# ING Bank N.V. Hungary Branch

# Local Data Protection Policy for Employee Data

# INFORMATION SHEET

The present Local Data Protection Policy is aimed at executing and implement on local basis the Global Data Protection Policy for Employee Data of ING as to design a Local Data Protection Policy (LDPP 2.0) for employee data of ING Bank N.V. Hungary Branch.

**Target audience:**
All employees (temporary or permanent) of all majority owned ING businesses (or business units), inclusive of **ING Bank N.V. Hungary Branch** (“**ING Hungary”)** businesses under ING’s management control and staff departments.

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

**Version:**
2.0

**Replaces:**
This ING Local Data Protection Policy for Employee Data (**“Policy”**) supersedes all ING Hungary data protection employee 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 Hungary NFRC

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



| | |
|---|---|
| Effective date | 1. March 2020. |
| Last modified | 15. January 2020. |
| Version number | 2.0 |
| Supervision | Yearly |
| Group related | Global Data Protection Policy |

| | |
|---|---|
| Person liable for regulation | Legal |
| Issued by | Legal |
| Last modified by | Dóra Orosz Dr. |

# CONTENT

# PART I GENERAL INTRODUCTION

## 1 Introduction

**1.1** All employees are expected to handle information with care. In particular, the security and confidentiality of all proprietary information and data processing, including employees' personal confidential information, must be safeguarded in accordance with inter alia, the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC **(General Data Protection Regulation, "GDPR"),** as well as the Act CXII of 2001 on Information Self-Determination and Freedom of Information (hereinafter: Act of Information) with due regard to the Act I of 2012 on the Labor Code (Hungarian Labor Code) and other applicable laws and regulations.

In this Policy it is explained that the protection of personal data is about:

- being transparent in what ING Hungary does with personal data of employees;
- 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 employees about the purposes for which their personal data are processed;
- and which ING business is responsible for the processing;
- allowing employees to obtain an overview of their personal data;
- allowing employees to correct or delete their personal data or object to the processing of 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 client personal data please refer to the Local Data Protection Policy for Client, Supplier and Business Partner Data ("Local Data Protection Policy for Clients").

The capitalised terms which are used in this Policy are explained in **Appendix 1**.

## 2 Objective of this Policy

**2.1** This Policy aims to provide a clear statement on the protection of Employee Data of ING Hungary in order to provide an adequate level of protection for all Employee Data Processed within ING globally.

## 3 Scope

**3.1** This Policy addresses the Processing of all personal data of ING Employees ("**Employee Data**") by ING Hungary or by a Third Party on behalf of ING Hungary in accordance with Article 15.

### 3.2 Electronic and paper-based Processing

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

### 3.3 Data Protection Officer (DPO) advice

Where there is a question as to the applicability of this Policy, Staff shall seek the advice of the Local Data Protection Officer (BU DPO) defined in Article 19 of this Policy prior to the relevant Processing.

### 3.4 Compliance responsibility

These rules are binding on ING Hungary acting as a Data Controller and partially on ING Hungary acting as a Processor. The Local Data Protection Executive (BU DPE) defined in Article 19 of this Policy shall be responsible for business organisation's compliance with this Policy. Staff must comply with this Policy. When ING Hungary qualifies as a Data Processor, solely Article 16 of the Policy applies.

## 4 Applicability of local law and Policy

### 4.1 Employees keep local rights and remedies

Employees keep any rights and remedies they may have under applicable Hungarian law. This Policy shall apply only where it provides supplemental protection for Employee Data. Where Hungarian law provides more protection than this Policy, Hungarian law shall apply. Where this Policy provides more protection than applicable Hungarian law or provides additional safeguards, rights or remedies for Employees, this Policy shall apply, unless the application of the Policy would lead to conflict with Hungarian law in which case the Bank DPE based on advice of the Bank DPO will decide as to its application as closely as possible within the spirit of this policy.

## 5 Implementation

### 5.1 Effective Date

This Local Policy has been adopted by ING Hungary NFRC and shall enter into force as of 1. March 2020. ("**Effective Date**") and will be published on the ING Hungary Procedure Sharepoint at (Procedure Manual link) and made available to Employees upon request.

### 5.2 Policy supersedes prior policies

This Policy supersedes ING Hungary's data protection policies for employee data 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.

# PART II POLICY STATEMENTS

## 6 Purposes for processing Personal Data

**Policy statement**
ING Hungary shall only collect, use or otherwise Process Employee Data if the Processing falls within the scope of one (or more) of the legitimate Business Purposes listed below.

### 6.1 Legitimate Business Purposes

Employee Data shall be collected, used, stored or otherwise Processed if necessary, within the framework of responsible, efficient and effective human resources management, especially in light of one (or more) of the following activities:

(i) **Human resources and personnel management.** This purpose includes Processing that is necessary for the performance of an employment- or other contract with an Employee (or to take necessary steps at the request of an Employee prior to entering into a contract), or for managing the employment-at-will relationship, e.g., management and administration of recruiting and outplacement, compensation and benefits, payments, tax issues, career and talent development, insider trading regulations, performance evaluations, training, travel and expenses, Employee communications, workforce analytics and international assignments, dispute resolution and litigation; or

(ii) **(Electronic) Business process execution and internal management.** This purpose addresses activities such as scheduling work, recording time, managing company assets, provision of central processing facilities for efficiency purposes, conducting internal audits and investigations, implementing insider trading and other similar regulations, implementing business controls, and facilitating efficient and effective electronic communications within ING; or

(iii) **Health, safety and security.** This purpose addresses activities such as those involving occupational safety and health, the protection of assets, products, services or the reputation of ING, its Staff and clients or other financial institutions, the authentication of Employee status and access rights and monitoring compliance with ING regulations; or

(iv) **Organizational analysis and development and management reporting.** This purpose addresses activities such as conducting Employee surveys, managing mergers, acquisitions and divestitures, and Processing Employee Data for management reporting and analysis; or

(v) **Compliance with legal obligations.** This purpose addresses the Processing of Employee Data as necessary for compliance with laws, regulations and sector specific guidelines to which ING is subject; or

(vi) **Protecting the vital interests of Employees.** This is where Processing is necessary to protect the vital interests of an Employee, e.g., for urgent medical reasons.

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 Hungary, including but not limited to:
   a) misuse of products, services and facilities of financial institutions;
   b) (attempted) criminal or otherwise negative conduct;

c) 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 Employee Data finds legitimacy in one of the Business Purposes listed above, it is necessary to seek the advice of the Local Data Protection Officer (BU DPO) before the Processing takes place.

Legal basis for processing your personal data are set in line with the above defined purposes in Annex 9 of the *Procedure on the Personal Data Processing in the HR Department*.

