# General Terms and Conditions
# ING Multi Mandate

7 March 2022

# General terms and conditions of the ING Multi Mandate

## 1. General provisions

### 1.1. Purpose of the General Conditions

The purpose of these General Terms and Conditions for ING Multi Mandate (hereafter the "General Conditions") is to describe the electronic services offered by ING under the name ING Multi Mandate and to determine the rights and duties of the Client, the User and ING with regard to the provision by ING of the ING Multi Mandate in favour of the Client, as well as the access to these services and their use.

### 1.2. Definitions

The following terminology is used and applies for the purpose of these General Conditions and the documents to which they refer, subject to another terminology in the latter. The terms may be used indiscriminately in the plural or in the singular.

1° Agreement: all the provisions which determine the rights and obligations of the Client and ING in connection with the use of ING Multi Mandate, as listed in point 3.1 below.

2° Client: the natural person or legal entity in the name and on behalf of whom the Agreement is entered into and who/which is the holder, joint holder or has a mandate of account(s) opened with ING ), where such accounts or contracts are, in accordance with this Agreement once concluded, accessible via the ING Multi Mandate and, where appropriate, can be managed by the latter.

3° ING: ING Belgium SA/nv, Bank/Lender with its registered office at avenue Marnix 24, 1000 Brussels, VAT BE 0403.200.393, Brussels RPM/RPR, acting in its own name and on its own behalf.

4° HCL Technologies Belgium BVBA, with its principal place of business in Lozenberg 22 Bus 3, B-1932, Zaventem, Belgium registered under company number 0542.547.130 is a third company acting as an IT service provider, is in charge of the technical development and run of the ING Multi Mandate platform.

5° itsme Service  the access means and signature services that Belgian Mobile ID provides under the name "Belgian Mobile Identity"/"Itsme", as regulated under the General terms and conditions of the Belgian Mobile Identity for ING BE services and Belgian Mobile Identity Agreement].

6° Belgian Mobile ID: Belgian Mobile Wallet nv/SA - Sint Goedeleplein 5, 1000 Brussels – VAT BE 0541 659 084 -RPR Brussels - BE64 0017 1071 6652. Belgian Mobile ID nv/SA is a third company acting as an Internet service providers, holder of the Belgian Mobile Identity mobile application, certifying authority and issuer of access and signature means which the Client calls on for secured electronic data transmission.

7° ING Call Centre: telephone service offered by  by ING Client Services for which you can find the telephone number on ING website (www.ing.be) or, the information broadcast through the service itself.

8° Parties: ING and the Client

9° User: the individual(s) designated and authorised by the Client, in accordance with the provisions of point 4 below, to use ING Multi Mandate according to the conditions laid down by this Agreement.

If the Client is a natural person, he/she is also a User. Depending on the permissions granted by the Client (if different from the User), the User will be entitled to use a sub-set of the features offered by ING Multi Mandate to the Client or have access to a restricted amount of data within the platform.

The account data available for a User on ING Multi Mandate is only related to ING accounts for which the Client is holder, joint holder or has a mandate.

10° The ING Client Services: the support services as described in point 2 of the relevant Appendix of the GeneralRegulations of ING

11° Business'Bank: all the electronic services offered by ING in point 2 of the relevant Appendix to the General Regulations of ING including the authorisation for the execution of IMM Payment Requests.

12° Technical Documentation on the use of the electronic services of ING: any user manual of the ING Client Services, /Business'Bank, NG Multi Mandate and/or Belgian Mobile Identity for ING BE services and other technical documentation relating to the use of

such services and concerning, in particular, communication and electronic signature procedures on the ING site or broadcasted by the service itself.

13° Order: any order carried out via the electronic services of ING in the name of and on behalf of the Client who requests the execution of a Payment Transaction, a Financial Instrument Transaction or any other banking, financial or insurance Transaction, and/or any request to conclude (subject to acceptance by ING or another company of the relevant ING Group and by mutual agreement) or acceptance of a banking, financial or insurance product or service contract signed in the name and on behalf of the Client.

14° IMM Payment Request: a payment order prepared by the User in ING Multi Mandate, which can subsequently be transferred to Business'Bank for authorisation by the Client..

