Ground Floor, East View
Bryanston Place Office Park
199 Bryanston Drive, Bryanston
P O Box 67806, Bryanston, 2021

FABER GOËRTZ
ELLIS AUSTEN INC

Tel: 010 590 3378
Fax: 086 675 6808
E-mail: stephanie@fgea.co.za
Website: www.fgea.co.za

FABER GOËRTZ ELLIS AUSTEN INCORPORATED

2006/019504/21

COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

I N D E X

A. INTRODUCTION

1. Our firm is committed to protecting your privacy, as it has always done so, and ensuring transparency in how we collect, handle and store your data.

2. This Compliance Manual sets out the framework for our firm's compliance with POPI and details how we process your personal information.

3. Where reference is made to the "processing" of personal information, this will include any operation or activity concerning personal information, including:

   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; or merging, linking as well as restriction, erasure or destruction, regardless of whether the information is worked with manually, or by automated systems.

B. SUBJECTS AND CATEGORIES OF RECORDS HELD BY THE COMPANY

4. INFORMATION REGARDING CLIENTS

4.1 Client's full names/Company name;

4.2 Client Identity Number/Company Registration Number;

4.3 Copies of identity documents of directors and/or shareholders;

4.4 Telephone numbers;

4.5 Email addresses;

4.6 Business addresses;

4.7 Residential addresses;

4.8 Banking details;

4.9 Financial information including but not limited to banking confirmation, annual financial statements, assets and liabilities, debtors lists and management accounts;

4.10 Copies of statutory tax registrations and SARS related documents and correspondence;

4.11 Copies of Last Wills and Testaments;

4.12 Copies of Trust Deeds; and

4.13 Title Deeds

5. STATUTORY COMPANY INFORMATION

5.1 Certificate of Incorporation

5.2 Registration Certificate

5.3 Memorandum of Incorporation

5.4 Minutes of Board Meetings

5.5 Resolutions passed

5.6 Share certificates

5.7 Company disclosure certificates

5.8 Register of directors and public officers

5.9 Annual Financial Statements

5.10 Management Accounts

5.11 Director Reports

5.12 Auditors Reports

5.13 Books of Account

5.14 Supporting schedules and documentation relating to management accounts

6. CORPORATE GOVERNANCE

6.1 Code of conduct

6.2 Risk Management Registers

6.3 Legal Compliance Registers

8.10 PAYE records and returns

8.11 Returns to UIF

8.12 Payroll records

9. **HUMAN RESOURCES**

9.1 BEE Statistics

9.2 Personnel information

9.3 General terms of employment

9.4 Letters of employment

9.5 Leave records

9.6 Performance Management records

9.7 Retirement Benefit and Medical Aid records

9.8 Training manuals

9.9 Policies and procedures

9.10 CV's

9.11 Disciplinary codes and records

9.12 Job profiles

9.13 Social Responsibility

10. **FIXED PROPERTY**

10.1 Title deeds of all immovable property owned by the Company

10.2 Leases

10.3 Building plans

10.4 Mortgage bonds

10.5 Register of all immovable property owned by the company

11. MOVABLE PROPERTY

11.1 Asset Register

11.2 Finance and lease agreements

11.3 Notarial Bonds

11.4 Deeds of pledge

11.5 Vehicle registration documents

12. INTELLECTUAL PROPERTY

12.1 Agreements relating to intellectual property such as license agreements, secrecy agreements, research and development agreements, consulting agreements, use agreements, joint venture agreements

12.2 Litigation and other disputes involving intellectual property

12.3 Know-how

13. AGREEMENTS AND CONTRACTS

13.1 Shareholder's agreements

13.2 Acquisition or disposal agreements

13.3 Supplier, contractor and service provider agreements

13.4 Mandates

13.5 Sale agreements

13.6 Agency agreements

13.7 Restraint agreements

13.8 Non-disclosure agreements

13.9 Agreements with governmental agencies

13.10 Purchase or lease agreements

14. **TAXATION**

14.1 Copies of registration details for all statutory taxes

14.2 Copies of all statutory tax returns for the past 5 years

14.3 Correspondence with SARS

14.4 Assessments raised by SARS

14.5 Proof of all payments made to SARS

15. **LEGAL**

15.1 Complaints, pleadings, briefs and other documents relating to any current, pending and threatened litigation and/or commercial disputes against the Company and/or its clients

