Global Data Protection Policy
for Client, Supplier and Business Partner Data

INFORMATION SHEET

Target audience:
All employees (temporary or permanent) of all majority owned ING businesses (or business units), businesses under ING's management control and staff departments.

Issued by:
ING Legal Department Bank (IT, Procurement & Privacy)

Version:
1.0

Replaces:
This ING Global Data Protection Policy for Client, Supplier and Business Partner Data (**"Policy"**) supersedes all ING data protection policies and notices that exist on the Effective Date to the extent they address the same issues and are not consistent with this Policy.

Approved by:
ING Bank N.V. Management Board Banking per 22 July 2013

Effective Date:
1 August 2013

In the event of any discrepancies between the English version of this Policy and a translated version, the English version shall prevail.

This is the latest approved version by the Dutch Data Protection Authority on behalf of itself and each data protection authority located in the EU member states. The adjusted version (2.0) is currently under review with the Dutch Data Protection Authority .

CONTENT

PART I GENERAL INTRODUCTION

1 Introduction

1.1 Under ING's Business Principles all employees are expected to handle information with care. In particular, the security and confidentiality of all proprietary information and data processing, including personal confidential information, must be safeguarded in accordance with applicable laws and regulations. In this Policy it is explained that the protection of personal data is about:

- Being transparent in what ING does with personal data of clients, suppliers and business partners.
- Only processing personal data for specific business purposes.
- Only using sensitive data if necessary and where legally allowed.
- Making sure that personal data are up-to-date, complete and accurate.
- Informing clients, suppliers and business partners about the purposes for which their personal data; are processed and which ING business is responsible for the processing.
- Allowing clients, suppliers and business partners to obtain an overview of their personal data.
- Allowing clients, suppliers and business partners to correct, delete or block their personal data.
- Protecting the personal data from unauthorized loss, alteration, disclosure or access.
- Only disclosing personal data to third parties in accordance with this Policy.

Thus: the right **PEOPLE** use the right **DATA** for the right **PURPOSE**.

For the privacy rules applicable to employee personal data is referred to the ING Global Data Protection Policy for Employees ("GDP Policy for Employees"). This Policy pertains only to the personal data of natural persons that are, or are employed by, our clients, suppliers and business partners. The Policy does not apply to any other data relating to corporate, institutional or governmental clients, suppliers or business partners, except where local law determines otherwise. The Policy does not address obligations ING may be subject to under local banking secrecy and other applicable laws.

The capitalised terms which are used in this Policy are explained in Appendix 1. More detailed guidance can be found in the Guidance Documents that can be accessed by Staff via the ING intranet.

2 Objective of this Policy

2.1 This Policy aims to provide a clear statement on the protection of Clients, Suppliers and Business Partners Data in order to provide for an adequate level of protection for all Clients, Suppliers and Business Partners Data Processed within ING globally.

3 Scope

3.1 This Policy addresses the Processing of all Personal Data of Clients, Suppliers and Business Partners by ING or by a Third Party on behalf of ING globally in accordance with Article 15. This Policy does not address the Processing of Employee Data of ING.

Electronic and paper-based Processing

3.2 This Policy applies to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.

Data Protection Executive advice

3.3 Where there is a question as to the applicability of this Policy, Staff shall seek the advice of the appropriate Data Protection Executive prior to the relevant processing.

Compliance Responsibility

3.4 This Policy is binding on ING acting as a Data Controller. The Data Protection Executive shall be responsible for business organisation's compliance with this Policy. Staff must comply with this Policy. The Policy does not apply to ING when it is acting as a Data Processor.

4 Applicability of local law and Policy

Individuals keep local rights and remedies

4.1 Individuals keep any rights and remedies they may have under applicable local law. This Policy shall apply only where it provides supplemental protection for Personal Data. Where applicable local law provides more protection than this Policy, local law shall apply. Where this Policy provides more protection than applicable local law or provides additional safeguards, rights or remedies for Individuals, this Policy shall apply.

Minimum standards and notices

4.2 ING may supplement this Policy through minimum standards or notices that are consistent with this Policy, both on a local level and by ING Bank N.V. In the event that ING changes these minimum standards or notices to the Policy and as a consequence thereof substantial changes have to be made to the Policy, ING shall inform the Dutch Data Protection Authority of these substantial changes to the Policy in accordance with Article 26.1.

5 Implementation

Effective Date

5.1 This Policy has been adopted by the ING Bank N.V. Executive Board and shall enter into force as of 1 August 2013 ("**Effective Date**") and shall be published on the ING website and ING intranet and be made available to Individuals upon request.

Policy supersedes prior policies

5.2 This Policy supersedes all ING data protection policies and notices that exist on the Effective Date to the extent they address the same issues and are not consistent with this Policy or impose less restrictive requirements than the Policy.

Implementation

5.3 This Policy shall be implemented in the ING organization based on the timeframes specified in Article 27.

PART II POLICY STATEMENTS

6 Purposes for Processing Personal Data

Policy statement
ING shall only collect, use or otherwise Process Personal Data relating to Clients, Suppliers and Business Partners if the Processing falls within the scope of one (or more) of the legitimate Business Purposes listed below.

Legitimate Business Purposes

6.1 Personal Data shall be collected, used, stored or otherwise Processed if necessary,

- within the framework of responsible, efficient and effective business management, specifically for the following activities:

  - **Performing agreements** assessing and accepting Clients, entering into and executing of agreements with Clients, Business Partners and Suppliers as well as carrying out payment transfers and other financial transactions and recording and financially settling delivered services, products and materials to and from ING, including communication with Individuals and other parties involved in contracts (insured persons, beneficiaries, intermediaries) and responding to requests for (further) information from Clients, Business Partners or Suppliers, dispute resolution and litigation.
  - **Relationship management and marketing** for commercial activities including processing necessary for the development and improvement of ING products and/or services, account management, client service and the performance of (targeted) marketing activities in order to establish a relationship with a Client and/or maintaining as well as extending a relationship with a Client, Business Partner or Supplier and for performing analyses with respect to personal data for statistical and scientific purposes.
  - **Business process execution, internal management and management reporting** addressing activities such as managing company assets, conducting internal audits and investigations, finance and accounting, implementing business controls, provision of central processing facilities for efficiency purposes, managing mergers, acquisitions and divestitures and Processing Personal Data for management reporting and analysis.
  - **Safety and security** this purpose addresses activities such as those involving safety and health, the protection of ING and Client, Supplier or Business Partner assets and the authentication of Client, Supplier or Business Partner status and access rights.
  - **Protecting the vital interests of Individuals** this is where Processing is necessary to protect the vital interests of an Individual, e.g. for urgent medical reasons.
  - **Compliance with legal obligations** this addresses the Processing of Personal Data as necessary for compliance with laws, regulations and sector specific guidelines to which ING is subject.