15° Payment Transaction: an action consisting in transferring funds, irrespective of any underlying obligations between the payer and the payee of the Payment Order.

16° Payment Instruction: any instruction given through the authorisation of the IMM Payment Request, in the name and on behalf of the Client, requesting the execution of a Payment Transaction in Business'Bank.

17° IMM access and signature means: Itsme Service and the Belgium eID, used by the User for authentication purposes on the ING Multi Mandate platform.

18° Durable Medium: any instrument which enables the Client or the User to store the information addressed to him/her personally in a way accessible for future reference for a period of time adequate to the purposes of the information and which allows the unchanged reproduction of the information stored, such as DVD-ROMs, CD-ROMs, hard disks on personal computers on which electronic mail can be stored, etc.

19° Authentication : a procedure allowing ING to verify the identity of the User, or the validity of use of a specific payment instrument, including use of the User's personalised security credentials.

20° Strong Customer authentication of User : authentication based on the use of two or more elements categorised as knowledge (something only the user knows, such as a PIN), possession (something only the user possesses, such as a bank card) and inherence (something the user is, such a fingerprint) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

21° Personalised Security Credentials : personalised features provided to the User for authentication purposes.

## 2. Purpose of ING Multi Mandate

According to the possibilities offered by ING, the ING Multi Mandate services enables the User, via his/her computer system or tablet:

- To obtain information from ING accounts and
- To send IMM Payment Requests to be approved in Business'Bank.
  According to the possibilities offered by ING, the User can receive information and carry out IMM Payment Requests with regard to any account of which the Client is the holder, joint holder or has a mandate, open with ING. Similarly, the User can also receive information relating to all the accounts the Client is authorised to consult, provided he has been granted by the Client the corresponding permissions.
- To manage and structure account information (e.g balance or payment transaction data) by categorising, creating dossiers or uploading related documents.
- To create reports based on the payment transaction information available in ING Multi Mandate and other data entered or uploaded by the User.
- To create Users and grant them personalised permissions such as preparing IMM payments requests, managing dossiers or accessing specific ING accounts.

The electronic services of ING Multi Mandate are accessible in Dutch, French, and English.

## 3. Legal framework applicable to the ING Multi Mandate

### 3.1. Contract comprising the Agreement

**3.1.1.** List of documents comprising the Agreement

**3.1.1.1.** The Agreement includes the following documents:

- Where appropriate, the amendment notices referred to in point 3.1.2
- The Subscription Contract to the ING Multi Mandate service and, where appropriate, its appendices signed for and on behalf of the Client (hereafter the "ING Multi Mandate Subscription Contract")
- The Management Powers as granted to Users and displayed in the User Management Dashboard, in accordance with the process in 4.1 which are duly accepted by ING and by the Client or for and on behalf of the Client (hereafter " IMM Management Powers" )
- Special agreements relating to certain functions of ING Multi Mandate.
- These General Conditions of ING Multi Mandate and, where appropriate, the appendices thereto
- The prices applicable for ING Multi Mandate
- Technical Documentation on the use of ING Multi Mandate.

The order of priority of the documents making up the Agreement is governed according to the descending order laid down above, unless certain provisions of the Agreement expressly provide otherwise. The Agreement represents all of the agreements entered into between the parties and replaces all previous agreements (verbal or written) relating to the subject of the Agreement.

However, unless this Agreement expressly derogates therefrom, the contractual provisions relating to the electronic services of ING, and those relating to the banking products and services available via the ING Client Services/Home'Bank /Business'Bank/Smart Banking/Extrabranch Mobility/e-ID for Branch/Payconiq for ING BE and/or Belgian Mobile Identity for ING BE services and, in particular, to the Transactions available via these services, apply in full to ING Multi Mandate services, whether they are provisions agreed or to be agreed between the Client and ING, notably those of the General Regulations of ING, or the Special Regulations for Payment Transactions and the payment services covered by such Special Regulations[1],

Furthermore the documents referred to in this point 3.1.1.2, , are available from any ING branch

**3.1.1.2.** The Client and the User can obtain all necessary information about ING Multi Mandate services by calling the ING Client Services services, browsing the ING website (www.ing.be) or, the information broadcast through the service itself.