15.2 Settlement agreements

15.3 Material licenses, permits and authorisations

15.4 Agreements and contracts

15.5 Competition notifications

15.6 SAPS investigations and cases

15.7 Record of stolen goods

15.8 Subpoenas

15.9 Disputes with ex-employees

16. **INSURANCE**

16.1 Insurance policies

16.2 Claim records

16.3 Details of insurance coverage, limits and insurers

16.4 Insurance declaration

17. **INFORMATION TECHNOLOGY**

17.1 Hardware

17.2 Telephone exchange equipment

17.3 Telephone lines

17.4 Disaster recovery policy and systems

17.5 Internal systems support

17.6 Contracts and agreements with service provider

17.7 Licenses

17.8 Policies, procedures, standards, templates and guidelines

17.9 Faults, troubleshooting and reporting

17.10 Performance of IT infrastructure

17.11 Security access

C. OUR UNDERTAKINGS TO OUR CLIENTS

18. We undertake to remain compliant with POPI at all relevant times and to process personal information lawfully and reasonably, so as not to unnecessarily infringe on the privacy of our clients.

19. We undertake to only process personal information that is adequate, relevant and not excessive.

20. We undertake to process information only for the purpose for which it is intended, to enable us perform in terms of our mandate to which our client has signed.

21. Whenever necessary, we shall obtain consent in order to process personal information.

22. Where we do not seek consent, the processing of our client's personal information will be following a legal obligation placed upon us, or to protect a legitimate interest that requires protection.

23. We shall cease the processing of personal information if the required consent is withdrawn, or if a legitimate objection is raised.

24. We shall collect personal information directly from the client whose information we require, unless:

    24.1 the information is of public record; or

    24.2 the client has consented to the collection of their personal information from another source; or

    24.3 the collection of the information from another source does not prejudice the client; or

    24.4 the information is being collected to comply with a legal obligation, including an obligation to SARS; or

    24.6 the information collected is required for the conduct of proceedings in any court or tribunal, where these proceedings have commenced or are reasonably contemplated; or

    24.7 the information is required to maintain our legitimate interests; or

    24.8 where requesting consent would prejudice the purpose of the collection of the information; or

    24.9 where requesting consent is not reasonably practical in the circumstances.

25. We shall advise our clients of the purpose of the collection of the personal information before the information is collected or as soon as reasonably practicable.

26. We shall retain records of the personal information we have collected for the minimum period as required by law unless the client has furnished their consent or instructed us to retain the records for a longer period.

27. We shall destroy or delete records of the personal information (so as to 'de-identify' the client) as soon as reasonably possible after the time period for which we were entitled to hold the records have expired.

28. We shall restrict the processing of personal information:

    28.1 where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information;

    28.2 where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for the purposes of proof;

    28.3 where the client requests that the personal information is not destroyed or deleted, but rather retained; or

    28.4 where the client requests that the personal information be transmitted to another automated data processing system.

29. The further processing of personal information shall only be undertaken:

    29.1 if the requirements of paragraphs 19 – 27 above have been met;

    29.2 where the further processing is necessary because of a threat to public health or public safety or to the life or health of the client, or a third person;

    29.3 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or

    29.4 where this is required by the Information Regulator appointed in terms of POPI.

30. We undertake to ensure that the personal information which we collect and process is complete, accurate, not misleading and up to date.

31. We undertake to retain the physical file and the electronic data related to the processing of the personal information.

32. We undertake to take special care with our client's bank account details, and we are not entitled to obtain or disclose or procure the disclosure of such banking details unless we have the client's specific consent.