- to support the activities to safeguard and ensure the security and integrity of ING and/or the financial sector, including the following activities:
  (i) The identification, prevention and investigation of activities that may have a negative effect on financial institutions and ING, including but not limited to:
    (i) Misuse of products, services and facilities of financial institutions.
    (ii) (attempted) criminal or otherwise negative conduct.
    (iii) Violations of (legal) regulations.

(ii) Defending, preventing and tracing (attempted) (criminal or undesirable) conduct targeted towards the financial sector, ING Bank N.V., the Group Companies, Clients and Staff.
(iii) The use of and participation in warning systems (including sector-specific warning systems).
(iv) Compliance with legal requirements, such as anti-money laundering and anti-terrorist financing regulations.

Where there is a question whether a Processing of Personal Data is for one of the Business Purposes listed above, it is necessary to seek the advice of the appropriate Data Protection Executive before the Processing takes place.

6.2 Individual consent

If a Business Purpose does not exist or if applicable local law so requires, ING shall only Process Personal Data with the Individual's consent. If a Business Purpose does not exist and a specific Processing is undertaken at the request of an Individual (e.g. he subscribes to a service or seeks a benefit), he is deemed to have provided consent to the relevant Processing.

The Individual shall be made aware of:
(a) The purposes of the Processing for which consent is requested or shall be deemed to have been provided.
(b) Other relevant information necessary for the Individual to make a conscious decision about the Processing of his Personal Data (e.g. the nature of the and categories of the Processed Data, the categories of Third Parties to which the Data are disclosed (if any) and how Individuals can exercise their rights).

Denial or withdrawal of consent

6.3 The Individual may both deny consent and withdraw consent at any time.

Limitations on Processing Data of Dependants of Individuals

6.4 ING will Process Data of Dependants of an Individual if:
(i) The Data were provided with the consent of the Individual or the Dependant; or
(ii) Processing of the Data is reasonably necessary for the performance of a contract with the Individual; or
(iii) The Processing is required or permitted by applicable local law.

7 Use for other Purposes

Policy statement
ING shall in principle only use Personal Data for the purposes for which they were originally collected, but may use the Data also for other, related, purposes under the conditions set forth in this Article (8).

Use of Data for Secondary Purposes

7.1 Generally, Personal Data shall be used only for the purposes for which they were originally collected (**Original Purpose**). Personal Data may be Processed for legitimate purposes of ING different from the Original Purpose (**Secondary Purpose**) only if the Original Purpose and Secondary Purpose are closely related and only if use of Data for Secondary Purposes is allowed under applicable law. Depending on the sensitivity of the relevant Personal Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Individual, the secondary use may require one or more additional measures such as:

(i) Limiting access to the Data.
(ii) Imposing additional confidentiality requirements.
(iii) Taking additional security measures.
(iv) Informing the Individual about the Secondary Purpose.
(v) Providing an opt-out opportunity.
(vi) Obtaining Individual consent in accordance with Article 6.2, if required under applicable law.

Generally permitted uses of Data for Secondary Purposes

7.2 It is generally permissible to use Personal Data for the following Secondary Purposes provided appropriate additional measures are taken in accordance with Article 7.1:
(i) Transfer of the Data to an Archive; or
(ii) Internal audits or investigations; or
(iii) Implementation of business controls; or
(iv) Statistical, historical or scientific research; or
(v) Dispute resolution or litigation; or
(vi) Legal or business consulting or
(vii) Insurance purposes.

Data Protection Executive advice

7.3 Before Processing Personal Data for a Secondary Purpose, Staff shall seek the advice of the appropriate Data Protection Executive.

8 Processing Sensitive Data

Policy statement
ING shall only use Sensitive Data for one of the purposes listed in this Article (8) and only to the extent that this is needed for the relevant Business Purpose, the Secondary Purpose or the purposes for which the Individual has provided consent in accordance with Article 6.2, 6.3 or 7.1 ('the legitimate purposes') and to the extent required or permitted under applicable law.

Specific purposes for Processing Sensitive Data

8.1 This Article sets forth specific rules for Processing Sensitive Data. ING shall Process Sensitive Data only to the extent necessary to serve the applicable legitimate purposes.

The following categories of Sensitive Data may be collected, used or otherwise Processed for one (or more) of the purposes specified below:
(i) **Racial or ethnic data** (including pictures and moving images of an Individual): in some countries photos and video images of Individuals qualify as racial or ethnic data. ING may process photos and video images of Individuals (i) for inclusion in Client, Supplier or Business Partner directories and (ii) for site access and security reasons and (iii) to comply with legal obligations (e.g. performing client due diligence screenings).
(ii) **Physical or mental health data**; for assessing and accepting Clients, entering into and executing an agreement with a Client and for carrying out payment transfers and other financial transactions.
(iii) **Criminal data** (including data relating to criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour); for protecting the interests of ING with respect to criminal offences that have been or, given the relevant circumstances are suspected to be, committed against ING or its Employees.

(iv) **Social security numbers** (or other identifying numbers, including passports numbers): for complying with legal obligations e.g. on client identification and authentication.

General Purposes for Processing of Sensitive Data

8.2 In addition to the specific purposes listed in Article 8.1 above, all categories of Sensitive Data may be Processed only under (one or more of) the following:

(i) The Individual has given his explicit consent to the Processing thereof.
(ii) As required by or allowed under applicable local law.
(iii) For the establishment, exercise or defence of a legal claim.
(iv) To protect a vital interest of an Individual, but only where it is impossible to obtain the Individual's consent first.
(v) To the extent necessary to comply with an obligation of international public law (e.g. treaties).
(vi) If the Sensitive Data have manifestly been made public by the Individual.

Prior authorization of Data Protection Executive

8.3 Where Sensitive Data are Processed based on a requirement of law other than the local law applicable to the Processing, or based on the consent of the Individual, the Processing requires the prior authorization of the appropriate Data Protection Executive.