**3.1.1.3.** The Client and the User acknowledge that, prior to conclusion of the ING Multi Mandate Subscription Agreement , they received from ING, on a Durable Medium all the documents, electronic or otherwise, constituting the Agreement, as well as all the information they might reasonably expect, in particular with regard to the characteristics and functionalities of the electronic services of ING to check the latter's compliance with their requirements. As a result, by concluding the ING Multi Mandate Agreement, they absolve ING from any liability in this respect and acknowledge that the ING Multi Mandate services meet their needs.

**3.1.2.** Changes to the contractual framework on ING's initiative.

The Parties agree that this Agreement (in particular, although without the following list being restrictive, the prices and the ceiling for Orders), as well as the contents of, and the means of access, using and signing for the electronic services of ING, may be amended unilaterally by ING at any time, subject however to respect of the procedure described below.
ING must inform the Client individually of any amendment it wishes to make to this Agreement by means of dated change notices sent in writing or on a Durable medium, electronic or otherwise, provided to the Client and to which he/she has access, in particular but not limited to, messages enclosed with the account statements of the Client or the User, e-mail sent to the mailbox of the Client or the User and/ or messages displayed via the ING Multi Mandate, without prejudice to mandatory or public order legal provisions.
Such notification must take place at least fifteen calendar days before the amendment in question is implemented. The Client can refuse to accept such amendment and, in that case, exercise, before the effective date - as specified in the aforementioned notice – of the announced amendment and in accordance with point 18.2. of these General Conditions, his/her right to terminate the Agreement with immediate effect, without charges or compensation and without justification. In the absence of such termination, the Client is deemed to

[1] In particular the rules relating to execution deadlines and cut-off times applicable to the Payment Transactions covered by these Special Regulations.

have accepted this amendment.

**3.2.** Application of the Agreement

The application of the provisions of the Agreement does not prejudice any order public order or mandatory, legal or statutory provisions. If a provision or part of a provision of the Agreement is rendered void, the validity, scope and binding nature of the remaining provisions of this Agreement shall not be affected.

**3.3.** Applicable legislation and competent courts

The conclusion, application, interpretation and execution of the Agreement are governed exclusively by Belgian law.

Subject to imperative or public order legal or statutory provisions, stipulating the rules for allocating competence, and in particular in case of dispute with Consumers, the Bank, whether it is the plaintiff or defendant, is authorised to take or have taken any dispute relating to this Agreement and/or the services associated with it and/or the transactions referred to by this Agreement, in particular the rules on the execution deadlines and cut-off times applicable to Payment Transactions covered by these Special Regulations before the courts and tribunals of Brussels or before those in the district where its registered office is established with which the business relationship with the Client is conducted directly or indirectly through the intermediary of a subsidiary or a branch.

## 4. Subscription to the electronic services of ING and users of such services

**4.1.** Subscribing to ING Multi Mandate

**4.1.1.** The service is provided to ING Clients who wish to use these services for professional purposes and have a Business'bank subcription.

**4.1.2.** The ING Multi Mandate Agreement is concluded with a Client by entering into the ING Multi Mandate Subscription Contract by simply subscribing the Agreement in an ING Branch or through the subscription form provided for in Business'Bank.

Such subscription implies acceptance of the ING Multi Mandate Subscription Contract and, likewise, the confirmation of the ING Client ServicesBusiness'Bank and Belgian Mobile Identity for ING BE Agreement.

Once the ING Client ING Multi Mandate Agreement has been concluded, where appropriate by means of the aforementioned subscription, only the Client is authorised to activate and deactivate the ING Multi Mandate services. The Users can access and use the ING Multi Mandate services in accordance with the provisions of 4.1.4.

**4.1.3.** If the Client and the User wish to activate the ING Multi Mandate services, they are bound to comply with the terms, conditions or procedures set out in the Technical Documentation on use of the service or any other form at ING's discretion.

Once accepted by ING, activation of the ING Multi Mandate is equivalent to the commencement of the subscription to the ING Multi Mandate services.

