BNP Paribas SA South Africa Branch

("**The Company**")

MANUAL

as prescribed by the provisions of

THE PROMOTION OF ACCESS TO INFORMATION ACT, 2000

And

THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Contents

1 DEFINITIONS

1.1 **Company** means BNP Paribas SA - South Africa Branch (registration number 2011/100541/10), branch of a company duly incorporated in France with limited liability and registered in South Africa as an external Company in accordance with the laws of the Republic of South Africa and having its principal place of business situated at 4th floor, 11 Crescent Dr, Melrose Arch, Johannesburg, 2196, Gauteng, Republic of South Africa;

1.2 **Conditions for Lawful Processing** means the conditions for the lawful processing of Personal Information as fully set out in chapter 3 of POPI;

1.3 **Constitution** means the Constitution of the Republic of South Africa, 1996;

1.4 **Customer** refers to any natural or juristic person that received or receives services from the Company;

1.5 **Data Subject** has the meaning ascribed thereto in section 1 of POPI;

1.6 **Head of the Company** means the "head" as defined in section 1 of PAIA and referred to in clause 4;

1.7 **Information Officer** means the officer as referred to in clause 4

1.8 **Manual** means this manual prepared in accordance with section 51 of PAIA and regulation 4(1) (d) of the POPI Regulations;

1.9 **PAIA** means the *Promotion of Access to Information Act, 2000*;

1.10 **Personal Information** has the meaning ascribed thereto in section 1 of POPI;

1.11 **Personnel** refers to any person who works for, or provides services to or on behalf of the Company, and receives or is entitled to receive remuneration and any other person who assists in carrying out or conducting the business of the Company, which includes, without limitation, directors (executive and non-executive), all permanent, temporary and part-time staff as well as contract workers;

1.12 **POPI** means the *Protection of Personal Information Act, 2013*;

1.13 **POPI Regulations** mean the regulations promulgated in terms of section 112(2) of POPI;

1.14 **Private Body** has the meaning ascribed thereto in sections 1 of both PAIA and POPI;

1.15 **Processing** has the meaning ascribed thereto in section 1 of POPI;

1.16 **Responsible Party** has the meaning ascribed thereto in section 1 of POPI;

1.17 **Record** has the meaning ascribed thereto in section 1 of PAIA and includes Personal Information;

1.18 **Requester** has the meaning ascribed thereto in section 1 of PAIA;

1.19 **Request for Access** has the meaning ascribed thereto in section 1 of PAIA; and

1.20 **SAHRC** means the South African Human Rights Commission.

Capitalised terms used in this Manual have the meanings ascribed thereto in sections 1, of POPI and PAIA respectively, as the context specifically requires, unless otherwise defined herein.

2 PURPOSE OF THE MANUAL

2.1 This Manual:

(1) For the purposes of PAIA, details the procedure to be followed by a Requester and the manner in which a Request for Access will be facilitated; and

(2) For the purposes of POPI, amongst other things, details the purpose for which Personal Information may be processed; a description of the categories of Data Subjects for whom the Company Processes Personal Information as well as the categories of Personal Information relating to such Data Subjects; and the recipients to whom Personal Information may be supplied.

This manual is reviewed on a periodic basis and is managed and maintained by the Information Officer

3 COMPANY DETAILS

3.1 The details of the Company are as follows:

Physical address	**BNP Paribas SA South Africa Branch** 4th Floor 11 Crescent Drive, Melrose Arch Johannesburg 2196
Telephone number:	011 088 2101
Email	mea.communications.data.rights@bnpparibas.com

4 CONTACT DETAILS OF THE INFORMATION OFFICER

4.1 The Information Officer of the Company is: Benoit Pivot

4.2 The Information Officer's contact details are as follows:

Physical address	BNP Paribas SA South Africa Branch 4th Floor 11 Crescent Drive, Melrose Arch Johannesburg 2196
Telephone number:	011 088 2101
email address:	mea.communications.data.rights@bnpparibas.com

5 THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION

5.1 The SAHRC has compiled a guide, as contemplated in section 10 of PAIA, containing information to assist any person who wishes to exercise any right as contemplated in PAIA.

5.2 This guide is available from the SAHRC at:

Postal address	Private Bag 2700 Houghton 2041
Website	www.sahrc.org.za
Telephone number	011 877 3600
Fax number	011 403 0684

6 PUBLICATION AND AVAILABILITY OF CERTAIN RECORDS IN TERMS OF PAIA

6.1 Schedule of Records

The Schedule of Records as contained in

Appendix of this Manual details the Records that are held and/or Processed by the Company for the purposes of PAIA and POPI respectively. Access to such Records may not be granted if they are subject to the grounds of refusal which are specified in clause 7 below.