Use of Sensitive Data for Secondary Purposes

8.4 In addition to the requirements of this Article (8), Sensitive Data of Individuals may be Processed for Secondary Purposes in accordance with Article 7.

9 Quantity and quality of Data

Policy statement
ING shall not Process Personal Data that are not reasonably needed for or otherwise relevant to the legitimate purposes for which ING processes Personal Data. ING will use reasonable efforts to ensure that the Data are accurate, complete and up-to-date. ING shall only retain Personal Data for the period required to serve the applicable purposes or for legal reasons.

No Excessive Data

9.1 ING shall restrict the Processing of Personal Data to those Data that are reasonably adequate for and relevant to the applicable legitimate purposes. ING shall take reasonable steps to securely delete Personal Data that are not required for these legitimate purposes.

Storage period

9.2 ING generally shall retain Personal Data only:

(a) For the period required to serve the legitimate purposes for which the Personal Data are Processed; or
(b) To the extent reasonably necessary to comply with an applicable legal requirement; or
(c) As advisable in light of an applicable statute of limitations.

ING may specify (e.g., in a minimum standard, notice or records retention schedule) a time period for which certain categories of Personal Data may be kept.

Promptly after the applicable storage period has ended, the Data Protection Executive shall instruct that the Data be:

(i) Securely deleted or destroyed in accordance with the relevant Corporate ORM policies.

(ii) Anonymized; or
(iii) Transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).

Quality of Data

9.3 Personal Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable legitimate purposes for which the Personal Data are Processed.

Accurate, complete and up-to-date Data

9.4 It is the responsibility of ING to keep the Personal Data of Individuals accurate, complete and up-to-date. It is the responsibility of Individuals to inform ING regarding any changes to their Personal Data.

10 Individual information requirements

Policy statement
ING shall ensure that Individuals are adequately informed about the Business Purposes for which their Personal Data are Processed and shall provide any other information to the Individuals which may be required that pertains to the relevant Processing.

Information requirements

10.1 ING shall inform Individuals through a data protection policy or notice about:
(i) The Business Purposes for which their Data are Processed.
(ii) Which Group Company is responsible for the Processing; and
(iii) Other relevant information (e.g., the nature and categories of the Processed Data, the categories of Third Parties to which the Data are disclosed (if any) and how Individuals can exercise their rights).

Personal Data not obtained from the Individual

10.2 If applicable local law so requires, where Personal Data have not been obtained directly from the Individual, ING shall provide the Individual with the information as set out in Article 10.1:
(i) At the time that the Personal Data are recorded in a ING database; or
(ii) At the time that the Personal Data are used for a mailing, provided that this mailing is done within six months after the Personal Data are recorded in a ING database.

Exceptions

10.3 The requirements of Article 10.2 may be set aside if:
(i) It is impossible or would involve a disproportionate effort to provide the information to Individuals; or
(ii) It results in disproportionate costs.

11 Individual rights of access, rectification and deletion

Policy Statement
This Article addresses certain rights of Individuals whose Personal Data are Processed by ING in its role as a Data Controller.

Rights of Individuals

11.1 Every Individual has the right to request an overview of his Personal Data Processed by or on behalf of ING. Where reasonably possible, the overview shall contain information regarding the

source, type, purpose and categories of recipients of the relevant Personal Data. If the Personal Data are incorrect, incomplete or not Processed in compliance with applicable law or this Policy, the Individual has the right to have his Data rectified, deleted or blocked (as appropriate). In addition, the Individual has the right to object to the Processing of his Data on the basis of compelling grounds related to his particular situation.

Procedure

11.2 The Individual should send his request to the contact person or contact point indicated in the relevant privacy statement. If no contact person or contact point is indicated, the Individual may send his request to the relevant Group Company using the contact details indicated in the general contact section of the local ING website.

Prior to fulfilling the request of the Individual, ING may require the Individual to:

(i) Specify the type of Personal Data to which he is seeking access.
(ii) Specify, to the extent reasonably possible, the data system in which the Data likely are stored.
(iii) Specify the circumstances in which ING obtained the Personal Data; and
(iv) Show proof of his identity; and
(v) In the case of a request for rectification, deletion, or blockage, specify the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with applicable law or this Policy.

Response period

11.3 Within four weeks of ING receiving the request, the Data Protection Executive or any other responsible function indicated in the relevant local complaints procedures shall inform the Individual in writing either (i) of ING's position with regard to the request and any action ING has taken or will take in response or (ii) the ultimate date on which he will be informed of ING's position, which date shall be no later than eight weeks thereafter.

Complaint

11.4 An Individual may file a complaint in accordance with Article 22 if:

(i) The response to the request is unsatisfactory to the Individual (e.g. the request is denied); or
(ii) The Individual has not received a response as required by Article 11.3; or
(iii) The time period provided to the Individual in accordance with Article 11.3 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response.

Denial of requests

11.5 ING may deny a request of an Individual if:

(i) The request does not meet the requirements of Articles 11.1 and 11.2.
(ii) The request is not sufficiently specific.
(iii) The identity of the relevant Individual cannot be established by reasonable means; or
(iv) The request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights. A time interval between requests of 6 months or less shall generally be deemed to be an unreasonable time interval.
(v) The request entails a blockage or deletion and the Processing of the Personal Data is required by law.

12 Security and Confidentiality Requirements

Policy statement
ING shall take appropriate steps to protect the Data from unauthorized access and other unwanted or unlawful Processing, e.g. accidental loss or destruction.

Data security

12.1 ING shall take appropriate commercially reasonable technical, physical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, ING has developed and implemented the ING CORM (Technology) Risk Standards and other relevant policies relating to the security of Personal Data.

Staff access

12.2 Staff members shall be authorized to access Personal Data only to the extent necessary to serve the applicable legitimate purposes for which the Data are Processed by ING and to perform their job.

12.3 Staff members who access Personal Data must meet their confidentiality obligations.

13 Direct marketing

Policy statement
This Article addresses the requirements concerning the Processing of Personal Data for direct marketing purposes. ING must obtain prior consent of the Individual(s) if required under applicable law. In any event, Individuals shall be given the opportunity to opt-out of receiving these communications.