33. **Form 1** referred to in Section P below shall be sent to every client when we accept a mandate of any sort, to advise them of our duty to them in terms of POPI.

D. OUR CLIENT'S RIGHTS

34. In cases where the client's consent is required to process their personal information, this consent may be withdrawn.

35. In cases where we process personal information *without* consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the client has the right to object to such processing.

36. All clients are entitled to lodge a complaint regarding our application of POPI with the Information Regulator.

37. **Form 2** referred to in Section P below shall be completed by each client when we accept a mandate of any sort, to obtain the client's consent to process their personal information while we carry out our mandate, unless this consent has been obtained within another document signed by the client.

E. SECURITY SAFEGUARDS

38. In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, we have and continue to implement the following security safeguards:

    38.1 Our business premises where records are kept remain protected by access control, alarms and armed response.

    38.2 Archived files are off-site and access control to these storage facilities are implemented.

38.3 All the user terminals on our internal computer network and our servers are protected by passwords which must be changed on a regular basis.

38.4 Our email infrastructure complies with industry standard security safeguards, and we employ up to date technology to ensure the confidentiality, integrity and availability of the personal information in our care.

38.5 Vulnerability assessments are carried out on our digital infrastructure at least on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place.

38.6 We use an internationally recognised Firewall to protect the data on our local servers, and we run continuous antivirus protection to ensure our systems are kept updated with the latest patches.

38.7 Our staff are trained to carry out their duties in compliance with POPI, and this training is ongoing.

38.8 It is now a term of the contract with every staff member that they must maintain full confidentiality in respect of all of our clients' affairs, including our clients' personal information.

38.9 Employment contracts for staff whose duty it is to process a client's personal information, includes an obligation on the staff member to maintain the Company's security measures, and to notify their manager/supervisor immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person.

38.10 The processing of the personal information of our staff members take place in accordance with the rules contained in the relevant labour legislation.

38.11 The digital work profiles and privileges of staff who have left our employ is properly terminated.

38.12 The personal information of clients and staff are destroyed timeously in a manner that de-identifies the person.

39. These security safeguards are verified on a regular basis to ensure effective implementation, and these safeguards must be continually updated in response to new risks or deficiencies.

F. SECURITY BREACHES

40. Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, we must notify the Information Regulator and the relevant client/s, unless we are no longer able to identify the client/s. This notification must take place no later than 72 hours after the breach has occurred or as soon as reasonably possible.

41. Such notification must be given to the Information Regulator *first* as it is possible that they, or another public body, might require the notification to the client/s be delayed.

42. The notification to the client must be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the client:

42.1 by mail to the client's last known physical or postal address;

42.2 by email to the client's last known email address;

42.3 by publication on our website or in the news media; or

42.4 as directed by the Information Regulator.

43. This notification to the client must give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and must include:

43.1 a description of the possible consequences of the breach;

43.2 details of the measures that we intend to take or have taken to address the breach;

43.3 the recommendation of what the client could do to mitigate the adverse effects of the breach; and

43.4 if known, the identity of the person who may have accessed, or acquired the personal information.

G. CLIENTS REQUESTING RECORDS

44. On production of proof of identity, any person is entitled to request that we confirm, **free of charge**, whether or not we hold any personal information about that person in our records.

45. If we hold such personal information, on request, we shall provide the person with the record, or a description of the personal information, including information about the identity of all third parties or categories of third parties who have or have had access to the information. We shall do this within a reasonable period of time, in a reasonable manner and in an understandable form.

46. A client requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request shall be made on the prescribed application form.

47. In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have discretion as to whether or not to do so.

48. In all cases where the disclosure of a record will entail the disclosure of information that is additional to the personal information of the person requesting the record, the written consent of the Information Officer (or his/her Deputy) will be required, and that person shall make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.

49. If a request for personal information is made and part of the requested information may, or must be refused, every other part must still be disclosed.