6.2 List of applicable legislation

(1) The Company retains records which are required in terms of legislation other than PAIA.

(2) Certain legislation provides that private bodies shall allow certain persons access to specified records, upon a standard request for the same i.e. without a person having to request access in terms of PAIA specifically.

(3) Legislation that may be consulted to establish whether a Requester has a right of access to a record, other than in terms of the procedure set out in the PAIA, are set out in **Appendix** .

7 GROUNDS FOR REFUSAL OF ACCESS TO RECORDS IN TERMS OF PAIA

The following are the grounds on which the Company may, subject to the exceptions contained in Chapter 4 of PAIA, refuse a Request for Access in accordance with Chapter 4 of PAIA:

7.1 mandatory protection of the privacy of a third party, where such disclosure of Personal Information would be unreasonable;

7.2 mandatory protection of the commercial information of a third party, if the Records contain:

(1) trade secrets of that third party;

(2) financial, commercial, scientific or technical information of the third party, the disclosure of which could likely cause harm to the financial or commercial interests of that third party; and/or

(3) information disclosed in confidence by a third party to the Company, the disclosure of which could put that third party at a disadvantage in contractual or other negotiations or prejudice the third party in commercial competition;

7.3 mandatory protection of confidential information of third parties if it is protected in terms of any agreement;

7.4 mandatory protection of the safety of individuals and the protection of property;

7.5 mandatory protection of Records that would be regarded as privileged in legal proceedings;

7.6 protection of the commercial information of the Company, which may include:

(1) trade secrets;

(2) financial/commercial, scientific or technical information, the disclosure of which could likely cause harm to the financial or commercial interests of the Company;

(3) information which, if disclosed, could put the Company at a disadvantage in contractual or other negotiations or prejudice the Company in commercial competition; and/or

(4) computer programs which are owned by the Company, and which are protected by copyright and intellectual property laws;

7.7 research information of the Company or a third party, if such disclosure would place the research or the researcher at a serious disadvantage; and

7.8 Requests for Records that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources.

8 INFORMATION OR RECORDS NOT FOUND

If the Company cannot find the records that a Requester is looking for, despite reasonable and diligent search, and believes either that the records are lost or that the records are in its possession but unattainable, the Requester will receive a notice in this regard from the Information Officer in the form of an affidavit setting out the measures taken to locate the document and accordingly the inability to locate the document.

9 REMEDIES AVAILABLE TO THE REQUESTER UPON REFUSAL OF A REQUEST FOR ACCESS IN TERMS OF PAIA

9.1 The Company does not have any internal appeal procedures in the event that a request cannot be accommodated. As such, the decision made by the Information Officer is final, and Requesters will have to exercise such external remedies at their disposal if the Request for Access is refused.

9.2 In accordance with sections 56(3) (c) and 78 of PAIA, a Requester may apply to a court for relief within 180 days of notification of the decision for appropriate relief.

10 PROCEDURE FOR A REQUEST FOR ACCESS IN TERMS OF PAIA

10.1 A Requester must comply with all the procedural requirements prescribed by section 53 of PAIA relating to a Request for Access to a Record.

10.2 A Requester must complete the prescribed Request for Access form attached as **Appendix 3**, and submit the completed Request for Access form as well as payment of a request fee (if applicable) and a deposit (if applicable), to the Information Officer at the physical address or electronic mail address stated in clause 4 above.

10.3 The Request for Access form must be completed with enough detail so as to enable the Information Officer to identify the following:

(1) the Record/s requested;

(2) the identity of the Requester;

(3) the form of access that is required, if the request is granted;

(4) the postal address or fax number of the Requester; and

(5) the right that the Requester is seeking to protect and an explanation as to why the Record is necessary to exercise or protect such a right.

10.4 If a Request for Access is made on behalf of another person, the Requester must submit proof of the capacity in which the Requester is making the request to the reasonable satisfaction of the Information Officer.

10.5 If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally.

10.6 The Company will voluntarily provide the requested Records to a Personal Requester (as defined in section 1 of PAIA). The prescribed fee for reproduction of the Record requested by a Personal Requester will be charged in accordance with section 54(6) of PAIA and paragraph 11 below.

11 FEES

11.1 When the Request for Access is received by the Information Officer, the Information Officer will by notice require the Requester, other than a Personal Requester, to pay the prescribed request fee (if any), before further processing of the Request for Access.

11.2 Prescribed request fees are set out in **Appendix 4.**

11.3 If the search for a Record requires more than the prescribed hours for this purpose, the Information Officer will notify the Requester to pay as a deposit, the prescribed portion of the access fee (being not more than one third) which would be payable if the Request for Access is granted.