Direct marketing

13.1 This Article sets forth requirements concerning the Processing of Personal Data for direct marketing purposes (e.g. contacting the Individual by email, fax, phone, SMS or otherwise, with a view of solicitation for commercial, charitable or idealistic purposes).

Consent for direct marketing (opt-in)

13.2 If applicable law so requires, ING shall only send to Individuals unsolicited commercial communication (direct marketing communication) with the prior consent of the Individual ("opt-in"). In every direct marketing communication that is made to the Individual, the Individual shall be offered the opportunity to opt-out of further direct marketing communication.

Objection to direct marketing

13.3 If an Individual objects to receiving marketing communications from ING, or withdraws his consent to receive such materials, ING will take steps to refrain from sending further marketing materials as specifically requested by the Individual. ING will do so within the time period required by applicable law.

Third Parties and direct marketing

13.4 No Data shall be provided to, or used or otherwise Processed on behalf of, Third Parties for purposes of direct marketing of or for Third Parties without the prior consent of the Individual.

Personal Data of children

13.5 ING shall not use any Personal Data of Individuals under the age of fourteen (14) years for direct marketing.

Direct marketing records

13.6 ING shall keep local records of Individuals that used their "opt-in" or "opt-out" right and will regularly check the relevant local public opt-out registers.

14 Automated decision making

Automated decisions

14.1 Automated tools may be used to make decisions about Individuals but decisions may not be based solely on the results provided by the automated tool. This restriction does not apply if:

(i) The use of automated tools is required or authorized by law.

(ii) The decision is made by ING for purposes of (a) entering into or performing a contract or (b) managing the contract, provided the underlying request leading to a decision by ING was made by the Individual (e.g., where automated tools are used to filter promotional game submissions or in the context of the provision of mortgage and other financial products); or

(iii) Suitable measures are taken to safeguard the legitimate interests of the Individual, e.g., the Individual has been provided with an opportunity to express his point of view.

15 Transfer of Personal Data to Third Parties

Policy statement
ING shall make sure that the requirements for transferring Personal Data to Third Parties outside ING as listed in this Article (15) are met. Note that a transfer of Personal Data includes situations in which ING discloses Personal Data to Third Parties (e.g. in the context of corporate due diligence) or where ING provides remote access to Personal Data to a Third Party. ING shall also make sure the additional requirements in this Article are met if Personal Data is transferred to a Non-Adequate Country. In this Article, ING refers to the relevant Group Company.

Transfer of Personal Data

15.1 ING shall transfer Personal Data to a Third Party Controller to the extent necessary to serve the applicable legitimate purposes for which the Personal Data are Processed.

Third Party Controller contracts

15.2 Third Party Controllers (other than government agencies or other public bodies) may Process Personal Data only if they have a written contract or a contract in a similar form (e.g. electronic) with the relevant Group Company. In the contract, ING shall seek to contractually protect the data protection interests of the Individuals. All such contracts shall be drafted in consultation with or in accordance with guidelines provided by the appropriate Data Protection Executive. Individual Business Contact Data may be transferred to a Third Party Controller without a contract if it is reasonably expected that such Business Contact Data will be used by the Third Party Controller to contact the Individual for legitimate business purposes related to the Individual's job responsibilities with the relevant Client, Supplier or Business Partner.

Third Party Processor contracts

15.3 Third Party Processors may Process Personal Data only if they have a written contract or a contract in a similar form (e.g. electronic) with ING. Contracts with a Third Party Processor who will handle Personal Data must include the following provisions:

(i) The Processor shall Process Personal Data only in accordance with ING's instructions and for the purposes authorized by ING; and
(ii) The Processor shall keep the Personal Data confidential; and
(iii) The Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data; and
(iv) The Third Party Data Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to ING without the prior written consent of ING (or: the Processor warrants that the subcontractors will be compliant with the terms of the contract it has with ING); and
(v) ING has the right to review the security measures taken by the Third Party Processor and the Third Party Processor shall submit its relevant data processing facilities to audits and inspections by ING or any relevant government authority; and
(vi) The Third Party Processor shall promptly inform ING of any actual or suspected security breach involving Personal Data; and
(vii) The Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide ING with all relevant information and assistance as requested by ING regarding the security breach.

Transfer of Data to a Non-Adequate Country

15.4 This Article sets forth additional rules for the cross-border transfer of Personal Data to a Third Party located in a Non-Adequate Country that must be complied with in addition to the other requirements set out in this Policy. Personal Data may be transferred to a Third Party located in a Non-Adequate Country only if:

(i) The transfer is necessary for the performance of a contract with the Individual, for managing a contract with the Individual or to take necessary steps at the request of the Individual prior to entering into a contract, e.g., for processing orders; or
(ii) A contract has been concluded between ING and the relevant Third Party that provides for safeguards at a similar level of protection as that provided by this Policy or the contract shall conform to any model contract requirement under applicable local law, if any; or
(iii) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between ING and a Third Party; or
(iv) The Third Party has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an “adequate” level of data protection; or
(v) The Third Party has implemented binding corporate rules or a similar transfer control mechanism which provide adequate safeguards under applicable law, a copy of the binding corporate rules or evidence of the transfer control mechanism must be provided to ING prior to the transfer taking place; or
(vi) The transfer is necessary to protect a vital interest of the Individual; or
(vii) The transfer is necessary in connection with legal proceedings, advice or rights; or
(viii) The transfer is necessary to satisfy a pressing need to protect an important public interest; or
(ix) The transfer is required by any law or regulation to which the relevant Group Company is subject; or
(x) The Data that will be transferred is included in a public register.

Items (viii) and (ix) above require:

(i) The prior approval of the appropriate Data Protection Executive; and
(ii) That suitable measures are taken to safeguard the legitimate interests of the Individual (which may include consultation with the Dutch Data Protection Authority).

Consent for transfer

15.5 If none of the grounds listed in Article 15.4 exist or if applicable local law so requires ING shall (also) seek consent from the Individual for the transfer to a Third Party located in a Non-Adequate Country. Prior to asking for consent, the Individual shall be provided with the following information:

(i) The purpose of the transfer; and
(ii) The identity of the transferring Group Company; and
(iii) The identity or categories of Third Parties to which the Data will be transferred; and
(iv) The categories of Data that will be transferred; and
(v) The country to which the Data will be transferred; and
(vi) The fact that the Data will be transferred to a Non-Adequate Country.

Article 6.4 applies to the granting, denial or withdrawal of consent.