**4.1.4.** Subject to the possibilities offered by ING, the Client accepts that on concluding the ING Multi Mandate Agreement, all the accounts with ING of which he/she is the holder, joint holder or has a mandate on shall be accessible via ING Multi Mandate for all of the Transactions he/she is authorised to carry out in relation to the management of such accounts.

The Client has the possibility to restrict access to account information in ING Multi Mandate either by defining the "visibility" of the accounts in the interface for all Users, including him, or by limiting access to only certain Users.

By completing the electronic forms which ING provides to the Client, the latter can grant mandates to other Users for all or a selection of the following services offered through IMM

- consultation of selected accounts' data
- the management of dossiers
- the upload of documents
- the preparation of IMM Payment Requests
- the transfer of IMM Payment Request to Business'Bank

[Section on cancellation of IMM Management Power:

1) change
2) suspend/deactivate (temporary nature
3) remove

Procedure urgency // card stop

The powers and any specific limits to such powers, expressed in terms of maximum authorised transaction amount, number of signatures required

and/or types of Transactions authorised, indicated on the "Powers of Attorney" documents (electronic or otherwise) for the account(s) of which the Client is the holder, joint holder or has a mandate on, as well as any changes made subsequently to such powers and limits, apply to IMM Payment Request submitted via ING Multi Mandate . These changes will be reflected in ING Multi Mandate within 1 working day.

**4.2.** Users of ING Multi Mandate.

**4.2.1.** The Client accepts that him/herself, if they are Users, and each User designated by him/her in accordance with point 4.1 of the General Conditions may consult ING Multi Mandate.

Subject to the same reserves, the Client, if he/she is a User, and the Users provided they are duly mandated in accordance with point 4.1 of the General Conditions, may also, within the limits of their powers and with their electronic signature enter and/or send IMM Payment Requests for and on behalf of the Client requesting the authorisation of a Payment Transaction.

**4.2.2.** To revoke the powers granted to Users, the Client must use the revocation procedure laid down in the contracts and regulations applicable between the Client and ING.

To block the means of access to ING Multi Mandate, the Client must follow the procedures for blocking means of access described in the provisions of point 6.4 of these General Conditions. However, Users may only block their own means of access for the ING Multi Mandate.

If the Client or his/her/its Users subsequently wish to reverse the block, he/she/it is obliged to set-up a new valid itsme or eID account with the corresponding supplier.

If the Client asks ING to revoke a User's powers, by deactivating the User's profile in ING Multi Mandate, ING shall endeavour to block the User's access to the ING Multi Mandate as soon as possible on receipt of the request. It shall not, however, incur any liability in this regard until the lapse of the period of time specified for ING to actually take a revocation into account given in the contracts and regulations applicable between the Client and ING..

**4.2.3.** The Client undertakes to inform all Users of their obligations in the context of the Agreement and, in particular, of the conditions for accessing, using for the electronic services.

The Client is liable for his/her Users complying with such obligations and conditions and for all consequences arising from any shortcoming by his/her Users.

## 5. Access and use

**5.1.** ING Multi Mandate Access Means

**5.1.1.** According to the options offered by ING the User can choose between

- His/her Belgian e-ID
- His/her itsme Serviceitsme

The Client ING ID and the username additionally required by the User to access and use the ING Multi Mandate services, are provided to the User personally by the Client (if different from the Client).

The Belgian e-ID means of access Users need to access and use ING Multi Mandate, including those needed to append their electronic signature, are provided personally to the User by the Belgian public authorities, in particular by the municipality of their main residence and the Institutions and Population General Directorate of the Belgian Federal Public Service.

The itsme services are provided by Belgian Mobility ID and used via ING Multi Mandate in accordance with the Agreement and the Belgian Mobile Identity agreement.

**5.1.2.** The User is liable for direct and indirect loss associated with the use, by the User or a third party, of the means of access, in accordance with the provisions of these General Conditions.

The liability of the Client must be examined with regard to the provisions of these General Regulations (in particular Article 8) and, where appropriate, the Belgian Mobile Identity Agreement.