11.4 The Information Officer will withhold a Record until the Requester has paid the fees set out in **Appendix 4.**

11.5 A Requester whose Request for Access to a Record has been granted, must pay an access fee for reproduction and for search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the Record for disclosure including making arrangements to make it available in a requested form provided for in PAIA.

11.6 If a deposit has been paid in respect of a Request for Access which is refused, the Information Officer will repay the deposit to the Requester.

12 DECISION TO GRANT ACCESS TO RECORDS

12.1 The Company will decide whether to grant or decline the Request for Access within 30 days of receipt of the Request for Access and must give notice to the Requester with reasons (if required) to that effect.

12.2 The period referred to above may be extended for a further period of not more than 30 days if the Request for Access is for a large number of Records or the Request for Access requires a search for Records held at another office of the Company and the Records cannot reasonably be obtained within the original 30 day period.

12.3 The Company will notify the Requester in writing should an extension of time as contemplated above be required.

12.4 If, in addition to a written reply from the Information Officer, the Requester wishes to be informed of the decision on the Request for Access in any other manner, the Requester must state the manner and particulars so required.

13 AVAILABILITY OF THE MANUAL

13.1 This Manual is made available in terms of PAIA and section 4 of the Regulations to POPI.

13.2 This Manual is also available at: https://southafrica.bnpparibas.com/en/about-bnp-paribas/bnp-paribas-in-south-africa/

13.3 This Manual is further available at the SAHRC and at the offices of the Company for inspection during normal business hours. No fee will be levied for inspection as contemplated in this clause.

13.4 Copies of the Manual can be obtained from the Information Officer. A fee will be levied for copies of the manual in accordance with **Appendix 4.**

14 PROTECTION OF PERSONAL INFORMATION THAT IS PROCESSED BY THE COMPANY

14.1 Chapter 3 of POPI provides for the minimum Conditions for Lawful Processing of Personal Information by a Responsible Party. These conditions may not be derogated from unless specific exclusions apply as outlined in POPI.

14.2 The Company needs Personal Information relating to both individual and juristic persons in order to carry out its business and organisational functions. The manner in which this information is Processed and the purpose for which it is Processed is determined by the Company. The Company is accordingly a Responsible Party for the purposes of POPI and will ensure that the Personal Information of a Data Subject:

(1) is processed lawfully, fairly and transparently. This includes the provision of appropriate information to Data Subjects when their data is collected by the Company, in the form of

privacy or data collection notices. The Company must also have a legal basis (for example, consent) to process Personal Information;

(2) is processed only for the purposes for which it was collected;

(3) will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

(4) is adequate, relevant and not excessive for the purposes for which it was collected;

(5) is accurate and kept up to date;

(6) will not be kept for longer than necessary;

(7) is processed in accordance with integrity and confidentiality principles; this includes physical and organisational measures to ensure that Personal Information, in both physical and electronic form, are subject to an appropriate level of security when stored, used and communicated by the Company, in order to protect against access and acquisition by unauthorised persons and accidental loss, destruction or damage;

(8) is processed in accordance with the rights of Data Subjects, where applicable. Data Subjects have the right to:

(a) be notified that their Personal Information is being collected by the Company. The Data Subject also has the right to be notified in the event of a data breach;

(b) know whether the Company holds Personal Information about them, and to access that information. Any request for information must be handled in accordance with the provisions of this Manual;

(c) request the correction or deletion of inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained personal information;

(d) object to the Company's use of their Personal Information and request the deletion of such Personal Information (deletion would be subject to the Company's record keeping requirements);

(e) object to the processing of Personal Information for purposes of direct marketing by means of unsolicited electronic communications; and

(f) complain to the Information Regulator regarding an alleged infringement of any of the rights protected under POPI and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

14.3 **Appendix 5** details the following:

(1) Purpose of the Processing of Personal Information by the Company

As outlined above, Personal Information may only be Processed for a specific purpose. The purposes for which the Company Processes or will Process Personal Information is set out in **Part 1 of Appendix 5.**

(2) Categories of Data Subjects and Personal Information/special Personal Information relating thereto;

As per section 1 of POPI, a Data Subject may either be a natural or a juristic person. **Part 2 of Appendix 5** sets out the various categories of Data Subjects that the Company Processes Personal Information on and the types of Personal Information relating thereto.

(3) Recipients of Personal Information

Part 3 of Appendix 5 outlines the recipients to whom the Company may provide a Data Subjects Personal Information to.

14.4 Cross-border flows of Personal Information

Section 72 of POPI provides that Personal Information may be transferred out of the Republic of South Africa to a third party (in another country) in circumstances where the:

(1) third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that-

(a) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

(b) includes provisions, that are substantially similar to the Conditions for Lawful Processing as contained in POPI; or

(2) Data Subject consents to the transfer of their Personal Information; or

(3) transfer is necessary for the performance of a contractual obligation between the Data Subject and the Responsible Party; or

(4) transfer is necessary for the performance of a contractual obligation between the Responsible Party and a third party, in the interests of the Data Subject; or

(5) the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject, would in all likelihood provide such consent.