Transfers between Non- Adequate Countries

15.6 This Article sets forth additional rules for cross-border transfers of Personal Data that were collected in connection with the activities of a Group Company located in a Non-Adequate Country to a Third Party also located in a Non-Adequate Country. In addition to the grounds listed in Article 15.4, these transfers are permitted if they are:

(i) Necessary for compliance with a legal obligation to which the relevant Group Company is subject.
(ii) Necessary to serve the public interest.
(iii) Necessary to satisfy the legitimate purposes for which the Data are Processed.

16 Overriding Interests

Policy Statement
There may be circumstances in which ING can decide to override some of the obligations ING or rights of Individuals under this Policy, but only under the conditions set forth in this Article and to the extent that this is possible under applicable local law.

Overriding Interests

16.1 Some of the obligations of ING or rights of Individuals under this Policy may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Individual (**Overriding Interest**). An Overriding Interest exists if there is a need to:

(i) Protect the legitimate business interests of ING including but not limited to:
  (a) The health, security or safety of Employees or Individuals; or
  (b) ING's intellectual property rights, trade secrets or reputation; or
  (c) The continuity of ING's business operations; or
  (d) The preservation of confidentiality in a proposed sale, merger or acquisition of a business; or
  (e) The involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes.
(ii) Prevent or investigate (including cooperating with law enforcement) suspected or actual violations of law; or
(iii) Otherwise protect or defend the rights or freedoms of ING, its Employees or other persons.

Exceptions in the event of Overriding Interests

16.2 If an Overriding Interest exists, one or more of the following obligations of ING or rights of the Individual may be set aside:

(i) Article 7.1 (Processing Personal Data for closely related purposes); and

(ii) Article 10.1 and 10.2 (information provided to Individuals, Personal Data not obtained from the Individuals); and

(iii) Article 11.1 (rights of Individuals); and

(iv) Articles 12.2 and 12.3 (Staff access limitations and confidentiality obligations); and

(v) Articles 15.2, 15.3 and 15.4 (ii) (contracts with Third Parties).

Sensitive Data

16.3 The requirements of Articles 8.1 and 8.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 16.1 (i) (a), (c) and (e), (ii) and (iii).

Prior approval of Data Protection Executive

16.4 Setting aside obligations of ING or rights of Individuals based on an Overriding Interest requires prior approval of the appropriate Data Protection Executive.

Information to Individual

16.5 Upon request of an Individual, ING shall inform the Individual of the Overriding Interest for which obligations of ING or rights of the Individual have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 11.1 or 12.1, in which case the request shall be denied.

PART III SUPERVISION, COMPLIANCE AND LEGAL ISSUES

17 Supervision and compliance

17.1 Business management is responsible for compliance with the Policy in each Business Unit.

Bank Data Protection Executive (Bank DPE)

17.2 The Bank Data Protection Executive shall supervise the implementation of and compliance with the Policy in each Business Unit, which includes the responsibilities and activities as further described in Article 18 of this Policy. The Bank Data Protection Executive role shall be fulfilled by the Vice-Chairman.

Bank Data Protection Officer (Bank DPO)

17.3 The Bank Data Protection Officer is responsible for supervising general compliance with and for advice on the implementation and interpretation of the Policy throughout ING, which includes the responsibilities and activities as further described in Article 18. The Bank Data Protection Officer role shall be fulfilled by a Bank Tier 2 functionary.

BU Data Protection Executive (BU DPE)

17.4 Business management shall designate BU Data Protection Executives sufficient to direct compliance with this Policy within their respective Business Units. The Data Protection Executive shall perform its functions as further detailed in Article 18.

BU Data Protection Officer (BU DPO)

17.5 Business management shall designate BU Data Protection Officers sufficient to direct compliance with this Policy within their respective Business Units. The Data Protection Officer shall perform its functions as further detailed in Article 18. The BU Data Protection role shall be fulfilled by the appropriate second line of defence functionary.

Data Protection Officer with a statutory position

17.6 Where a Data Protection Officer holds his position pursuant to law, he shall carry out his job responsibilities to the extent they do not conflict with his statutory position.

18. Responsibilities

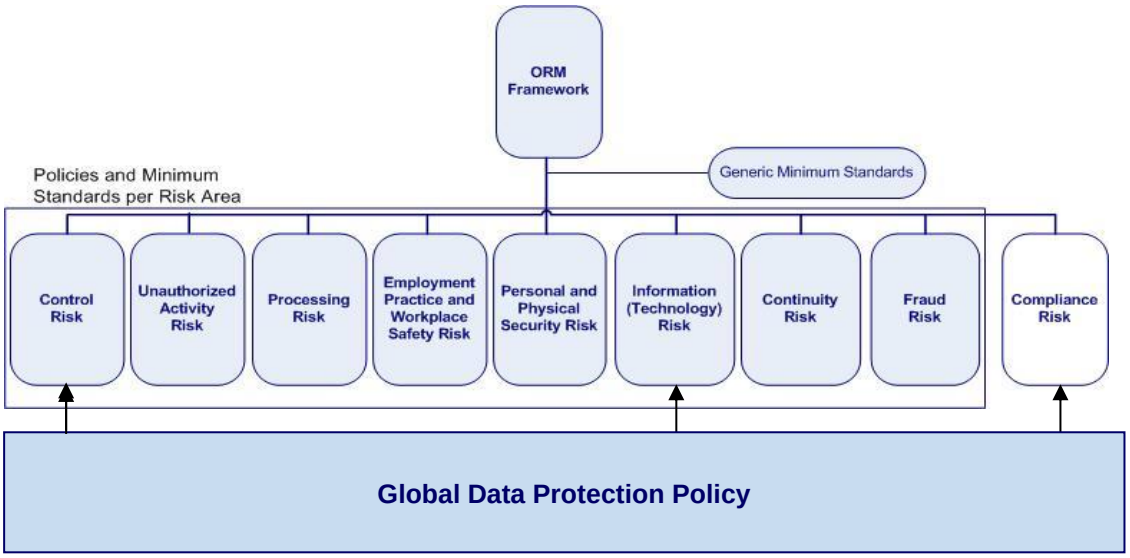
Who	Responsibilities
Data Protection Executive (DPE)	The appropriate BU Data Protection Executive is responsible for the compliance with and implementation of the Policy in a Business Unit from a business point of view. The Data Protection Executive shall decide on, provide the means for and facilitate the handling of all issues relating to data protection in the relevant Business Unit. The Data Protection Executive must: * Ensure that his Business Unit will process Personal Data in accordance with this Policy. * Implement the changes required within his Business Unit for achieving compliance. * Work together with and facilitate the appropriate DPO to create