### 6.2 Employee consent

Employee consent alone generally cannot be used as a legitimate basis for Processing Employee Data, unless specifically required or permitted under local law. One of the Business Purposes must exist for any Processing of Employee Data. If applicable local law so requires, in addition to having a Business Purpose for the relevant Processing, ING Hungary shall also seek Employee consent for the Processing. If none of the Business Purposes applies, ING Hungary may request Employee consent for Processing of Employee Data, but only if the Processing has no foreseeable adverse consequences for the Employee or is specifically required or permitted under local law.

When seeking Employee consent, ING Hungary must inform the Employee:

(i) of the purposes of the Processing for which consent is requested; and

(ii) of the possible consequences for the Employee of the Processing and other relevant information necessary for the Employee to make a conscious decision about the Processing of his Personal Data (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 Employees can exercise their rights); and

(iii) that he is free to refuse and withdraw consent at any time without consequence to his employment relationship.

- ING Hungary shall be able to demonstrate that an Employee has consented to the Processing of his Personal Data where ING processes Personal Data on the basis of the Employee's consent.
- Where the Employee's consent has been given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. ING shall, when assessing whether consent has been freely given take utmost account of whether inter alia the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.
- consent shall be freely given, specific, informed and an unambiguous indication of the Employee's wishes by means of a statement or a clear affirmative action signifying agreement to the Processing of Personal Data.

A request for Employee consent requires the authorization of the Local Data Protection Executive (BU DPE). The Local Data Protection Executive (BU DPE) is required to seek advice of the Local Data Protection Officer (BU DPO).

### 6.3 Denial or withdrawal of Employee consent

The Employee may both deny consent and withdraw consent at any time without consequence to his employment relationship unless such Employee's consent is required by local law or regulation. It shall be as easy to withdraw consent as to give consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Where Processing is undertaken at the Employee's request (e.g., he subscribes to a service or seeks a benefit), he is deemed to have provided consent to a Processing.

### 6.4 Employee consent for direct marketing

No Employee Data shall be provided to, or used or otherwise Processed on behalf of, Third Parties for purposes of direct marketing without prior consent of the Employee. Employee Data may be used by ING Hungary in the context of ING benefits for Staff including agreed upon discounts for products or services for Staff, unless this is not allowed under applicable law without the Employee's consent.

### 6.5 Limitations on Processing Data of Dependants of Employees

ING Hungary will Process Data of Dependants of an Employee if:

(i) the Data were provided with the consent of the Employee or the Dependant; or
(ii) Processing of the Data is reasonably necessary for the performance of a contract with the Employee or for managing the employment-at-will relationship; or
(iii) the Processing is required or permitted by applicable local law.

## 7 Use for other Purposes

**Policy statement**
ING Hungary shall in principle only use Employee Data for the purposes for which they were originally collected, but may use Employee Data also for other, related, purposes under the conditions set forth in this Article 7.

### 7.1 Use of Data for Secondary Purposes

Generally, Employee Data shall be used only for the purposes for which they were originally collected (**Original Purpose**). Employee Data may be Processed for legitimate purposes of ING Hungary 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. To determine if there is a Secondary Purpose, ING Hungary shall consider the context in which data is processed, including if appropriate, such factors as:

(i) any link between the Original Purpose and the Secondary Purpose;
(ii) the context in which the Employee Data have been collected, in particular regarding the relationship between Employees and ING Hungary;
(iii) the nature of Employee Data, in particular where Sensitive data is processed;
(iv) the possible consequences of the intended further processing for Employees;
(v) the existence of appropriate safeguards which may include encryption or pseudonymisation.

Depending on the sensitivity of the relevant Employee Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Employee, ING Hungary may include additional measures such as:

(i) limiting access to the Data;
(ii) imposing additional confidentiality requirements;
(iii) taking additional security measures;
(iv) informing the Employee about the Secondary Purpose;
(v) providing an opt-out opportunity; or
(vi) obtaining Employee consent in accordance with Articles 6.2.

### 7.2 Generally permitted uses of Data for Secondary Purposes

It is generally permissible to use Employee 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) HR analyses, statistical, historical or scientific research; or
(v) dispute resolution or litigation; or
(vi) legal or business consulting; or
(vii) insurance purposes.

### 7.3 Data Protection Executive (DPE) advice

Before commencing Processing Personal Data for a Secondary Purpose, Staff shall seek the approval of the Local Data Protection Executive (BU DPE). The Local Data Protection Executive (BU DPE) shall seek advice of the Local Data Protection Officer (BU DPO) before providing or denying approval.

## 8 Processing Sensitive Data

**Policy statement**
ING Hungary 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 Employee 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 Hungarian law.

### 8.1 Specific purposes for Processing Sensitive Data

This Article sets forth specific rules for Processing Sensitive Data. ING Hungary 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 Employee):
  (a) providing preferential status to persons from particular racial, ethnic or cultural minorities to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Sensitive Data allows an objective determination that an Employee belongs to a minority group and the Employee has not filed a written objection to the relevant Processing;
  (b) in some countries photos and video images of Employees are qualified as racial or ethnic data. ING Hungary may process photos and video images (i) for inclusion in (electronic) Employee directories and (ii) for site access and security reasons;

(i) **Physical or mental health data** (including any opinion of physical or mental health and data relating to short- or long term disabilities and absence due to illness or pregnancy, or in case of receiving treatment related to a human reproduction procedure):
   (a) providing health services to an Employee provided that the relevant health data are processed by or under the supervision of a health professional who is subject to professional confidentiality requirements;
   (b) administering pensions, health and welfare benefit plans, maternity, paternity or family leave programs, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee;
   (c) reintegrating or providing support for Employees entitled to benefits in connection with illness or work incapacity;
   (d) assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities, including initial hiring decision;
   (e) providing facilities in the workplace to accommodate occupational health and safety, health problems or disabilities;
   (f) providing facilities for safeguarding the security and integrity of ING (e.g. biometrical access tools);

(ii) **Criminal data** (including data relating to suspected criminal behaviour, criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour):
   (a) assessing an application by an Employee to make a decision about the Employee on (continued) eligibility for positions, projects or scope of responsibilities; including initial hiring decision or provide a service to the Employee;
   (b) safeguarding and ensuring the security and integrity of the financial sector, ING, its Staff and clients

(iii) **Genetic and Biometric data**
   (a) for site access and security reasons.

**8.2 General purposes for Processing of Sensitive Data**

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

(i) as required by or allowed under applicable local law;
(ii) for the establishment, exercise or defence of a legal claim or whenever courts are acting in their legal capacity;
(iii) to protect a vital interest of an Employee, when it is impossible to obtain the Employee's consent first;
(iv) to the extent necessary to comply with an obligation of international public law; or
(v) in the context of job applications if these are voluntarily provided by the job applicant.