H. THE CORRECTION AND DESTRUCTION OF PERSONAL INFORMATION

50. A client is entitled to require us to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

51. A client is also entitled to require us to destroy or delete records of personal information about the client that we are no longer authorised to retain.

52. Any such request must be made on the prescribed form.

53. Upon receipt of such a lawful request, we must comply as soon as reasonably practicable.

54. In the event that a dispute arises regarding the client's rights to have information corrected, and in the event that the client so requires, we must attach to the information, in a way that it will always be read with the information, an indication that the correction of the information has been requested but has not been made.

55. We must notify the client who has made a request for their personal information to be corrected or deleted what action we have taken as a result of such a request.

I. SPECIAL PERSONAL INFORMATION

56. Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.

57. We shall not process any of this Special Personal Information without the client's consent, or where this is necessary for the establishment, exercise or defense of a right or an obligation in law.

58. Having regard to the nature of our work, it is unlikely that we will ever have to process special personal information, but should it be necessary the guidance of the Information Officer, or their deputy, must be sought.

J. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

59. We may only process the personal information of a child if we have the consent of the child's parent or legal guardian.

K. INFORMATION OFFICER

60. Our Information Officer is **STEPHANIE BLAKE** who is an associate Legal Practitioner and has been nominated by the Partners in writing. Our Information Officer's responsibilities include:

    60.1 Ensuring compliance with POPI.

    60.2 Dealing with requests which we receive in terms of POPI.

    60.3 Working with the Information Regulator in relation to investigations.

61. Our Information Officer has designated **NICHOLAS MCAUGHLIN** and **MATTHEW NICHOLLS** as Deputy Information Officers.

62. Our Information Officer and our Deputy Information Officers have registered themselves with the Information Regulator.

63. In carrying out their duties, our Information Officer must ensure that:

    63.1 this Compliance Manual is implemented;

    63.2 a Personal Information Impact Assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;

    63.3 that this Compliance Manual is developed, monitored, maintained and made available;

    63.4 that internal measures are developed together with adequate systems to process requests for information or access to information;

63.5 that internal awareness sessions are conducted regarding the provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator; and

63.6 that copies of this manual are provided to persons at their request, hard copies to be provided upon payment of a fee (to be determined by the Information Regulator).

L. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

64. In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:

64.1 In the event that we intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;

64.2 if we are processing information on criminal behaviour or unlawful or objectionable conduct;

64.3 if we are processing information for the purposes of credit reporting (this will be important if we are making reports to assist with tenant profiling, for example, to TPN or ITC).

64.4 if we are transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

65. The Information Regulator must be notified of our intention to process any personal information as set out above prior to any processing taking place and we may not commence with such processing until the Information Regulator has decided in our favour. The Information Regulator has 4 weeks to make a decision but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator, which must not exceed 13 weeks. If the Information Regulator does not make a decision within the stipulated time periods,

we can assume that the decision is in our favour and commence processing the information.

M. DIRECT MARKETING

66. We may only carry out direct marketing (using any form of electronic communication) to clients if:

    66.1 they were given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected; and

    66.2 they did not object then or at any time after receiving any such direct marketing communications from us.

67. We may only approach clients using their personal information, if we have obtained their personal information in the context of providing services associated with our mandate, and we may then only market legal services to them.

68. We may only carry out direct marketing (using any form of electronic communication) to other people if we have received their consent to do so.

69. We may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent.

70. A request for consent to receive direct marketing must be made in the prescribed manner and form.

71. All direct marketing communications must disclose our identity and contain an address or other contact details to which the client may send a request that the communications cease.

N. TRANSBORDER INFORMATION FLOWS

72. We may not transfer a client's personal information to a third party in a foreign country, unless:

    72.1 the client consents to this, or requests it; or

72.2 such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country; or

72.3 the transfer of the personal information is required for the performance of the contract between ourselves and the client; or

72.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between ourselves and the third party; or

72.5 the transfer of the personal information is for the benefit of the client and it is not reasonably possible to obtain their consent and that if it were possible the client would be likely to give such consent.

