processing of the *Personal Information* and the further Processing does not correspond with the initial purpose of Processing of the *Personal Information*, the Company is required to acquire further consent from the Employee for the further Processing of the *Personal Information* or as further permitted in accordance with the provisions of *POPIA*.
- 8.2. The Company will take reasonably practicable steps to ensure that all *Personal Information* collected is complete, accurate and not misleading, having regard to the purpose for which the *Personal Information* is being processed.
- 8.3. The Company will provide a means for Employees to review the accuracy of their

Personal Information and a means to rectify inaccurate *Personal Information*. Employees must report any inaccuracies to the Company's Personnel responsible for the administration of *Personal Information* in accordance with **Annexure B**.

- 8.4. Employees are entitled to request access to their *Personal Information*. The responsible Company Personnel will respond to these requests and may, if permissible in terms of the Promotion of Access to Information Act 2 of 2000 ("PAIA"), provide the information requested within a reasonable time and on payment of the prescribed fee. Should the Company refuse to grant access, reasons shall be furnished.
- 8.5. The Company will take all reasonably practicable steps to ensure that all Processed *Personal Information* remains confidential and is not distributed to unauthorised third parties.
- 8.6. The Company will appoint Operators to Process *Personal Information* and to establish and maintain security measures to safeguard against any risks identified. The Operator will only process such information with the knowledge and authorisation of the Company. The Operator will notify the Company where there are reasonable grounds to believe that the *Personal Information* of Employees has been accessed or acquired by an unauthorised person.
- 8.7. Any Operator processing *Personal Information* on behalf of the Company or any Personnel who has access to *Personal Information* of Employees will treat the *Personal Information* which comes to their knowledge as confidential and will not disclose it.
- 8.8. Some of the *Personal Information* relating to the Company's employees and job applicants is stored in a database located in South Africa and France. The database is controlled by the Company's administrative staff and can be accessed electronically from South Africa. The Company has security measures in place which will ensure the confidentiality of the information contained in the database and these measures will be reviewed over time and upgraded in line with technological developments and in accordance with POPIA.
- 8.9. The Company will seek to obtain the consent of all Data Subjects to the transfer of their *Personal Information* between South Africa and any other country should this become necessary in due course.
- 8.10. In obtaining such consent from *Data Subjects* and/or Company Employees, *Data Subjects* must be aware that the Company will be responsible for proving that the *Data Subjects* and/or the Company's Employee's consent was obtained. Notwithstanding this, failure to obtain such consent will not preclude the Company from transferring the *Personal Information* of *Data Subjects* in certain circumstances where it is permitted to do so strictly as set out in *POPIA*.
- 8.11. The remainder of the *Personal Information* is contained in personnel folders which are safely kept in the People & Culture Department, to which access is limited to People & Culture Department members only.

- 8.12. Certain Data is captured also on PaySpace for Payroll Processing profiles as well as with Benefits brokers for their records.
- 8.13. Upon termination of employment with the Company, *Personal Information* will be handed to the relevant Operators for the purposes of post-employment benefits, if any, and save as required by law, thereafter will be destroyed, deleted and/or de-identified.

9. Distribution of *Personal Information* to Third Parties

- 9.1. The Company may provide access to or transfer an Employee's *Personal Information* where it is necessary for the purposes for which the *Personal Information* is processed.
- 9.2. Such third parties include but are not limited to the Company's branches, subsidiaries or affiliated companies, the Company's registered clients, parties providing products and services to the Company, regulatory authorities or as required by law.

10. Transborder Information Flows

- 10.1. The Company will only transfer the *Personal Information* of a data subject to a third party who is in a foreign country if:-
- 10.1.1. The third-party is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection and which is substantially similar to the conditions of lawful processing in POPIA and which includes provisions which are substantially similar to section 72 of POPIA; or
 - 10.1.2. The *Data Subject* consents to the transfer; or
 - 10.1.3. The transfer is necessary for the performance of a contract between the *Data Subject* and the Company; or
 - 10.1.4. The transfer is necessary for the implementation of pre-contractual measures taken in response to the *Data Subject's* request; or
 - 10.1.5. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the *Data Subject* between the Company and a third party; or
 - 10.1.6. The transfer is for the benefit of the *Data Subject* and it is not reasonably practicable to obtain his/her/its consent and if such consent could have been obtained the data subject would have given it.

11. Information Officer

- 11.1. The details of the Information Officer are set out below. The Information Officer shall perform the duties set out in *POPIA* and be responsible for all issues dealt with in this Policy.
- 11.2. The Company shall also appoint one or more Deputy Information Officers as it deems necessary to assist the Information Officer and to comply with section 56 of *POPIA*.

INFORMATION OFFICER DETAILS:

NAME: Tracey Chas
TELEPHONE NUMBER: 0769579264
E-MAIL ADDRESS: Tracey.Chas@edf-re.co.za

DEPUTY INFORMATION OFFICER DETAILS:

NAME: Helen Du Plessis
TELEPHONE NUMBER: 0826157314
EMAIL ADDRESS: Helen.Duplessis@edf-re.co.za

COMPANY DETAILS:

TELEPHONE NUMBER: [021 657 4200](tel:0216574200)
POSTAL ADDRESS: 1 Oakdale Road, Newlands,
Cape Town, South Africa,
7700
PHYSICAL ADDRESS: 1 Oakdale Road, Newlands,
Cape Town, South Africa,
7700
E-MAIL ADDRESS: legalcompliance@edf-re.co.za ;
info@edf-re.co.za
WEBSITE: <https://edf-re.co.za/>

12. Review

- 12.1. Changes to POPIA and its Regulations will be monitored by the Company and further amendments may be required to this Policy in order for the Company to remain compliant with its legal obligations.

[illegible]

Signed at this day of20....

.....
Signature of Data Subject (applicant)

ANNEXURE “B” 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 POPIA

Note:

1. Affidavits or other documentary evidence in support of the objection must 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.

Reference Number

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 authorised to retain the record of information.

A: DETAILS OF DATA SUBJECT

Name and surname of <i>Data Subject</i> :	
Residential, postal or business address:	Code ()
Contact number(s):	
Fax number:	
E-mail address:	

B: DETAILS OF RESPONSIBLE PARTY

Name and surname of responsible party (if the responsible party is a natural person):	
Residential, postal or business address:	Code ()
Contact number(s):	
Fax number:	
E-mail address:	
Name of public or private body (if the responsible party is not a natural person):	
Residential, postal or business address:	Code ()
Contact number(s):	
Fax number:	
E-mail address:	

C: REASONS FOR *CORRECTION OR DELETION OF THE *PERSONAL INFORMATION* ABOUT THE *DATA SUBJECT* / *DESTRUCTION OR DELETION OF A RECORD OF *PERSONAL INFORMATION* ABOUT THE *DATA SUBJECT* WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY (*Please provide details for the request*)

****Delete whichever is not applicable***

Signed at this day of 20.....

.....
Signature of Data Subject