Part 4 of Appendix 5 sets out the planned cross-border transfers of Personal Information and the condition from above that applies thereto.

14.5 Description of information security measures to be implemented by the Company

Part 5 of Appendix 5 sets out the types of security measures to implemented by the Company in order to ensure that Personal Information is respected and protected. A preliminary assessment of the suitability of the information security measures implemented or to be implemented by the Company may be conducted in order to ensure that the Personal Information that is processed by the Company is safeguarded and Processed in accordance with the Conditions for Lawful Processing.

14.6 Objection to the Processing of Personal Information by a Data Subject

Section 11 (3) of POPI and regulation 2 of the POPI Regulations provides that a Data Subject may, at any time object to the Processing of his/her/its Personal Information in the prescribed form attached to this manual as **Appendix 6** subject to exceptions contained in POPI.

14.7 Request for correction or deletion of Personal Information

Section 24 of POPI and regulation 3 of the POPI Regulations provides that a Data Subject may request for their Personal Information to be corrected/deleted in the prescribed form attached as **Appendix 7** to this Manual.

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 1: Description of the subjects on which the Company holds records, and the categories of records held on each subject. Each of these records are available on request in terms of PAIA

1 Client Records

(1) Client correspondence and records;
(2) Client fee files;
(3) Client contracts;
(4) Client business information;
(5) Legal documentation;
(6) Proposal and tender documents;
(7) Standard terms and conditions relevant to services;
(8) Client financial records;
(9) Client treasury-related records

2 Corporate Governance

(1) Codes of conduct;
(2) Corporate social investment records;
(3) Board meeting minutes; and
(4) Executive committee meeting minutes;
(5) Legal compliance records;
(6) Policies.

3 Finance and Administration

(1) Accounting records;
(2) Annual financial statements;
(3) Agreements; Banking records;
(4) Correspondence;
(5) Purchase orders.
(6) Remittances;
(7) Invoices and statements;
(8) Tax records and returns;

4 Human Resources

(1) BEE statistics;
(2) Career development records;
(3) Personnel information;
(4) Employment equity reports;
(5) General terms of employment;
(6) Letters of employment;
(7) Leave records.
(8) PAYE records and returns;
(9) Performance management records;
(10) Assessments; Policies and procedures;
(11) UIF returns;
(12) Retirement benefit
(13) Medical Aid records; and

5 Information Management and Technology

(1) Agreements;
(2) Equipment register;
(3) Information policies;
(4) standards, procedures and guidelines; and
(5) CCTV footage

6 Learning and Education

(1) Training material;

(2) Training records and statistics;

(3) Training agreements; and

(4) Learnership Programmes.

7 Library and Information and Research Centre

(1) External publications;

(2) Internal publications;

(3) Reference works;

(4) Periodicals; and

(5) Research files and articles.

8 Marketing and Communication

(1) Proposal documents;

(2) New business development;

(3) Brand information management;

(4) Marketing strategies;

(5) Communication strategies;

(6) Agreements;

(7) Client relationship programmes;

(8) Marketing publications and brochures; and

(9) Sustainability programmes.

9 Operations

(1) Access control records;

(2) Agreements;

(3) Archival administration documentation;

(4) Communication strategies;

(5) General correspondence;

(6) Insurance documentation;

(7) Service level agreements;

(8) Standard terms and conditions of supply of services and goods;

(9) Procurement agreements and documentation; and

(10) Cellular phone registration documents, including RICA.

10 Secretarial Services

(1) Applicable statutory documents, including but not limited to, constitutional documents and regulatory licenses;

(2) Statutory Returns to relevant authorities;

(3) Minutes of meetings; and

(4) Resolutions passed.