**5.2.** Accessing ING Multi Mandate

**5.2.1.** To access ING Multi Mandate, the User uses his or her validly registered Belgian Identity card in accordance with point 5.7 of these General Regulations, or his/her smartphone for the itsme service.itsme

**5.2.2.** The ING Multi Mandate services are accessible to the User only after he/she/it has been

authenticated by the access means of his/her Belgian Identity Card or itsme (Belgian Mobile Identity) itsmeitsmeitsme

When using the itsme account activated for the Belgian Mobile Identity for ING BE services on his/her smartphone in order to access ING Multi Mandate services, and notwithstanding the provisions of points 5 and 8 of these General Regulations, the Client accepts that the entry of the User's personal PIN code into the duly working Belgian Mobile Identity app is valid and sufficient proof of that person's identity as the User of the ING Multi Mandate services who is the holder of the Belgian Mobile Identity for ING BE account and smartphone in question, provided the means of access are validated by the computer systems of Belgian Mobile ID and ING and in particular is recognised by these electronic systems as originating from the User, and provided the use of his/her Belgian Mobile Identity account is valid and has not expired or been revoked.

**5.2.3.** Once the User has accessed the ING Multi Mandate services and has been identified in accordance with point 5.2.2., the User may use the ING Multi Mandate services a described in 4.1.4 via the aforementioned services by entering data on the keyboard of his/her IT system.

## 6. Obligations of the Client and the User with regard to security

**6.1.** The Client is liable for the proper use of the electronic services of ING by all Users, in accordance with the provisions for access and use of stipulated in the Agreement and, or itsme Services in the Belgian Mobile Identity Agreement.

**6.2.** The Client and the Users must take all reasonable precautionary measures to ensure the security of access to their operating stations and their (Mobile) IT systems from which the ING Multi Mandate services can be accessed.

In particular, the Client and Users undertake only to use the ING Multi Mandate services on a (mobile) IT system equipped with a recent firewall, and anti-malware (for example, spyware) and anti-virus software which are permanently enabled and updated regularly.

**6.3.** The User is obliged to save and use his/her ING Multi Mandate access means in accordance with the provisions of this Agreement, or the Belgian Mobile Identity Agreement and which come into effect upon the issuing or use of said services, within the limits of use agreed on with ING.

The User undertakes to respect the cautionary advice in order to avoid any risk of misuse of its means of access the electronic services of ING Multi Mandate. Such cautionary advice includes:

- That annexed to these Terms and Conditions as well as, , those mentioned in the Belgian Mobile Identity Agreement, and are an integral part of it
- That regularly provided to the User by ING or, for Itsme Service, by Belgian Mobile ID notably via their website, as well as
- That which, for the e-ID, is provided to the User by the Belgian public authorities, in particular the Institutions and Population General Directorate of the Belgian Federal Public Service.

The User shall take all reasonable precautions to ensure that his/her ING Multi Mandate services means of access are secure. The means of access chosen by the User him/herself (such as a password, PIN and/or any other authentication code) are strictly personal and confidential to the User, without prejudice to the right of the User to use the services of a payment initiation or account information service provider who is duly authorised to carry out activity. The User alone is liable for their use and the preservation of their confidentiality. The User undertakes not to communicate his/her ING Multi Mandate access means to a third party (including, but not limited to, a spouse, a family member and/or a colleague) under any circumstances and/or not to allow a third party to obtain them, without prejudice to the right of the User to use the services of a payment initiation or account information service provider who is duly authorised to carry out activity. Similarly, the User shall not communicate to a third party any confidential information on the security procedures applied.

**6.4.** The Client and/or User is/are obliged to immediately notify ING and, for the itsme Service, to Belgian Mobility ID, as soon as he/she becomes aware of:

1. the loss, theft, misappropriation or any unauthorised use of his/her/their ING Multi Mandate means of access."Loss" or "theft", within the meaning of these General Terms and Conditions, refers to any involuntary dispossession of the ING Multi Mandate means of access ( Belgian Identity Card or Belgian Mobile Identity). "Misappropriation" or any "unauthorised use" means any illegitimate or

unauthorised use of the ING Multi Mandate services means of access;

2. any technical incident or any other failure associated with the use of his/her/their access means; and/or capable of jeopardising the security of these services.

An itsme account can be blocked via the itsme app itself, on the website of itsme or on the ING website. The instructions and Technical Documentation which the User is required to follow carefully for this purpose are available on each of those sites.