O. OFFENCES AND PENALTIES

73. POPI provides for serious penalties for the contravention of its terms. For minor offences a guilty party can receive a fine or be imprisoned for up to 12 months. For serious offences the period of imprisonment rises to a maximum of 10 years. Administrative fines for the company can reach a maximum of R10 million.

73. Breaches of this Compliance Manual will also be viewed as a serious disciplinary offence.

73. It is therefore imperative that we comply strictly with the terms of this Compliance Manual and protect our client's personal information in the same way as if it was our own.

P. SCHEDULE OF ANNEXURES AND FORMS

74. Privacy Notice (to be attached to Mandate)

75. Consent to process personal information (to be attached to Mandate)

76. Objection to the Processing of Personal Information (Form 1 of the Regulations & to be attached to Mandate).

77. Request for correction or deletion of personal information (Form 2 of the Regulations).

78. Application for consent to direct marketing (Form 4 of the Regulations)

79. Addendum to the employee's letter of appointment

PRIVACY NOTICE

THE PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013

OUR DUTY TO YOU

Dear Client

1. The Protection of Personal Information Act, 4 of 2013 (POPI) is now in operation and we are committed to protecting your privacy and ensuring transparency in how we collect, process and retain your data.

2. POPI requires us to provide you with the details on how we process your personal information and in particular, what information we collect, why we collect such information, how we go about collecting such information, the parties with whom we may distribute this information to and your rights and obligations as the legal data subject.

THE COLLECTION AND PROCESSING OF PERSONAL INFORMATION

3. We will request and collect the majority of your personal information directly from yourself. This will include, but is not limited to your full names, identity number, company name and registration number, copies of identity documents, copies of company registration documents, telephone numbers, email addresses, business address, residential address, postal address as well as financial and tax information.

4. We will be collecting your personal information to enable us to fulfil the mandate that we have been provided by you.

5. You are legally obliged to supply some of the information that we need in order to comply with the Financial Intelligence Centre Act (FICA). This information is required to combat money laundering and the financing of terrorism. Any other information that we ask for will be required to enable us to effectively fulfill our mandate.

6. We will be passing your personal information on to all third parties that may require it in order for our offices to fulfill our mandate. In these circumstances, only the information that is necessary and relevant will be shared for this purpose.

7. If there is an international component to the legal service which we are rendering, and if we are required to share your personal information with an offshore recipient, you are

entitled to request details as to how your personal information will be protected in this foreign country, and we will endeavor to assist you.

8. You have the right of access to your personal information and the right to correct any errors relating to the information that we have on record. In addition, you have the right to object to us continuing to process your personal information. In this regard, please note that if you do exercise this right, we may not be able to fulfil our mandate effectively.

9. We are obliged by law to retain our records for a period of time after we have completed our work. During this period, your personal information will also remain protected. After this period has expired, your personal information will be destroyed in a way that de-identifies you.

THE SECURITY OF OUR SYSTEMS

10. In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, we have and continue to implement the following security safeguards:

    10.1 Our business premises where records are kept remain protected by access control, alarms and armed response.

    10.2 Archived files are off-site and access control to these storage facilities are implemented.

    10.3 All the user terminals on our internal computer network and our servers are protected by passwords which must be changed on a regular basis.

    10.4 Our email infrastructure complies with industry standard security safeguards, and we employ up to date technology to ensure the confidentiality, integrity and availability of the personal information in our care.

    10.5 Vulnerability assessments are carried out on our digital infrastructure at least on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place.

    10.6 We use an internationally recognised Firewall to protect the data on our local servers, and we run continuous antivirus protection to ensure our systems are kept updated with the latest patches.

10.7 Our staff are trained to carry out their duties in compliance with POPI, and this training is ongoing.

10.8 The personal information of clients are destroyed timeously in a manner that de-identifies the person.

11. These security safeguards are verified on a regular basis to ensure effective implementation, and these safeguards must be continually updated in response to new risks or deficiencies.