**8.3 Employee consent for Processing Sensitive Data**

Employee consent alone generally cannot be used as a legitimate basis for Processing Sensitive Data unless specifically required or permitted under local law. One of the grounds listed in Article 8.1 or 8.2 must exist for any Processing of Sensitive Data. If applicable local law so requires, in addition to having one of the grounds listed in Article 8.1 or 8.2, ING shall also seek Employee consent for the Processing. If none of the grounds listed in Article 8.1 or 8.2 applies, ING may request Employee consent for Processing Sensitive Data, but only if the Processing has no foreseeable adverse consequences for the Employee (e.g. Employee diversity programs or networks, research). Articles 6.2.and 6.3 apply to the granting, denial or withdrawal of Employee consent.

### 8.4 Prior authorization of the Local Data Protection Executive (BU DPE)

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 Employee, the Processing requires the prior authorization of the Local Data Protection Executive (BU DPE), after the Data Protection Executive has sought advice of the Local Data Protection Officer (BU DPO).

### 8.5 Use of Sensitive Data for Secondary Purposes

In addition to the requirements of this Article 8. Sensitive Data of Employees may be Processed for Secondary Purposes in accordance with Article 7.

## 9 Quantity and quality of Data

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

### 9.1 No Excessive Data

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

### 9.2 Retention period

ING Hungary generally shall retain Employee 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 Hungary may specify (e.g., in a minimum standard, notice or records retention schedule) a time period for which certain categories of Employee Data may be kept.
Promptly after the applicable retention period has ended, the Data Owner will take steps to make sure that the Data be:

(i) securely deleted or destroyed in accordance with the Global Data Protection Minimum Standard; or
(ii) anonymized; or
(iii) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).

### 9.3 Quality of Data

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

### 9.4 Self-service

Where ING requires an Employee to update his own Employee Data, ING shall remind him at least once a year to do so.

### 9.5 Processing which does not require identification

If the purposes for which ING processes Personal Data do not or no longer require identification of the Individual involved, ING is not obliged to maintain, acquire or process additional information to identify the Individual for the sole purpose of complying with any provision of the GDPP and/or applicable laws.

## 10 Accountability and maintaining records

**Policy statement**
ING Hungary has to be able to demonstrate compliance with the Policy, by among other things maintaining records of processing activities under its responsibility.

### 10.1 Accountability

ING Hungary shall be able to demonstrate compliance with this Policy to the extent applicable to ING Hungary.

### 10.2

ING shall maintain records of its processing activities in writing, including in electronic form.
The record will contain the following information:

(i) the name and contact details of ING Hungary and, where applicable, the joint controller, and the Local Data Protection Officer (BU DPO);
(ii) the purposes of the processing;
(iii) a description of the categories of Individuals and of the categories of personal data;
(iv) the categories of recipients to whom the Personal Data have been or will be disclosed including their location;
(v) where applicable, transfers of personal data to a Non-Adequate Country, including the identification of that Non-Adequate Country and, in the case of transfers referred to in Article 15.5 (xii), the documentation of suitable safeguards;
(vi) where possible, the envisaged retention period of the different categories of data;
(vii) where possible, a general description of the technical and organisational security measures.

### 10.3 ING Hungary shall document the assessment as set out in Article 15.5 (xii).

## 11 Employee information requirements

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

### 11.1 Information requirements

ING shall inform Employees through the Privacy Statement for Employees about:

(i) the Business Purposes and Secondary Purposes for which their Data are Processed and if applicable the accompanying of Legitimate Interests pursued by ING Hungary or other legal bases if applicable as defined above;
(ii) the nature and categories of the Processed Data;
(iii) ING Bank, ING Group Companies and the categories of Third Parties to which the Data are disclosed (if any);
(iv) how Employees can exercise their rights including, if applicable, the right to lodge a

complaint with a supervisory authority;

(v) the transfer of Personal Data to a Non-Adequate Country or a country with an Adequacy Decision, the safeguards in place and the process to obtain a copy of them or where they have been made available;

(vi) the period for which the Data is retained, or if that is not possible, the criteria used to determine this period;

(vii) the contact details of the relevant Data Protection Officer, where applicable;

(viii) the existence of automated decision-making, including profiling and in case of Articles 14.1 and 14.3 meaningful information about the logic involved and the significance and the envisaged consequences of such processing for the Employee.

### 11.2 Easy access and clear language

The information provided to the Employee shall be concise, transparent, intelligible and easy accessible, using clear and plain language.

## 12 Employee rights

**Policy statement**
This Article addresses certain rights of Employees whose Personal Data are Processed by ING Hungary in its role as a Data Controller.

### 12.1 Rights to access

Every Employee has the right to request an overview of his Employee Data Processed by or on behalf of ING Hungary. Where reasonably possible, the overview shall contain**:**

(i) the Legitimate Business Purposes of the processing;

(ii) categories of Employee Data concerned;

(iii) categories of recipients of the relevant Employee Data;

(iv) where possible the retention period and if not possible the criteria used to determine that period;

(v) if applicable law so requires, the source of the Employee Data, where the Employee Data are not collected from the Employee,

(vi) if applicable law so requires, the existence of automated decision making, including profiling, as well as the significance and the envisaged consequences of such processing for the Employee; and

(vii) where personal data are transferred to a Non-Adequate Country or a country with an Adequacy Decision, the appropriate safeguards relating to the transfer.

In addition to the overview, ING Hungary shall in response to a request provide Employee with the following information:

(i) the existence of Employee's right to request rectification-, or erasure- of Employee Data, or restriction of processing of Employee Data and to object to such processing.

(ii) the right to lodge a complaint with the local data protection authority.

**12.2** If the Employee Data are incorrect or incomplete the Employee has the right to have his Personal Data rectified or completed (as appropriate).

**12.3 Right to erasure**

Every Employee has the right to erasure of Employee Data if:

(i) the Employee Data are no longer necessary in relation to the Business Purposes for which they were collected or otherwise processed;
(ii) the Employee withdraws consent and where there is no other Legitimate Business Purpose for the Processing;
(iii) the Employee has successfully objected to the Processing of Employee Data pursuant to Article 12.9;
(iv) the Employee Data have been unlawfully processed;
(v) the Employee Data have to be erased to comply with a legal obligation under applicable law;

**12.4 Right to restriction**

Every Employee has the right to obtain restriction of processing of his Employee Data if:

(i) the Employee has contested the accuracy of the Employee Data for a period enabling ING Hungary to verify this;
(ii) the Processing is unlawful;
(iii) ING Hungary no longer needs the Employee Data for the Business Purpose but the Employee requires the Employee Data for the establishment, exercise of defence of legal claims.
(iv) Employee has objected to the Processing of Employee Data pursuant to Article 12.9, pending ING Hungary's verification whether Legitimate Interests exist.

It is noted that the restricting of processing Employee Data can have consequences for the performance of ING as an employer.

**12.5** When Processing has been restricted, such Employee Data shall, with the exception of retention, only be Processed with the Employee's consent or for establishment, exercise or defence of legal claims or for the protection of rights of another natural or legal person. In such case, the authorization of the Local Data Protection Executive (BU DPE) is required. The Data Protection Executive is required to seek advice of the Local Data Protection Officer (BU DPO).