For Belgian Identity Card, the User undertakes to follow the procedures for blocking the aforementioned means of access and signature stipulated by the Belgian public authorities (in particular with **DOC STOP** (free n° 00800 2123 2123 or, in countries where 00800 is not accessible, +32 2 518 2123), as quickly as possible whenever the security of such means of access could be jeopardised, whether for the reasons mentioned in point 6.4. or for any other reason.

In the event of theft, misappropriation or unauthorised use of the ING Multi Mandate means of access, the Client or User must also file a statement or report with the relevant local Belgian or foreign competent authorities as soon as possible. If requested by ING, the Client or User must send proof, as well as references, of the statement or report made. The Client or User undertakes to send ING any information required for the investigation.

**6.5** The Client acknowledges that the introduction of an IMM Payment Request in the IMM Service does not automatically lead to the execution of a Payment Transactions by ING. After transfer of the IMM Payment Request to Business'Bank, it is the responsibility of the Client/User in Business Bank to check and subsequently authorise the corresponding Payment Orders in Business Bank.

**6.6.** Clients or Users who subscribe to ING Multi Mandate are required to read regularly, and at least once a month, the notices provided by ING via ING Multi Mandate services, in particular for the application of point 3.1.2.

Without prejudice to the Business'Bank terms and conditions relating to the deadline for disputing Payment Transactions, any complaint relating to a Transaction carried out through ING Business'Bank, after signing a Payment Order corresponding to a transferred IMM Payment Request, must be notified as soon as the Client or the User becomes aware of it, and whatever the case within two months from the provision, or in the absence of provision, from the supply of the information relating to such Transaction, whether by means of an account statement, a bank statement or any other document on a durable medium, whether electronic or otherwise, received following the receipt, acceptance or execution of such Transactions. After such deadline, the Transaction shall be deemed to be correct and exact and can no longer be disputed.

## 7. ING's obligations as regards security

**7.1.** Without prejudice to the obligations of the Client and the User stipulated in Article 6, ING guarantees the secrecy of the access means chosen by the User him/herself (such as a password, PIN and/or any other confidential authentication code known only to the User).

**7.2.** At the very least ING shall ensure that the User receives an electronic (where appropriate, by e-mail), confirmation of receipt of his/her IMM Payment Request, via the ING Multi Mandate services. ING, shall also ensure that the User or Client receives an electronic (where appropriate, by e-mail) confirmation that the IMM Payment Request has or has not been accepted and, if accepted, when the Payment Order has been executed.

Without prejudice to the above, to enable the Client in particular to monitor his/her expenditure to a reasonable extent and, where appropriate, to provide notification in accordance with point 6.4. or 6.6, shall provide or make available to the Client, regularly and at least once a month following the receipt, acceptance of execution of Orders relating to Transactions transmitted in connection with the ING Client Business'Bank services through the channel of the User's access or signature means, information relating to such Orders, whether it be through an account statement, a bank statement or any other document on a durable medium, electronic or otherwise.

**7.4.** As soon as ING receives the notification referred to in points 6.4 or 6.6 of these General Conditions in accordance with the blocking procedures mentioned in said points, ING shall prevent any further use of the ING Multi Mandate access means.

**7.5**. At the Client's or the User's request, ING shall provide proof that the Client or the User has duly made such notification within eighteen months from

the said notification referred to in point 6.4.

## 8. Liabilities of the Parties

### 8.1. Liability of ING

**8.1.1.** Unless otherwise provided for in this Agreement (in particular those of Article 8.2.), ING, in accordance with its general duty of care as laid down, in particular, in ING's General Regulations, accepts liability for any gross negligence or a deliberate transgression of duty (with the exception of minor offences) committed while carrying out its professional activities, either by it, by its employees or sub-contractors approved by it.

ING exercises the utmost care in executing the Agreement properly. However, unless expressly provided otherwise in the Agreement (in particular in Article 8.2), the obligations arising from the latter which are incumbent on ING are only best effort obligations. In particular for ING, are considered to be result obligations the obligations stipulated in points 6.4., 7.1., 7.4 and 12.1.1. of these General Terms and Conditions.