Appendix 2: List of applicable legislation

Administration of Adjudication of Road Traffic Offences Act 46 of 1998
Advertising on Roads & Ribbon Development Act 21 of 1940
Basic Conditions of Employment Act 75 of 1997
Bills of Exchange Act 34 of 1964
Broad-Based Black Economic Empowerment Act 53 of 2003
Broadcasting Act 4 of 1999
Companies Act 71 of 2008
Compensation for Occupational Injuries and Diseases Act 130 of 1993
Competition Act 89 of 1998
Constitution of South Africa Act 108 of 1996
Consumer Protection Act
Copyright Act 98 of 1987
Criminal Procedure Act 51 of 1977
Currency & Exchanges Act 9 of 1933
Customs and Excise Act 91 of 1964
Electronic Communications and Transactions Act 2 of 2000
Employment Equity Act 55 of 1998
Environment Conservation Act 73 of 1989
Financial Advisory & Intermediary Services Act 37 of 2002
Financial Intelligence Centre Act 38 of 2001
Firearms Control Act 60 of 2000
Formalities In Respect of Leases of Land Act 18 of 1969
Health Act 63 of 1977
Income Tax Act 58 of 1962
Labour Relations Act 66 of 1995
Long Term Insurance Act 52 of 1998
National Building Regulations and Building Standards Act 103 of 1997
National Credit Act 34 of 2005
National Environmental Management Act 107 of 1998
National Environmental Management: Air Quality Act 39 of 2004
National Environmental Management: Waste Act 59 of 2008
National Water At 36 of 1998
National Road Traffic Act 93 of 1996
Occupational Health and Safety Act 85 of 1993
Patents Act 57 of 1987

Pension Funds Act 24 of 1956
Prescription Act 18 of 1943
Prevention & Combating of Corrupt Activities Act 12 of 2004
Prevention of Constitutional Democracy Against Terrorist & Related Activities Act 33 of 2004
Prevention of Organised Crime Act 121 of 1998
Promotion of Access to Information Act 2 of 2000
Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000
Protected Disclosures Act 26 of 2000
Regulation of Interception of Communications and Provisions of Communication Related Information Act 70 of 2002
Sales and Service Matters Act 25 of 1964
Second-Hand Goods Act 23 of 1955
Securities Services Act 36 of 2004
Securities Transfer Act 25 of 2007
Short-Term Insurance Act 53 of 1998
Skills Development Act 97 of 1997
Skills Development Levies Act 9 of 1999
South African Reserve Bank Act 90 of 1989
The South African National Roads Agency Limited & National Roads Act 7 of 1998
Tobacco Products Control Act 12 of 1999
Trade Marks act 194 of 1993
Transfer Duty Act 40 of 1949
Unemployment Insurance Act 63 of 2001
Unemployment Insurance Fund Contributions Act
Value-Added Tax Act 89 of 1991

Although we have used our best endeavours to supply a list of applicable legislation, it is possible that this list may be incomplete. Whenever it comes to our attention that existing or new legislation allows a Requester access on a basis other than as set out in PAIA, we shall update the list accordingly. If a Requester believes that a right of access to a record exists in terms of other legislation listed above or any other legislation, the Requester is required to indicate what legislative right the request is based on, to allow the Information Officer the opportunity of considering the request in light thereof.

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 3: Access request form - record of private body
(Section 53(1) of the Promotion of Access to Information Act, 2000)

Regulation 10 of PAIA

1 An Access Request Form must be completed. The current version of the Access Request Form, as prescribed by Regulation 10 of PAIA, may be accessed at: https://www.justice.gov.za/forms/paia/J752_paia_Form%20C.pdf

2 Proof of identity is required to authenticate the identity of the Requester. The Requester must attach a copy of his/her identification document, to the Access Request Form when submitting the same to the Company.

3 When completing the Access Request Form, please remember:

3.1 To type or print in BLOCK LETTERS an answer to every question.

3.2 If a question does not apply, state “N/A”.

3.3 If there is nothing to disclose in reply to a question, state “nil”.

3.4 When there is insufficient space on a printed form, additional information may be provided on an attached page, and each answer on such page must reflect the applicable title.

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 4 : Fees

1 The fee for a copy of the manual as contemplated in regulation 9(2)(c) is R1,10 for every photocopy of an A4-size page or part thereof.

2 The fees, in South African Rands, for reproduction referred to in regulation 11(1) are as follows:

(a)		For every photocopy of an A4-size page or part thereof	1,10
(b)		For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form	0,75
(c)		For a copy in a computer-readable form on -	
	(i)	stiffy disc	7,50
	(ii)	compact disc	70,00
(d)	(i)	For a transcription of visual images, for an A4-size page or part thereof	40,00
	(ii)	For a copy of visual images	60,00
(e)	(i)	For a transcription of an audio record, for an A4-size page or part thereof	20,00
	(ii)	For a copy of an audio record	30,00

3 The request fee payable by a requester, other than a personal requester, referred to in regulation 11(2) is R50,00.

4 The access fees, in South African Rand, payable by a requester referred to in regulation 11(3) are as follows:

(1)	(a)		For every photocopy of an A4-size page or part thereof	1,10
	(b)		For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form	0,75
	(c)		For a copy in a computer-readable form on -	
		(i)	stiffy disc	7,50
		(ii)	compact disc	70,00
	(d)	(i)	For a transcription of visual images, for an A4-size page or part thereof	40,00
		(ii)	For a copy of visual images	60,00
	(e)	(i)	For a transcription of an audio record, for an A4-size page or part thereof	20,00
		(ii)	For a copy of an audio record	30,00
	(f)		To search for and prepare the record for disclosure, R30,00 for each hour or part of an hour reasonably required for such search and preparation.	