ING shall inform the Employee before the restriction of Processing is lifted.

**12.6 Notification obligation for ING Hungary**

ING Hungary shall communicate any rectification, erasure of Employee Data or restriction of Processing carried out in accordance with Articles 12.2, 12.3 and 12.4 to each recipient to whom the Employee Data have been disclosed, unless this proves impossible or involves disproportionate effort. ING Hungary shall inform the Employee about the recipients upon request.

**12.7 Right to data portability**

The Employee has the right to receive the Employee Data that the Employee has provided to ING Hungary in a structured, commonly used and machine- readable format and has the right to transmit his Employee Data to another Controller if:

(i) such processing is based on the Employee's consent pursuant to Article 6.2; or such processing is based on performance an agreement pursuant to Article 6.1; and such Processing is carried out by automated means. The Employee has the right to have Employee Data transferred directly from ING Hungary to another Controller, where technically feasible.

**12.8 Right to Object**

The Employee has the right to object to the Processing of his Data on the basis of compelling grounds related to his particular situation. If applicable law so requires, the

Employee has the right to object to the Processing of his Data based on Legitimate Interest, unless ING Hungary demonstrates compelling legitimate grounds for the Processing that constitute a Legitimate Interest for ING Hungary or for the establishment, exercise or defence of legal claims.

**12.9 Procedure**

The Employee should send his request to the contact person or contact point indicated in the relevant privacy statement to the address of dataprotection.hu@ing.com.

Prior to assessing the ING Hungary's requirement to fulfil the request of the Employee, ING Hungary may require the Employee to:

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

**12.10 Response period**

Within one month (30 calendar days) of ING Hungary receiving the request, the Data Protection Executive shall inform the Employee in writing either:

(i) of ING Hungary's position with regard to the request and any action ING Hungary has taken or will take in response, or
(ii) the reasons for the delay and the ultimate date on which he will be informed of ING Hungary's position, which date shall be no later than two months (60 calendar days) thereafter. If local law so requires, ING Hungary shall, in the event that ING does not take action on the Employee's request,
(i) inform the Employee without delay and at the latest within one month (30 calendar days) of receipt of the request of the reasons for not taking action, and
(ii) on the possibility of lodging a complaint with the data protection authority, where applicable, and
(iii) seeking a judicial remedy.

**12.11 Complaint**

An Employee may submit a complaint in accordance with Article 23 if:

(i) the response to the request is unsatisfactory to the Employee (e.g. the request is denied);
(ii) the Employee has not received a response as required by Article 12.10; or
(iii) the time period provided to the Employee in accordance with Article 12.10 is, in light of the relevant circumstances, unreasonably long and the Employee has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response.

**12.12 Denial of requests**

ING Hungary may deny a request of an Employee if:

(i) the request does not meet the requirements;
(ii) the request is not sufficiently specific;
(iii) the identity of the relevant Employee cannot be established by reasonable means;
(iv) the request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights;
(v) the request entails objection, restriction to processing or a deletion and the Processing of the Employee Data is required by law.

## 13 Security and Confidentiality Requirements

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

**13.1 Data security**

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

**13.2 Data protection by design and by default**

ING Hungary shall implement appropriate technical and organizational *(e.g.: regular review of business impact assessment of IT application which consist personal data, or PC protected by password...)* measures which are designed to implement data protection principles in an effective manner and to integrate necessary safeguards into the Processing, taking into account the state of the art and the cost of implementation as well as the nature, scope, context and purposes of the Processing and the risks of varying likelihood and severity for rights and freedoms of Employees posed by the Processing.

**13.3** ING Hungary shall implement appropriate technical and organizational *(e.g.: regular review of business impact assessment of IT application which consist personal data, or PC protected by password...)* measures for ensuring that, by default, only Employee Data which are necessary for each specific Legitimate Business Purpose are processed.

**13.4 Staff access**

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

**13.5 Confidentiality obligations**

Staff members who access Employee Data must meet their confidentiality obligations.

**13.6 Personal Data breach**

ING Hungary shall, in case of a Personal Data Breach, without undue delay and no later than 72 hours after having become aware of it notify the Personal Data Breach to the relevant supervisory authority, that is currently the Hungarian National Authority for Data Protection and Freedom of Information, unless such breach is unlikely to result in a risk to the rights and freedoms of the Employees. Where such notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

**13.7** The notification shall at least:

a) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Employees concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the relevant Data Protection Officer or other contact point where more information can be obtained;
c) describe the likely consequences of the Personal Data Breach;
d) describe the measures taken or proposed to be taken by ING Hungary to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

**13.8** ING Hungary shall document any Personal Data Breaches comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken.

**13.9** ING Hungary shall in case the Personal Data Breach which is likely to result in a high risk to the rights and freedoms of natural persons, communicate the Personal Data Breach to the Employee without undue delay containing at least the same information laid down in Article 13.7 (b), (c) and (d).

Exceptions to this obligation exist if:

a. ING Hungary has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the Personal Data Breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b. ING Hungary has taken subsequent measures which ensure that the high risk to the rights and freedoms of Employees referred to in this Article 13.9 is no longer likely to materialise;
c. it would involve disproportionate effort, in which case there shall instead be a public communication or similar measure whereby the Employees are informed in an equally effective manner.

**13.10 Data Protection Impact Assessment**

ING Hungary shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (Data Protection Impact Assessment (or DPIA), in the case of:

(i) Processing that is likely to result in a (high) risk to the rights and freedoms of Employees; and/or
(ii) Automated decision making, including profiling, as set out in Article 14; and/or
(iii) Processing of Sensitive Data as set out in Article 8; and or
(iv) Systematic monitoring of a publicly accessible area.

To achieve this, ING Hungary has developed a DPIA and implemented the DPIA in its existing Business Impact Analyses process (BIA) and Product Approval (Review) Process (PA(R)P)as well as in other relevant processes.

**13.11** Where necessary, ING Hungary shall carry out a review to assess if processing is performed in accordance with the DPIA at least when there is a change of risk represented by processing operations.

**13.12** ING Hungary shall consult the relevant authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures which can be

reasonably taken by ING Hungary to mitigate the risk.

## 14 Automated decision making

### 14.1 Automated decisions

Automated tools may be used to make decisions about Employees but decisions may not be based solely on the results provided by the automated tool, if such decision produces legal effects concerning the Employee or similarly significantly affects the Employee. 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 employment-at-will relationship, provided the underlying request leading to a decision by ING Hungary was made by the Employee (e.g., where automated tools are used to filter job applications);
iii. is based on consent of the Employee; or
iv. suitable measures are taken to safeguard the legitimate interests of the Employee,

e.g. the Employee has been provided with an opportunity to express his point of view.

**14.2** ING Hungary shall, in case the automated decision is based on Article 14.1 (ii, a) and (iii) in addition implementing suitable measures as set out in (iv) also implement a process to allow to contest the decision, in particular when the Employee requests human intervention.