12. Should you dispute the way in which we are processing your personal information, you are entitled to lodge a complaint with the Information Regulator, whose contact details are:

JD HOUSE
27 Stiemans Street
Braamfontein
Johannesburg
2001
Complaint's email: complaints.IR@justice.gov.za
General enquiries email: inforeg@justice.gov.za

13. We do wish to emphasize that the processing of your personal information will be handled in a way that complies with all the relevant laws and that your rights to privacy will be protected.

14. If you wish to have greater insight into the way in which we implement POPI, you may request a copy of our company's internal POPI Compliance Manual, and any forms relating to the consent, objection and requests for correction, deletion or destruction of your personal information.

Kind regards

FABER GOERTZ ELLIS AUSTEN INCORPORATED

CONSENT TO PROCESS (USE) PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT

I/We the undersigned

_____

_____

(NAME & ID / PASSPORT NUMBER)

hereby give my/our consent for the processing (use) of our personal information and/or the information of _____ (juristic person) by FABER GOERTZ ELLIS AUSTEN INCORPORATED for the purposes of rendering professional legal services in terms of their mandate which I/We confirm having signed.

This consent specifically includes the right to work with my/our bank account details as and when required to ensure that I/we receive payments or refunds due to me/us.

This consent is furnished on condition that my/our personal information shall be used and processed in accordance with the Protection of Personal Information Act.

SIGNED AT _____ ON THIS THE _____ DAY OF _____ 2021

_____

CLIENT
DULY AUTHORISED

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) TO THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number/Reg Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	FABER GOERTZ ELLIS AUSTEN INCORPORATED
Residential, postal or business address:	EAST VIEW, GROUND FLOOR, BRYANSTON PLACE OFFICE PARK, 199 BRYANSTON DRIVE, BRYANSTON, JOHANNESBURG
	Code (2021)
Contact number(s):	010 590 3378
Fax number/ E-mail address:	stephanie@fgea.co.za
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)** *(Please provide detailed reasons for the objection)*

SIGNED AT ..... THIS ..... DAY OF .....20.....

.....

Signature of data subject/designated person

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

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 isin possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number/Reg no:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	FABER GOERTZ ELLIS AUSTEN INCORPORATED
Residential, postal or business address:	EAST VIEW, GROUND FLOOR, BRYANSTON PLACE OFFICE PARK, 199 BRYANSTON DRIVE, BRYANSTON, JOHANNESBURG
	Code (2021)
Contact number(s):	010 590 3378
Fax number/ E-mail address:	stephanie@fgea.co.za
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**

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 AUTHORISED TO RETAIN.** *(Please provide detailed reasons for the request)*

SIGNED AT ..... THIS ..... DAY OF .....20.....

.....

Signature of data subject/ designated person

APPLICATION FOR CONSENT TO DIRECT MARKETING
REQUEST FOR CONSENT TO RECEIVE DIRECT MARKETING MATERIAL
SECTION 69(2) AND REGULATION 6 OF THE PROTECTION OF PERSONAL INFORMATION ACT

PART A

Dear Client

We regularly send out newsflashes and other interesting information using electronic means and this could be categorized as direct marketing. We would love to have you on our mailing list, but for this to happen we need your consent.

If you would like to receive these communications, please sign off on the consent below and send it back to us.

We look forward to staying in touch.

Kind regards

FABER GOERTZ ELLIS AUSTEN INC

PART B

I/We, _____ (full names)

1. hereby give my/our **CONSENT** to receive direct marketing of legal services to be marketed by means of electronic communications from FABER GOERTZ ELLIS AUSTEN INCORPORATED by way of emails; or
2. hereby refuse my/our **CONSENT** to receive direct marketing of legal services to be marketed by means of electronic communications from FABER GOERTZ ELLIS AUSTEN INCORPORATED

Signed: Signed:

_____ _____

CLIENT **CLIENT**