Who	Responsibilities
	and maintain a framework for the development, implementation and updating of local data protection policies and procedures (including training and education). * Ensure that the Staff working in his Business Unit follow the required training. * Duly fill out and sign off audit related questionnaires and Data Protection Impact Assessments. * Notify the appropriate Data Protection Officer and obtain the DPO's advice on all data protection risks or incidents, compliance issues or questions in the Business Unit where he is responsible for the privacy compliance. * Escalate to the Bank DPE, where needed. * Provide reports, as appropriate but for a minimum every quarter, to the Bank DPE on data protection risks and compliance issues.
Bank Data Protection Executive (Bank DPE)	The Bank Data Protection Executive is responsible for supervising general compliance with and implementation of the Policy throughout ING. The Bank Data Protection Executive must: * Liaise with the Bank DPO for all data protection risks, incidents, compliance issues or questions that have been escalated to the Bank DPE. * Shall provide a report on data protection risks and compliance issues to the Bank DPO and to the Bank NFRC for a minimum once a year, but more frequently where needed.
Data Protection Officer (DPO)	The appropriate BU Data Protection Officer is responsible for supervising compliance of the relevant Business Unit(s) with the Policy and for providing advice to the appropriate DPE. The appropriate Data Protection Officer must: * Have expert knowledge of data protection law and practices. * Provide advice to the appropriate DPE on all data protection risks or incidents, compliance issues or questions in the Business Unit when requested by the DPE. * Work together with the DPE to create and maintain a framework for the development, implementation and updating of local data protection policies and procedures to support and monitor the implementation and embedding of the Policy within its Business Unit. * Advice on and support the correct interpretation of the Policy with communication and training of Staff. * Be able to operate independently from the business and (senior) management without conflict of interests with its other professional duties. * Have control and monitoring powers (the right to perform

Who	Responsibilities
	internal investigations and to access information). * Report data protection risks and compliance issues to the Bank DPO for a minimum every quarter, but more frequently where needed.
Bank Data Protection Officer (Bank DPO)	The Bank DPO is responsible for supervising general compliance with the Policy throughout ING. The Bank DPO must: * Coordinate, in conjunction with the appropriate DPO, official investigations or inquiries into the Processing of Data by a government authority. * Where possible, provide guidance to the DPOs on the interpretation of the Policy in relation to local data protection issues and will ensure that the Policy is updated when necessary. * shall provide a report on data protection risks and compliance issues to the Bank DPE and to the Bank NFRC for a minimum once a year, but more frequently where needed.
Staff handling Personal Data	Staff who have access to Personal Data as part of their job are responsible for complying with this Policy. Staff must: * Only access Personal Data to the extent necessary to serve the applicable legitimate purposes for which ING processes Personal Data and to perform their job. * Apply reporting mechanisms of any (possible) incident or issue relating to Personal Data to their manager or alternatively to the appropriate DPE or via the Whistleblower Procedure.

19 Policies and procedures

19.1 ING shall develop and implement policies, minimum standards and procedures to comply with this Policy. This Policy is related to a number of other policies in the ING Bank Policy House. As a rule this Policy provides the basis for other more detailed policies. The graph below shows the most relevant relations.



Information system documentation

19.2 ING shall maintain documentation (e.g. Data Protection (Privacy) Impact Assessments, Control Framework/Register, Operational Security Guidelines) regarding the structure, functioning, security and control of its information technology systems that Process Personal Data.

20 Training

Staff training

20.1 ING shall provide training on this Policy and related confidentiality obligations to Staff members who have access to Personal Data. In-depth trainings shall be provided on an ongoing basis to specific functions, including in any event the Data Protection Executives and Data Protection Officers. More detailed trainings focusing on specific local requirements relevant for compliance with this Policy shall be provided on a local or regional level. All of these trainings may be provided through the global ING Learning Center and on a regional or local basis.

21 Monitoring compliance

Audits

21.1 Corporate Audit Services shall audit business processes and procedures that involve the Processing of Personal Data for compliance with this Policy. The audits shall be carried out in the course of the regular activities of Corporate Audit Services or at the request of the Bank Data Protection Executive. The Bank Data Protection Executive may also request to have an audit as specified in this Article 21.1 conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Bank Data Protection Executive shall be informed of the results of the audits. The Bank Data Protection Executive shall provide a copy of the audit results to the relevant Data Protection Executive(s) and to the Bank Data Protection Officer. A copy of the audit results will be provided to the Dutch Data Protection Authority upon request.

Mitigation

21.2 ING shall, if so indicated, ensure that adequate steps are taken to address breaches of this Policy identified during the monitoring or auditing of compliance pursuant to this Article 21.

22 Complaints procedure

Complaint to BU Data Protection Executive

22.1 Without prejudice to the Individual's rights and remedies available in their local jurisdictions as set out in Article 23.1, Individuals may file a complaint regarding compliance with this Policy or violations of their rights under this Policy or under applicable local law in accordance with the local complaints procedure set forth in the relevant privacy policy or contract or as otherwise communicated to the Individual. The local complaints procedure shall ensure the initiation of an investigation into the complaint and ensure the involvement of the appropriate BU Data Protection Executive.

22.2 The BU Data Protection Executive shall:

(a) Support the investigation; and

(b) Always obtain advice from the relevant BU Data Protection Officer on the appropriate measures for compliance; and

(c) Advise the business in accordance with the advice provided by the relevant BU Data Protection Officer on the appropriate measures for compliance and monitor, through completion, the steps designed to achieve compliance; and

(d) Notify the Bank Data Protection Officer, where relevant.

The appropriate Data Protection Officer may consult with any government authority having jurisdiction over a particular matter about the measures to be taken.

Reply to Individual

22.3 Within four weeks of ING receiving a complaint, ING shall inform the Individual in writing either (i) of ING's position with regard to the complaint and any action ING has taken or will take in response or (ii) when he will be informed of ING's position which date shall be no later than four weeks thereafter. The appropriate BU Data Protection Executive shall send a copy of the complaint and ING's written reply to the relevant BU Data Protection Officer and to the Bank Data Protection Officer, if notified pursuant to Article 22.2 (d).