**14.3** Automated decision making shall not be based on Sensitive Data referred to in Article 8, unless 8.2 (i) applies and suitable measures are taken to safeguard the legitimate interests of the Employee.

## 15 Transfer of Employee Data to Third Parties

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

### 15.1 Transfer of Employee Data

ING Hungary shall transfer Employee Data to a Third Party Controller to the extent necessary to serve the applicable legitimate purposes or legal obligation for which the Data are Processed.

### 15.2 Third Party Controller contracts

Third Party Controllers (other than government agencies or other public bodies) may Process Employee Data only if they have a written contract or a contract in a similar form (e.g. electronic) with the relevant Group Company of ING. In the contract, ING Hungary shall seek to contractually protect the data protection interests of its Employees. All such contracts shall be drafted in consultation with or in accordance with guidelines provided by the appropriate Data Protection Officer who will apprise the Data Protection Executive of the existence of such contract and the measures taken to protect the data protection interest

of its employees.

**Third Party Processor contracts**

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

(i) the Data Processor shall Process Employee Data only in accordance with ING Hungary's instructions and for the purposes authorized by ING Hungary; and
(ii) the Data Processor shall keep the Employee Data confidential; and
(iii) the Data Processor shall take appropriate technical, physical and organizational security measures to protect the Employee Data and, assist ING Hungary in ensuring compliance with this obligation; and
(iv) the Data Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to ING Hungary without prior written consent of ING Hungary; (the Third Party Processor warrants that the subcontractors will be compliant with the terms of the contract it has with ING Hungary); and
(v) ING Hungary 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 Hungary or any relevant government authority;
(vi) the Third Party Processor shall promptly inform ING Hungary 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 Hungary with all relevant information and assistance as requested by ING Hungary regarding the security breach.

**15.4** If applicable law so requires, contracts with a Third Party Processor who will handle Personal Data must in addition to the previous provisions include the following provisions:

(i) the Third Party Processor shall assist ING Hungary by appropriate technical and organizational measures to the extent this is possible for the fulfilment of ING Hungary's obligation to respond to requests to exercise the Employee rights laid down in Article 11, 12 and 14;
(ii) the Third Data Processor shall assist ING Hungary in ensuring compliance with the obligation to take appropriate technical, physical and organizational security measures to protect the Personal Data; and
(iii) the Third Party Processor shall assist ING Hungary in ensuring compliance with the obligation to promptly inform ING Hungary of any actual or suspected security breach involving Personal Data; and
(iv) the Third Data Processor shall assist ING Hungary in ensuring compliance with ING Hungary's obligation to inform Individuals in case of a security breach involving Personal Data; and
(v) the Third Data Processor shall assist ING Hungary in ensuring compliance with its obligation to perform a DPIA; and
(vi) the Third Party Data Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to ING Hungary without the prior written consent of ING Hungary and the Third Party Processor warrants that the subcontractors will be compliant with the terms of the contract it has with ING Hungary;
(vii) at the choice of ING Hungary, the Third Party Processor shall delete or return to ING all personal data, including copies thereof, after the end of the provision of the services relating to the processing unless applicable law requires storage of the Personal Data; and
(viii) the Third Party Processor shall make available to ING Hungary all information necessary to demonstrate compliance with the obligations laid down in Articles 15.3

and 15.4 and allow for and contribute to audits conducted or mandated by ING Hungary.

**15.5 Transfer of Data to a Non-Adequate Country**

This Article sets forth additional rules for the cross-border transfer of Employee 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. Employee 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 Employee, for managing the employment-at-will relationship or to take necessary steps at the request of the Employee prior to entering into a contract or an employment-at-will relationship, e.g., for processing job applications; or

(ii) a contract has been concluded between ING Hungary 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 Employee between ING Hungary and a Third Party (e.g. booking an airline ticket); or

(iv) the Third Party has been certified under the United States Privacy Shield Program or any other similar program that is recognized as providing an "adequate" level of data protection by the European Commission; 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 Hungary prior to the transfer taking place; or

(vi) an approved code of conduct or certification mechanism together with binding and enforceable commitments of the relevant Third Party to apply the appropriate safeguards, including Employee's rights;

(vii) the transfer is necessary to protect a vital interest of the Employee; or

(viii) the transfer is necessary in connection with legal proceedings, advice or rights; or

(ix) the transfer is necessary to satisfy a pressing need to protect an important public interest; or

(x) the transfer is required under any law or regulation to which the relevant Group Company is subject; or

(xi) the Data that will be transferred is included in a public register; or

(xii) the transfer is not repetitive, concerns only a limited number of individuals, is necessary for the purposes of compelling of legitimate interest pursued by ING which are not overridden by the interests or rights and freedoms of the Employees and ING has provided suitable safeguards, provided that ING Hungary has informed the relevant supervisory authority and the Employee on the transfer and the compelling interest pursued.

Items (viii), (ix) and (xii) above require:

(i) the prior approval of the appropriate Data Protection Executive who will seek advice from the appropriate Data Protection Officer; and

(ii) that suitable measures are taken to safeguard the legitimate interests of the Employee (which measures may include consultation with the relevant Data Protection Authority).

**15.6 Employee consent for transfer**

If none of the grounds listed in Article 15.5 exist, or if applicable local law so requires ING Hungary shall (also) seek consent from Employees for the transfer to a Third Party located in a Non- Adequate Country. When asking Employee consent, the Employee 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.

**15.8 Transfers between Non-Adequate Countries**

This Article sets forth additional rules for cross-border transfers of Employee Data that were collected in connection with the activities of an ING 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 15.5, these transfers are permitted if they are:

(i) necessary for compliance with a legal obligation to which ING Hungary is subject; or
(ii) necessary to serve the public interest; or
(iii) necessary to satisfy the legitimate purposes for which the Personal Data are Processed.

**16 ING Data Processor**

**16.1** ING Data Processor shall not engage another processor without prior specific or general written authorisation of ING Hungary. In case of general written authorisation, ING acting as a processor shall inform ING Hungary of any intended changes concerning the addition or replacement of other processors, giving ING Hungary the opportunity to object to such changes.

**16.2** ING Data Processor shall immediately inform ING Hungary if in its opinion an instruction as mentioned in Article 15.3 (i) infringes this Policy or any applicable law.

**16.3** ING Data Processor, engaging another processor, shall impose on that processor the obligations as set out Article 15.3 and 15.4 if applicable, in particular providing sufficient guarantees to implement appropriate technical and organizational measures.

**16.4** ING Data Processor, shall not process Employee Data except on instructions of ING Hungary, unless required by applicable law.