5 For purposes of section 54(2) of the Act (see clause 11.3 above) the following applies:

5.1 six hours as the hours to be exceeded before a deposit is payable; and

5.2 one third of the access fee is payable as a deposit by the requester.

6 The actual postage is payable when a copy of a record must be posted to a requester.

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 5 Part 1: Processing of personal information in accordance with POPI

Purpose of the Processing of Personal Information	Type of Processing

1	To comply with the Company's various legal and regulatory obligations including:	Collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
1.1	banking and financial regulations:	
1.2	monitor transactions to identify those which deviate from normal routine/patterns ;	
1.3	manage, prevent and detect fraud including, where required by law, the establishment of a fraud list (which will include a list of fraudsters) ;	
1.4	monitor and report risks (financial, credit, legal, compliance or reputational risks, default risks etc.) that the Company/and or the BNP Paribas Group could incur;	
1.5	monitor and record phone calls, chats, email, etc. notwithstanding other usages described hereafter;	
1.6	prevent and detect money-laundering and financing of terrorism and comply with regulation relating to sanctions and embargoes through our Know Your Customer (KYC) process (to identify Customers, verify Customer identity, screen Customer details against sanctions lists and determine Customer profiles);	
1.7	detect and manage suspicious orders and transactions;	
1.8	carry out an assessment of appropriateness or suitability in our provision of investment services to each client in compliance with Markets in Financial Instruments regulations (MiFiD);	
1.9	contribute to the fight against tax fraud and fulfil tax control and notification obligations (including compliance with FATCA and AEOI requirements);	
1.10	record transactions for accounting purposes;	
1.11	prevent, detect and report risks related to Corporate Social Responsibilities and sustainable development;	

1.12	detect and prevent bribery;	
1.13	exchange information and report on different operations, transactions or orders or reply to official requests from duly authorised local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or meditators, law enforcement, state agencies or public bodies.	
2	The Company use personal information to enter into and perform its contracts as well as to manage its relationship with Customers, including to:	
2.1	define the Customer's credit risk score and the Customer's reimbursement capacity;	
2.2	evaluate (e.g. based on the Customer's credit risk score) if the Company can offer the Customer a product or service and under which conditions (including price);	
2.3	assist the Customer in particular by answering the Customer's requests;	
2.4	provide Customer with products or services; and	
2.5	manage outstanding debts (identification and exclusion of customers with outstanding debts).	
3	The Company use Customer Personal Information, including transaction data, for:	
3.1	Risk management purposes;	
	proof of transactions including electronic evidence;	
	• management, prevention and detection of fraud including, where required by law, the establishment of a fraud list (which will include a list of fraudsters) ;	

• monitoring transactions to identify those, which deviate from the normal routine/patterns . • debt collection; • assertion of legal claims and defence in case of legal disputes; • development of individual statistical models in order to help define Customer creditworthiness; • consultation and exchange of data with credit agencies to identify credit risks. 3.2 Personalisation of Customer offering to: • improve the quality of our products or services; • advertise products or services that match with Customer situations and profiles; • deduce Customer preference and needs and propose personalised commercial offers; • This personification can be achieved by: o segmenting Company prospects and Customer; o analysing Customer habits and preferences in various communications channels (visits to Company branches, emails or messages, visits to our website, etc.); o sharing Customer data with another BNP Paribas entity; o matching the products or services that Customer already hold or use with other data the Company holds about the Customer; and	

○ considering common traits or behaviours among current Customers, and seeking other individuals who share those same characteristics for targeting purposes. 3.3 Research & Development (R&D) and analytics consisting of establishing statistical/predictive models to: • optimise and automate Company operational processes (e.g. creating FAQ chatbots); • offer products and services that will best meet Customer needs; • adapt products and services distribution, content and pricing in accordance with a Customer's profile; • create new offers; • prevent potential security failures, improve customer authentication and access rights management; • enhance security management; • enhance risk and compliance management; • enhance the management, prevention and detection of fraud; and • enhance the fight against money laundering and financing of terrorism. 3.4 Security reasons and IT systems performance, including to: • manage IT, including infrastructure management (e.g. shared platforms), business continuity and security (e.g. internet user authentication and data leak prevention); and	