Complaint to Bank Data Protection Officer

22.4 An Individual may escalate a complaint with the Bank Data Protection Officer if:

(i) The resolution of the complaint by the appropriate Business Unit is unsatisfactory to the Individual (e.g., the complaint is rejected).

(ii) The Individual has not received a response as required by Article 22.3.

(iii) The time period provided to the Individual pursuant to Article 22.3 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response; or

(iv) In one of the events listed in Article 11.4.

The procedure described in Articles 22.1 through 22.3 shall apply to complaints escalated to the Bank Data Protection Officer in accordance with Article 22.4. The Bank Data Protection Officer shall notify the Bank Data Protection Executive of any such escalated complaint, where relevant.

23 Legal issues

Local law and jurisdiction

23.1 Any Processing by ING of Personal Data shall be governed by applicable local law. Individuals keep their own rights and remedies as available in their local jurisdictions, e.g. the right to lodge a complaint with the local data protection authority or bring claims before the local court. Local government authorities having jurisdiction over the relevant matters shall maintain their authority.

Supplemental protection provided by this Policy

23.2 This Policy shall be governed by and interpreted in accordance with Dutch law. This Policy shall apply only where it provides supplemental protection for Personal Data. Where applicable local law provides more protection than this Policy, local law shall apply. Where this Policy provides more protection than applicable local law or provides additional safeguards, rights or remedies for Individuals, this Policy shall apply.

Lead authority for supervision of rules

23.3 Compliance with this Policy shall be exclusively supervised by the Dutch Data Protection Authority in the Netherlands, which is also exclusively authorized to advise ING Bank N.V. on the application of this Policy at all times. The Dutch Data Protection Authority shall have investigative powers based on the Dutch Data Protection Act. To the extent the Dutch Data Protection Authority has discretionary powers related to enforcement of the Dutch Data Protection Act, it shall have similar discretionary powers for enforcement of this Policy.

Exclusive jurisdiction under Policy

23.4 Any complaints or claims of an Individual concerning any supplemental right the Individual may have under this Policy shall be directed to ING Bank N.V. only and shall be brought before the Dutch Data Protection Authority in the Netherlands or the competent court in Amsterdam, the Netherlands. The Dutch Data Protection Authority and courts in Amsterdam, the Netherlands have exclusive jurisdiction over any supplemental rights provided by this Policy. Complaints and claims shall be admissible only if the Individual has first followed the complaints procedure set forth in Article 22 of this Policy.

Policy enforceable against ING Bank N.V. only

23.5 Any additional safeguards, rights or remedies granted to Individuals under this Policy are granted by and enforceable in the Netherlands against ING Bank N.V. only.

Available remedies, limitation of damages and burden of proof

23.6 In addition to any remedies Individuals may have under their applicable local law, on the basis of this Policy, Individuals shall only be entitled to remedies available to data subjects under the Dutch Data Protection Act, the Dutch Civil Code and the Dutch Code on Civil Procedure. However, ING Bank N.V. shall only be liable for direct damages suffered by an Individual resulting from a violation of this Policy. Provided an Individual can demonstrate that it has suffered damage and establishes facts which show it is plausible that the damage has occurred because of a violation of this Policy, it will be for ING Bank N.V. to prove that the damages suffered by the Individual due to a violation of the Policy are not attributable to the relevant Group Company**.**

Mutual assistance and redress

23.7 All Group Companies shall co-operate and assist each other to the extent reasonably possible to handle:

(i) A request, complaint or claim made by an Individual; or

(ii) A lawful investigation or inquiry by a competent government authority.

The Group Company who receives a request, complaint or claim from an Individual is responsible for handling any communication with the Individual regarding his request, complaint or claim except where circumstances dictate otherwise.

The Group Company that is responsible for the Processing to which the request, complaint or claim relates, shall bear all costs involved and reimburse ING Bank N.V. at ING Bank N.V.'s first request.

24 Sanctions for non-compliance

Non-compliance

24.1 Non-compliance of Staff with this Policy may be regarded as a serious breach of the trust ING must be able to place in its Employees and other members of Staff. Non-compliance by an Employee may therefore result in a sanction, such as suspension or other disciplinary measures or measures under labour law, which may include summary dismissal. Non-compliance by members of Staff that are not Employees may result in termination of the relevant contract with this member of Staff. Staff will not be penalized for raising issues relating to compliance with this Policy. The ING Whistleblower procedure is applicable.

25 Conflicts between this Policy and applicable local law

Conflict of law when transferring Data

25.1 Where a legal requirement to transfer Personal Data conflicts with the laws of the Member States of the EEA or the law of Switzerland, the transfer requires the prior approval of the Bank Data Protection Executive. The Bank Data Protection Executive shall seek the advice of the Bank Data Protection Officer. The Bank Data Protection Officer may seek the advice of the Dutch Data Protection Authority or another competent government authority.

Conflict between this Policy and law

25.2 In all other cases, where there is a conflict between applicable local law and the Policy, the relevant Data Protection Executive or manager of Employees or Staff raising the issue shall consult with the Bank Data Protection Executive to determine how to comply with this Policy and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

New conflicting legal requirements

25.3 The relevant Data Protection Executive shall promptly inform the Bank Data Protection Executive of any new legal requirement that may interfere with ING's ability to comply with this Policy.

26 Changes to the Policy

26.1 Any changes to this Policy require the prior approval of General Legal Counsel. The General Legal Counsel shall consult the Bank Data Protection Officer before approving any such changes. ING Bank N.V. shall notify the Dutch Data Protection Authority in case of

substantial changes to the Policy on a yearly basis, or earlier if this is required by the nature of the substantial change.

26.2 This Policy may be changed without Individual's consent even though an amendment may relate to a benefit conferred on Individuals.

26.3 Any amendment shall enter into force after it has been approved by the General Legal Counsel and has been published on the ING Intranet and ING website(s).

26.4 Any request, complaint or claim of an Individual involving this Policy shall be judged against this version of the Policy as it is in force at the time the request, complaint or claim is made.

27 Transition Periods

General transition period

27.1 Except as indicated below, there shall be a two-year transition period for compliance with this Policy. Accordingly, except as otherwise indicated, within two years of the Effective Date, all Processing of Personal Data shall be undertaken in compliance with the Policy. During any transition period, ING shall strive to comply with the Policy.