**16.5** ING Data Processor shall maintain a record of its processing activities in writing, including in electronic form, containing the following information:

(iv) the name and contact details and, where applicable, the processor(s) and of each controller on behalf of which the processor is acting and the Data Protection Officer;
(v) the categories of processing carried out on behalf of each controller;
(vi) where applicable, transfers of personal data to a third country, including the identification of that third country and, in the case of transfers referred to in Article 15.5, the documentation of suitable safeguards;
(vii) where possible, a general description of the technical and organisational security measures.

**16.6** ING Data Processor shall notify ING Hungary without undue delay after becoming aware of a

personal data breach in accordance with article 13.6.

## 17 Overriding Interests

**Policy statement**
There may be circumstances in which ING Hungary can decide to override some of the obligations of ING Hungary or rights of Employees 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.

### 17.1 Overriding Interests

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

(i) protect the legitimate business interests of ING Hungary 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 Hungary'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, breaches of the terms of employment, or non-compliance with the ING Orange Code or other ING policies or procedures; or
(iii) establish, exercise or defence of legal claims; or
(iv) otherwise protect or defend the rights or freedoms of ING, its Employees or other persons
(v) the safeguard important objectives of public interest.

### 17.2 Exceptions in the event of Overriding Interests

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

(i) Article 7.1 (the requirement to Process Employee Data for closely related purposes); and
(ii) Article 11. (information provided to Employees); and
(iii) Article 12. (rights of Employees); and
(iv) Articles 13.4 and 13.5 (Staff access limitations and confidentiality obligations); and
(v) Articles 15.2, 15.3, 15.4 and 15.5 (ii) (contracts with Third Parties).

### 17.3 Sensitive Data

The requirements of Articles 8.1 and 8.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 17.1 (i) (a), (c) and (e), (ii) and (iii).

### 17.4 Prior Consultation with Data Protection Officer

Setting aside obligations of ING Hungary or rights of Employees based on an Overriding Interest, requires the prior consultation with the Local Data Protection Officer (BU DPO).

### 17.5 Information to Employee

Upon request of an Employee, ING Hungary shall inform the Employee of the Overriding Interest for which obligations of ING Hungary or rights of the Employee have been set aside, unless the particular. Overriding Interest sets aside the requirements of Articles 11.1 or 12, in which case the request shall be denied.

# PART III SUPERVISION, COMPLIANCE AND LEGAL ISSUES

## 18 Supervision and compliance

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

### 18.2 Bank Data Protection Executive (Bank DPE)

The Bank Data Protection Executive shall supervise the implementation of and compliance with the Global Data Protection Policy in each Business Unit, which includes the responsibilities and activities as further described in Article 19 of the Global Data Protection Policy. The Bank Data Protection Executive role shall be fulfilled by a member of the Executive Board of ING Bank N.V.

### 18.3 Bank Data Protection Officer (Bank DPO)

The Bank Data Protection Officer is responsible for supervising general compliance with and for advice on the implementation and interpretation of the Global Data Protection Policy throughout ING, which includes the responsibilities and activities as further described in Article 19 of the Global Data Protection Policy. The Bank Data Protection Officer role shall be fulfilled by a Bank Tier 2 functionary.

### 18.4 BU Data Protection Executive (BU DPE)

Business management shall designate BU Data Protection Executives – this function is performed by the dedicated DPE role, reporting to CAO of ING Hungary - 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 19.

### 18.5 BU Data Protection Officer (BU DPO)

Business management shall designate BU Data Protection Officers – this function is reporting to Head of Legal of ING Hungary – 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 19. The BU Data Protection role shall be fulfilled by the appropriate second line of defense functionary.

### 18.6 Data Protection Officer with a statutory position

Data Protection Officer shall carry out his job responsibilities to the extent they do not conflict with his statutory position.

## 19 Responsibilities

| Who | Responsibilities |
|---|---|
| **Local 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.<br><br>The Data Protection Executive must:<br>• ensure that his Business Unit will process Personal Data in accordance with this Policy;<br>• implement the changes required within his Business Unit for achieving compliance;<br>• work together with and facilitate the appropriate DPO to create and maintain a framework for the development, implementation and updating of Local Data Protection Policies and procedures (including training and education);<br>• verify that a Data Repository, in line with the central template, for all identified processes whereby personal data is processed is completed and maintained and that is done through a pre-defined process by the Data Owner and Data Steward<br>• verify that the Data Repository is complete (includes all processes whereby personal data is processed) and can be delivered to data protection authorities upon request (in line with local requirements, if local law so requires)<br>• review the process description on accuracy and completeness at least once every year but also during major process or system changes<br>• ensure that the Staff working in his Business Unit follow the required training;<br>• duly fill out and sign off audit related questionnaires and Data Protection Impact Assessments<br>• 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;<br>• escalate to the Bank DPE, where needed;<br>• provide reports in close cooperation with the BU DPO, as appropriate in every month, to the Bank DPE and the Bank DPO 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.<br><br>The Bank Data Protection Executive must:<br>• liaise with the Bank DPO for all data protection risks, incidents, compliance issues or questions that have been escalated to the Bank DPE;<br>• provide a report on data protection risks and compliance issues in close conjunction with the Bank DPO, to the Bank NFRC and to Head of HR at a minimum once a year, but more frequently where needed. |

| | |
|---|---|
| **Local 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.<br><br>The appropriate Data Protection Officer must:<br>• have expert knowledge of data protection law and practices;<br>• 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;<br>• work together with the DPE to create and maintain a framework for the development, implementation and updating of local Employee data protection policies and procedures to support and monitor the implementation and embedding of the Policy within its Business Unit;<br>• advice on and support the correct interpretation of the Policy with communication and training of Staff;<br>• be able to operate independently from the business and (senior) management without conflict of interests with its other professional duties;<br>• have control and monitoring powers (the right to perform internal investigations and to access information);<br>• 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.<br><br>The Bank DPO must:<br>• coordinate, in conjunction with the appropriate DPO, official investigations or inquiries into the Processing of Data by a government authority;<br>• 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;<br>• provide a report on data protection risks and compliance issues In close conjunction with the Bank DPE to the Bank NFRC at 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.<br><br>Staff must:<br>• 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;<br>• 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. |

| | First Line of Defence | Second Line of Defence |
|---|---|---|
| GDPP compliance Overall | **Bank DPE (Data Protection Executive)**<br>Accountable for compliance with and implementation of the GDPP within ING globally. | **Bank DPO (Data Protection Officer)**<br>Responsible for interpretation of the policy, advice and supervising compliance with the GDPP within ING global. |
| | **Bank DPE Office**<br>On behalf of the Bank DPE performing the (coordinating) activities for compliance with and implementation of the GDPP. | **Bank DPO Office**<br>On behalf of the Bank DPO performing the activities re. policy, advice and supervising compliance GDPP. |
| GDPP Compliance Business Unit | **BU DPE Beáta Vodli / DPE role, reporting to CAO (beata.vodli@ing.com)**<br>Accountable for compliance with and implementation of the GDPP within the business unit. | **BU DPO Dóra Orosz / DPO role, reporting to Head of Legal (dora.orosz@ing.com)**<br>Responsible for providing advice to BU DPE and supervising compliance with the GDPP within the business unit. |
| | **BU DPE Office (for WB only countries: BU DPE)**<br>Performs operational activities relating to the compliance of GDPP commissioned by the BU DPE and the CDO. | |
| Personal Data Management** | **CDO (Chief Data Officer) (for WB only countries: BU DPE)**<br>Responsible for setting up the data mgt. strategy and data governance and accountable coordinating with the Data Owners within the BU. | |
| | **Data Owner**<br>Responsible for managing data during its lifecycle, including Data Access, Data Lineage and archiving/deletion. | |