• prevent personal injury and damages to people and goods (for instance video protection). 3.5 More generally to: • inform Customers about Company products and services; • carry out financial operations such as debt portfolio sales, securitisations for financing or refinancing of the BNP Paribas Group; • organise contests, games, competitions, lotteries or any other promotional campaigns; • perform Customer satisfaction and opinion surveys; • improve process efficiency (train Company staff by recording phone calls in call centres and improve Company calling scenario); and • automate Company processes such as application testing, automatic filling of complaints handling, etc. 4 To provide services to the Customer in accordance with terms agreed to by the Customer; 5 To undertake activities related to the provision of services and transactions, including: 5.1 to fulfil foreign and domestic legal, regulatory and compliance requirements and comply with any applicable treaty or agreement with or between foreign and domestic governments applicable to the Company 5.2 to verify the identity of Customer representatives who contact the Company or may be contacted by the Company;	

5.3 for risk assessment, information security management, statistical, trend analysis and planning purposes; 5.4 to monitor and record calls and electronic communications with the Customer for quality, training, investigation and fraud prevention purposes; 5.5 for crime detection, prevention, investigation and prosecution; 5.6 to enforce or defend the Company's rights; and 5.7 to manage the Company's relationship with the Customer. 6 The purposes related to any authorised disclosure made in terms of agreement, law or regulation; 7 Any additional purposes expressly authorised by the Customer; and 8 Any additional purposes as may be notified to the Customer or Data Subjects in any notice provided by the Company.	

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 5 Part 2 : Categories of Data Subjects and categories of Personal Information relating thereto

Categories of Data Subjects of and categories of Personal Information relating thereto	Data Subject	Personal Information Processed
Customer Juristic Customer Profile information including, account details, payment information, corporate structure, customer risk rating and other customer information including to the extent the categories of information relate to individuals or representatives of customers (e.g., shareholders, directors, etc.) required for the above mentioned purposes, Strategic Trades (GM) Individual Name; contact details (Company E-Mail Address, Company Telephone Number), client details (Home Facsimile Number, Home Postal Address, Home Telephone Number, Personal Cellular, Mobile Or Wireless Number, Personal E-Mail Address); regulatory identifiers (e.g. tax identification number); Account information (Bank Account Currency Code, Bank Account Id, Bank Account Name, Bank Account Number, Bank Account Type, Bank account balance); transaction details and branch details; “know-your customer” data, photographs; other identification and verification data as contained in images of ID card, passport and other ID documents; images of customer signatures)	• Natural Persons • Juristic Persons.	Personal data relating to a Data Subject received by or on behalf of the Company from the Customer, Customer affiliates and their respective representatives and related parties in the course of providing accounts and services to the Customer or in connection with a transaction or services. Customer personal data may include names, contact details, identification and verification information, nationality and residency information, taxpayer identification numbers, voiceprints, bank account and transactional information (where legally permissible), to the extent that these amount to personal data under POPI.
Payment beneficiaries: Bank Account Currency Code, Bank Account Id, Bank Account Name, Bank Account Number, Bank Account Type; beneficiary address, transaction details; payment narrative and, for certain data transferred from the UK only, National Insurance numbers.		
Personnel :	• Natural Persons	

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Categories of Data Subjects of and categories of Personal Information relating thereto	Data Subject	Personal Information Processed
Name; employee ID number; marital status, tax status, physical and postal address; telephone number; email address, medical history, conditions of employment and other personnel-related contractual and quasi-legal records; Internal evaluation records and other internal records; correspondence relating to personnel; records provided by a third party relating to personnel; personal records provided by personnel; including but not limited training schedules and material		

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 5 Part 3 : Recipients of Personal Information

Sharing of information within the BNP Paribas Group

The Company is part of the BNP Paribas Group, which is an integrated bank and insurance group, i.e. a group of companies working closely together all over the world to create and distribute various banking, financial, insurance services and products.

The Company may share personal information within the BNP Paribas Group for commercial and efficiency needs such as:

1 based on its legal and regulatory obligations:

- sharing of the data collected for AML/FT, sanctions, embargoes and for KYC;
- risk management including credit and operational risks (risk rating /credit scoring/etc.);

2 based on its legitimate interest:

- prevention, detection and fight against fraud;
- R&D activities, particularly for compliance, risk, communication and marketing purposes;
- global and consistent overview of its clients';
- offering the full range of products and services of the BNP Paribas Group.

If a Data Subject is a client of the Company's Corporate & Institutional Banking business, this would include, for example, personal information being accessed and/or stored in: jurisdictions where investments are held; jurisdictions in which and through which transactions are effected; and jurisdictions from which it regularly receives or transmits information about its investments or business with the Company.

3 Personalisation of products and services' (including content and pricing).

Disclosing information outside the BNP Paribas Group

The Company may disclose personal information from time to time with:

1 service providers who perform services on its behalf (e.g. IT services, logistics, printing services, telecommunication, debt collection, advisory and consulting, distribution and marketing).