Transition period for new Group Companies

27.2 Any entity that becomes a Group Company after the Effective Date shall comply with this Policy within two years of becoming a Group Company.

Transition period for IT Systems

27.3 Where implementation of this Policy requires updates or changes to information technology systems (including replacement of systems), the transition period shall be four years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process.

Transition period for existing agreements

27.4 Where there are existing agreements with Third Parties that are affected by this Policy, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

Transition period for local-for-local systems

27.5 Processing of Personal Data that were collected in connection with activities of a Group Company located in a Non-Adequate Country shall be brought into compliance with this Policy within three years of the Effective Date.

Contact details

ING Bank Data Protection Officer
c/o ING Bank N.V.
Email address: DPO.office@ing.nl
Telephone number: +31 (0) 20 430 8015

APPENDIX 1 DEFINITIONS AND INTERPRETATION

Definitions

Archive shall mean a collection of Personal Data that are no longer necessary to achieve the purposes for which the Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, litigation, investigations or general archiving purposes. An archive includes any data set that can no longer be accessed by any Employee other than the system administrator.

Article shall mean an article in this Policy.

Bank Data Protection Executive (Bank DPE) shall mean the officer as referred to in Article 17.2.

Bank Data Protection Officer (Bank DPO) shall mean the officer as referred to in Article 17.3.

Bank NFRC shall mean the Bank Non-Financial Risk Committee.

BU Data Protection Executive (BU DPE) or **Data Protection Executive (DPE)** shall mean the first line Data Protection Executive for a Business Unit appointed pursuant to Article 17.4, that is someone in local business management with primary budget responsibility that can be held accountable for the actual implementation of and compliance with the Policy, which function is further determined in Article 18.

BU Data Protection Officer (BU DPO) or **Data Protection Officer (DPO)** shall mean the second line Data Protection Officer for a Business Unit appointed pursuant to Article 17.5, which function is further determined in Article 18.

Business Contact Data shall mean any data typically found on a business card and used by the Individual in his contact with ING.

Business Partner shall mean any Third Party, other than a Client or Supplier, that has or had a business relationship or strategic alliance with ING (e.g. joint marketing partner, joint venture or joint development partner).

Business Purpose shall mean a purpose for Processing Personal Data as specified in Article 6 or 7 or for Processing Sensitive Data as specified in Article 7 or 8.

Business Unit shall mean a Group Company that is a local, regional or universal bank. Under this Policy, corporate and other staff departments are considered Business Units and have the same responsibilities.

Client shall mean any Third Party that purchases, may purchase or has purchased an ING product or service.

Data Controller shall mean the party processing the Personal Data that determines the means and the purposes of the Processing.

Data Processor shall mean the party Processing the Personal Data on behalf of the Data Controller and at its direction that is not under the direct authority of the Data Controller.

Dependant shall mean the spouse, partner or child belonging to the household of the Individual.

Effective Date shall mean the date on which this Policy becomes effective as set forth in Article 5.1.

Employee shall mean an employee, job applicant or former employee of ING. This term does not include people working at ING as external consultants or employees of Third Parties providing services to ING.

Employee Data shall mean any information relating to an identified or identifiable Employee.

EEA or **European Economic Area** shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein.

EU Data Protection Directive shall mean the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of and the free movement of such data.

Group Company shall mean ING Groep N.V. and ING Bank N.V. and any company or legal entity, including branches and representative offices, of which ING Bank N.V., directly or indirectly, owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint or remove the majority of the member of the board of directors or equivalent governing body or cast the majority of votes at meetings of the board of directors or equivalent governing body.

General Legal Counsel shall mean the head of legal of ING Bank N.V.

Guidance Documents shall mean the documents with additional information on and an explanation of the adequate standards in this Policy.

Individual shall mean any Client, Supplier or Business Partner that is a natural person or any employee or any person working for a Client, Supplier or Business Partner, including individuals whose personal data ING Processes on the basis of a legal or contractual requirement towards a third party (e.g. beneficiaries, mandated persons or legal representatives).

ING Bank NV shall mean ING Bank N.V., having its registered seat in Amsterdam, The Netherlands.

ING shall mean ING Bank N.V. and its Group Companies.

Non- Adequate Country shall mean a country that under applicable local law (such as Article 25 of the EU Data Protection Directive) is deemed not to provide an "adequate" level of data protection. A schedule of Adequate Countries is available on the ING website.

Original Purpose shall mean the purpose for which Personal Data was originally collected.

Overriding Interest shall mean the pressing interests set forth in Article16.1 based on which the obligations of ING or rights of Individuals set forth in Article 16.2 and 16.3 may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Individual.

Personal Data or **Data** shall mean any information relating to an identified or identifiable Individual.

Policy or **GDP Policy for Clients** shall mean this ING Global Data Protection Policy for Client, Supplier and Business Partner Data.

Processing or **to Process** shall mean any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.

Secondary Purpose shall mean any purpose other than the Original Purpose for which Personal Data is further Processed.

Sensitive Data shall mean Personal Data that reveal an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sexual orientation, criminal offences, criminal records, proceedings with regard to criminal or unlawful behaviour, or social security numbers issued by the government, or any other type of Data that qualifies as Sensitive Data under applicable local law.

Supplier shall mean any Third Party that provides goods or services to ING (e.g. an agent, consultant, intermediary or vendor).

Staff shall mean all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities using ING information technology systems or working primarily from ING's premises.

Third Party shall mean any person, private organization or government body outside ING.

Third Party Controller shall mean a Third Party that Processes Personal Data and determines the purposes and means of such Processing.

Third Party Processor shall mean a Third Party that Processes Personal Data on behalf of ING and at its direction that is not under the direct authority of ING.

Interpretations

INTERPRETATION OF THIS CODE:

(i) Unless the context requires otherwise, all references to a particular Article or Appendix are references to that Article or Appendix in or to this document, as they may be amended from time to time.

(ii) Headings are included for convenience only and are not to be used in construing any provision of this Policy.

(iii) If a word or phrase is defined, its other grammatical forms have a corresponding meaning.

(iii) The male form shall include the female form (and vice versa).

(iv) The words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa; and

(v) A reference to a document (including, without limitation, a reference to this Policy is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Policy or that other document.