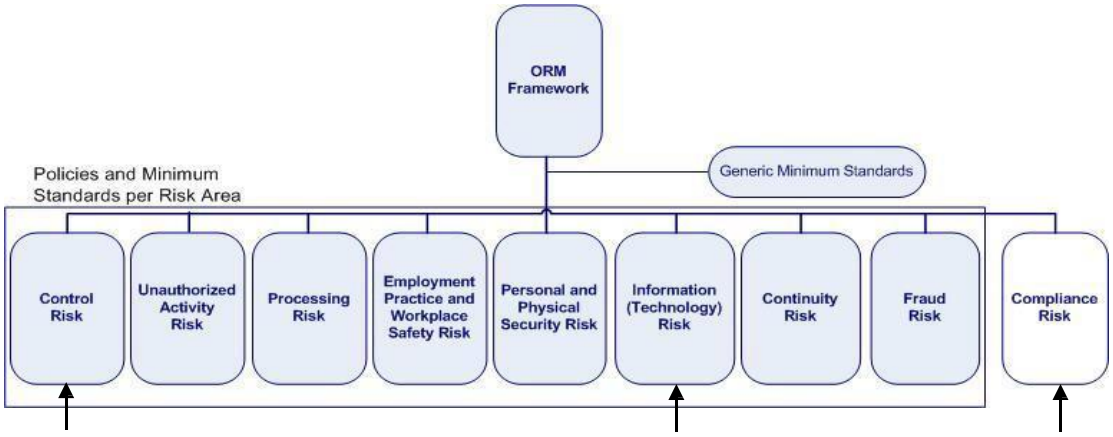
## RACI matrix

(A = accountable, R = responsible, C = consulted, I = informed)

| Data Protection activities | DPE | DPO | CDO, supported by the DPE Office* | Data Owner | Remarks |
|---|---|---|---|---|---|
| ***General*** | | | | | |
| Status overviews implementation and compliance | A | C | R | | DPE Office regularly prepares status overviews for Local Data Protection Board or NFRC |
| Monthly /ad hoc reports incidents & events | A | R | | | BU DPE, after alignment with the BU DPO, sends monthly report to Bank DPE |
| Support B.U.'s departments to be GDPP compliant | A | C | R | | DPE Office provides tools and support, DPO provides advice. |
| Personal Data management life-cycle | A | I | I | R | Life-cycle: collect, store, share, use, monitor, maintain, archive/destroy |
| ***Accountability (global standardised tools)*** | | | | | |
| Data Repository: fill out and maintain | A | C | R *coordination* | R *execution* | Data owner is responsible for implementation; CDO coordinates |
| DPIA (as triggered by BIA and as per 1/1/'18 uBIA or PARP) | A | C | R *coordination* | R *execution* | DPO must be present when conducting DPIA and gives advice on involving other NFR functions |
| Adhere to R.A. Data Protection | A | | R | | R.A. = Reference Architecture CDO is responsible for data mgt. strategy and governance |
| ***Local procedures*** | | | | | |
| Document Legitimate basis or explicit consent | A | C | | R | Various types of data processing must have identified legal basis |
| Local procedure re. data breach management | A | C | R | | |
| Local procedures re. individual rights | A | C | R | | This concerns individual rights for access, data portability, rectification, deletion |
| Privacy notes/statements | A | C | R | | DPE Office develop privacy notes together with DPO and Communication |
| Awareness & In-depth training | A | C | R | | DPO delivers the (local) content and DPE Office ensures that relevant staff are identified and trained |
| ***Controls*** | | | | | |
| Testing Control Framework | A | C | R | | DPE Office prepares yearly testing, 1 LoD performs testing of control framework |
| Control Review & Monitoring 2nd LoD | | R | | | The responsibility of the DPO is shared with the NFR functions that support the DPO in these activities |
| Sign off Control Framework | A/R | C | | | Sign off by DPE; quality assurance by DPO (and obtain assistance from other NFR functions if necessary) |

## 20 Policies and procedures

**20.1** ING shall develop and implement policies, minimum standards and procedures to uphold the compliance 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.




## 21 Local Data Protection Policy Training

### 21.1 Staff training

ING Hungary 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 by the BU DPO yearly basis. All of these trainings may be provided through the global ING Learning Center and on a regional or local basis. Completion ratio/individuals is monitored by Local HR Department.

## 22 Monitoring compliance Audits

### 22.1 Audits

Corporate Audit Services shall audit business processes and procedures that involve the Processing of Employee Data on 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 or Officer. The Bank Data Protection Executive or Officer may also request to have an audit as specified in this Article 22.1 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 and Officer 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.

### 22.2 Mitigation

ING Hungary shall ensure that adequate steps are taken to address breaches of this Policy identified during the monitoring or auditing of compliance pursuant to this Article 22.

## 23 Complaints procedure

### 23.1 Complaint to BU Data Protection Executive

Without prejudice to the Employees' rights and remedies available in their local jurisdictions as set out in Article 24.1, any Employee may file a complaint regarding compliance with this Policy or violations of his rights under this Policy or under applicable local law in accordance with the local complaints procedure set forth herein, in the relevant privacy policy or employment contract or as otherwise communicated to the Employee. The local complaints procedure shall require an investigation into the complaint and ensure the involvement of the appropriate BU Data Protection Executive and Officer. If the complaint involves the BU Data Protection Executive or Officer, the Employee may address his complaint to the Bank Data Protection Officer.

**23.2** 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.

### 23.3 Reply to Employee

Within one month (30 calendar days) of ING Hungary receiving a complaint, ING Hungary shall inform the Employee in writing either (i) of ING's position with regard to the complaint and any action ING Hungary has taken or will take in response or (ii) when he will be informed of ING Hungary's position, which date shall be no later than one month (30 calendar days) thereafter**.** The appropriate BU Data Protection Executive shall send a copy of the complaint and ING Hungary's written reply to the relevant BU Data Protection Officer and to the Bank Data Protection Officer, if notified pursuant to Article 23.2 (d).

### 23.4 Complaint to Bank Data Protection Officer

An Employee 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 Employee (e.g., the complaint is rejected); or
(ii) the Employee has not received a response as required by Article 23.3; or
(iii) the time period provided to the Employee pursuant to Article 23.3 is, in light of the relevant circumstances, unreasonably long and the Employee has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response; or
(iv) in the events listed in Article 12.12.