2 banking and commercial partners, independent agents, intermediaries or brokers, financial institutions, counterparties, trade repositories with which it has relationships with, if such transmission is required to allow the Company to provide the services and products or execute contractual obligations or transactions (e.g. banks, correspondent banks, depositaries, custodians, issuers of securities, paying agents, exchange platforms, insurance companies, payment system operators, issuers or payment card intermediaries);

3 credit reference agencies;

4 local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, law enforcement, state agencies, fraud prevention agencies or public bodies, the Company or any member of the BNP Paribas Group is required to disclose to pursuant to:

- their request;
- defending or responding to a matter, action or proceeding; and/or

- complying with regulation or guidance from authorities applying to us or any member of the BNP Group;

5 payment service provider(s) (information on payment account(s)) based on the authorisation granted to this third party; and

6 certain regulated professionals such as lawyers, notaries, rating agencies or auditors when needed under specific circumstances (litigation, audit, etc.) as well as to actual or proposed purchasers of the companies or businesses of the BNP Paribas Group or its insurers

Sharing aggregated or anonymized information

The Company shares aggregated or anonymised information within and outside the BNP Paribas Group with partners such as research groups, universities or advertisers. Data Subjects will not be able to be identified from this information.

Personal Information may be aggregated into anonymised statistics that may be offered to professional clients to assist them in developing their business. In this case, personal Information will never be disclosed and those receiving these anonymised statistics will be unable to identify data subjects.

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 5 Part 4: Cross border transfers of Personal Information

In certain circumstances, the Company may transfer personal information to another country. This includes transfers of personal information to BNP Paribas Group entities in France, Bahrain, the United Kingdom, Portugal, India, the United States of America etc. The Company is a branch of BNP Paribas SA and as such is extension of the French entity (as opposed to being a separate legal entity). Transfers of Personal Information from the Company to BNP Paribas SA or any of its branches are accordingly not strictly transfers to a third party. Any such transfers do however occur within the parameters of binding corporate rules (see 14.4(1) above.

In case of transfers of personal data to a third party in a foreign state, the Company makes sure to transfer Personal Information to countries and regions with legal frameworks that provide an adequate level of protection for the privacy and fundamental rights and freedoms in respect of the processing of personal information. Such transfers are done pursuant to the requisite authorizations by the relevant authorities and laws.

Furthermore, in case of cross border transfers, we will only disclose personal information to such third party or parties where they have undertaken, in advance and in writing, to maintain the confidentiality, integrity and security of the personal data concerned, in accordance with applicable laws.

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 5 Part 5: Description of information security measures

The Company undertakes to institute and maintain the data protection measures to accomplish the following objectives outlined below. The details given are to be interpreted as examples of how to achieve an adequate data protection level for each objective. The Company may use alternative measures and adapt to technological security development, as needed, provided that the objectives are achieved.

1 Access Control of Persons

The Company shall implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the data are processed.

2 Data Media Control

The Company undertakes to implement suitable measures to prevent the unauthorized manipulation of media, including reading, copying, alteration or removal of the data media used by the Company and containing personal data of Customers.

3 Data Memory Control

The Company undertakes to implement suitable measures to prevent unauthorized input into data memory and the unauthorized reading, alteration or deletion of stored data.

4 User Control

The Company shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons by means of data transmission equipment.

5 Access Control to Data

The Company represents that the persons entitled to use the Company's data processing system are only able to access the data within the scope and to the extent covered by their respective access permissions (authorization).

6 Transmission Control

The Company shall be obliged to enable the verification and tracing of the locations / destinations to which the personal information is transferred by utilization of the Company's data communication equipment / devices.

7 Transport Control

The Company shall implement suitable measures to prevent Personal Information from being read, copied, altered or deleted by unauthorized persons during the transmission thereof or during the transport of the data media.

8 Organization Control

The Company shall maintain its internal organization.

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 6: Objection to the processing of personal information in terms of

Section 11(3) of POPI

Regulations relating to the protection of personal information, 2018

[Regulation 2]

Note:

1 Affidavits or other documentary evidence as applicable in support of the objection may be attached.

2 If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

3 Complete as is applicable.

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ registered name of data subject:	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)**

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

.....

Signature of data subject/designated person

BNP PARIBAS
CORPORATE & INSTITUTIONAL BANKING

Appendix 7: 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

Regulations relating to the protection of personal information, 2018

Regulation 3

Note:

1. Affidavits or other documentary evidence as applicable in support of the request may be attached.

2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

3. Complete as is applicable.

Mark the appropriate box with an "x".

Request for:

☐ **Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.**

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

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ registered name of data subject:	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	

C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)**
D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. (Please provide detailed reasons for the request)**