The procedure described in Articles 23.1 through 23.3 shall apply to complaints escalated to the Bank Data Protection Officer in accordance with Article 23.4. The Bank Data Protection Officer shall notify the Bank Data Protection Executive of any such escalated complaint, where relevant.

## 24 Legal issues

### 24.1 Local law and jurisdiction

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

### 24.2 Supplemental protection provided by this Policy

This Policy shall be governed by and interpreted in accordance with Hungarian law. This Policy shall apply only where it provides supplemental protection for Employee Data. Where applicable local law provides more protection than this Policy, local, Hungarian law shall apply. Where this Policy provides more protection than applicable local, Hungarian law or provides additional safeguards, rights or remedies for Employees, this Policy shall apply unless this leads to potential conflict with the applicable law in which case the Bank Data Protection Executive will decide within the spirit of this Policy upon advice of the Bank Data Protection Officer.

### 24.3 Available remedies, limitation of damages and burden of proof

In addition to any remedies Employees 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 Act of Information, the Hungarian Civil Code and Hungarian procedural law. However, ING Bank N.V. shall only be liable for direct damages suffered by an Employee resulting from a violation of this Policy. Provided an Employee 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 Employee due to a violation of the Policy are not attributable to the relevant Group Company.

### 24.4 Mutual assistance and redress

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

The Group Company employing the Employee is responsible for handling any communication with the Employee 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.

## 25 Sanctions for non-compliance

### 25.1 Non-compliance

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 or 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.

## 26 Conflicts between this Policy and applicable local law

### 26.1 Conflict of law when transferring Data

Where a legal requirement to transfer Employee 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, such as the Hungarian Data Protection Authority.

### 26.2 Conflict between this Policy and law

In all other cases, where there is a conflict between applicable local law and this 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 the spirit of this Policy and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

### 26.3 New conflicting legal requirements

The Local Data Protection Officer (BU DPO) and the Local Data Protection Executive (BU DPE) 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.

## 27 Changes to this Policy

**27.1** This Policy may be changed without Employee consent even though an amendment may relate to a benefit conferred on Employees; however, Employee must be informed of any change by announcing the modification.

**27.2** Any amendment shall enter into force after it has been approved by ING Hungary NFRC and has been published on the ING Intranet.

**27.3** Any request, complaint or claim of an Employee involving this Policy shall be judged against this Policy that is in force at the time the request, complaint or claim is made.

## 28 Legal remedies

### 28.1 Right to lodge a complaint with the supervisory authority

Employees and data subjects in general have the right to lodge a complaint with or supervisory authority, in particular in the Member State of residence, place of work or where the alleged infringement has been made. The national supervisory authority in Hungary is the Hungarian National Authority for Data Proection and Freedom of Information (address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c.; phone: +36 1 391 1400; e-mail: ugyfelszolgalat@naih.hu).

**Contact details**

**ING Bank Data Protection Officer c/o ING BankN.V.**
**Email address**: dpo.office@ing.nl

**ING Hungarian Branch Data Protection Officer**
1068 Budapest, Dózsa György út 84. B. ép.
E-mail: dataprotection.hu@ing.com
Phone number: +36 (1) 2358705

**ING Hungarian Branch Data Protection Executive**
1068 Budapest, Dózsa György út 84. B. ép.
E-mail: dataprotection.hu@ing.com
Phone number: +36 (1) 2555164

# APPENDIX 1 DEFINITIONS AND INTERPRETATIONS

**Definitions**

**Archive** shall mean a collection of Employee Data that are no longer necessary to achieve the purposes for which the Personal 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 set of Employee Data 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 18.2.

**Bank Data Protection Officer (Bank DPO)** shall mean the officer as referred to in Article 18.3.

**ING Hungary NFRC** shall mean the Bank Non-Financial Risk Committee.

**Biometric Data** shall mean personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an Individual, which allow or confirm the unique identification of that Individual, such as facial images or dactyloscopic data;

**Local/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 18.4, 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 19.

**Local/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 18.5, which function is further determined in Article 19.

**Business Purpose** shall mean a purpose for Processing Employee Data as specified in Article 6 or 7 or for Processing Sensitive Data as specified in Article 8 or 9.

**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.

**Country with an Adequacy Decision** shall mean a country outside the EEA where the European Commission has decided that the country, a territory or one or more specified sectors within that country, ensures an adequate level of protection.

**Consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**Data Controller** shall mean the party Processing the Employee Data that determines the means and the purposes of the Processing.

**Data Processor** shall mean the party Processing the Employee Data on behalf of the Data Controller 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 Employee.

**Data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

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

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

**Employee Data** or **Data** shall mean any information relating to an identified or identifiable Employee (and his Dependants).

**Employee** shall mean an employee, job applicant, former employee or trainee of ING, inclusive of present or former employees of ING Hungary acting in accordance with Section 24 of the Act CXXXII of 1997 on Hungarian Branch Offices and Commercial Representative Offices of Foreign-Registered Companies. This term also includes people working at ING Hungary as consultants, independent contractors, agents, volunteers or employees of Third Parties providing services to ING Hungary.

**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.

**GDPR** shall mean the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**).

**GDPP or Global Data Protection Policy for Employee Data** shall mean the ING Global Data Protection Policy for Employee Data.

**Genetic Data** shall mean Personal Data relating to the inherited or acquired genetic characteristics of an Individual which give unique information about the physiology or the health of that Individual and which result, in particular, from an analysis of a biological sample from the Individual in question.

**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.

**Guidance Documents** shall mean the documents with additional information on and an explanation of the adequate standards in this Policy made available for Staff via the ING intranet or on request.

**ING Hungary** shall mean ING N.V. Hungarian Branch acting on behalf of ING Bank N.V. in accordance with Section 24 of the Act CXXXII of 1997 on Hungarian Branch Offices and Commercial Representative Offices of Foreign-Registered Companies

**ING Data Processor** shall mean an ING entity that processes personal Data on behalf of any other ING entity (ies) and at its direction, that is not under the direct authority of such ING entity or branch.

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

**Legitimate Interest** shall mean the legitimate (business) interest of ING or a Third Party outweighing the interest or fundamental rights, or freedoms of Individual(s), which is relevant when Processing is based on a Legitimate Business Purpose other than performing a contract with the Individual, vital interest or a legal obligation.

**Non-Adequate Country** shall mean a country that under applicable local law (such as Article 25 of the EU Data Protection Regulation) 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 Employee Data was originally collected.

**Overriding Interest** shall mean the pressing interests set forth in Article 17.1 based on which the obligations of ING Hungary or rights of Employees set forth in Article 17.2 and 17.3 may, under specific circumstances, be overridden if this pressing interest outweighs the privacy interests of the Employee.

**Personal data** means any information relating to an identified or identifiable natural person ('**Data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.