Unless stipulated otherwise in this Agreement (in particular in Article 8.2), under no circumstances is ING liable for indirect loss, notably, although not limited to, the loss of data, expected earnings, profit, opportunity, clients or savings, the cost of procuring an equivalent service or product or damage to reputation.

8.1.2**.** The liability and/or guarantee of ING services available via the ING Multi Mandate are governed exclusively by the agreements and other contractual conditions entered into with the Client, in particular, but not limited as far as ING is concerned to, the General Regulations of ING, the Special Regulations for Payment Transactions of ING.
These Transactions are proposed as such via the ING Multi Mandate, without any guarantee or additional liability on the part of ING as a result of providing them via such services, except for gross negligence or a deliberate transgression of duty on the part of ING or unless otherwise provided for in this Agreement.

**8.1.3.** ING is liable for any gross negligence or intentional misconduct on its part (with the exception of slight negligence) in the design of the ING Multi Mandate provided it designed them, or in the choice of the ING Multi Mandate platform where they were developed by third parties. Such liability only covers direct loss which may be caused to the Client or the User's computer, telecommunications, broadcasting or any other equipment, software or configurations as a result of accessing, or using the ING Multi Mandate provided by ING, or the impossibility to use them.

**8.1.4.** Except in the event of serious or deliberate error on its part, and unless this Agreement provides otherwise, ING cannot be held liable for direct and indirect loss caused to the Client, a User or a third party which might result from the use of the ING Multi Mandate by the Client or a User in a way which does not comply with the conditions for access and use of these services which are stipulated in this Agreement or, for the Belgian Mobile Identity for ING BE services supplied via the Belgian Mobile Identity services, in the Belgian Mobile Identity Agreement, or in the case of the e-ID services supplied by the public authorities.

**8.1.5.** Prior to receipt of the notification referred to in point 6.4 of these General Conditions, unless ING has committed a gross serious or deliberate transgression of duty, the Client is liable for any direct or indirect loss which might result for him/her, for ING or for third parties, from any use, whether improper or otherwise, of the ING Multi Mandate by third parties using access and signature means of a User. This provision does not prejudice point 8.2. of these General Conditions.

Furthermore, the liability of both Belgian Mobile ID and the Client in the event of theft, loss, misappropriation or unauthorised use of the itsme services means of access and signing is governed by the provisions of the Belgian Mobile Identity Agreement. As ING is not the issuer of these means of access and signing, it cannot incur liability with regard to the Belgian Mobile Identity for ING BE services for the consequences resulting from the theft, loss, misappropriation or unauthorised use of such access and signing means, except in the event of gross negligence or intentional misconduct on its part.

**8.1.6.** Except in the event of serious or deliberate transgression of duty on its part or that of its sub-contractors approved by it, ING refuses any liability for direct or indirect loss caused to the Client or to a User for the purpose of ING Multi Mandate by devices, networks, terminals or equipment or configurations not approved by ING, resulting in particular from defects, breakdowns or failures in electronic communications networks or from the poor functioning or poor configuration of devices, networks or computer, telecommunications or

broadcasting equipment not approved by ING that were made available or chosen by Belgian Mobile ID for purposes itsme services.

For this point 8, devices, networks or means of equipment or configurations not approved by ING, mean those acquired from third parties or from the Client or the User him/herself, free or at a cost, by the Client or by the User to access and use the electronic services of ING and:

- Which are not supplied by ING or its sub-contractors and
- Which are not specifically designated by ING as approved by it, or
- Which have not been validly created by Belgian Mobile ID for the supply of Belgian Mobile Identity services.

However, are also considered as not approved by ING, those made available: devices, networks, terminals, equipment or configurations supplied by Belgian Mobile ID for the supply of Belgian Mobile Identity services in connection with the Belgian Mobile Identity for ING BE services (in particular, the network connected to the Belgian Mobile Identity services and the access and signing means for Belgian Mobile Identity for ING BE services).

Subject to the same reserves as mentioned above, ING refuses any liability for direct or indirect loss caused to the Client or to a User in connection with the ING Multi Mandate arising from notably:

- Acts or omissions which can in any way be attributed to third parties, including the Client or the User, which have not been approved by ING, and in particular:
    - any addition or alteration to the ING Multi Mandate or "jailbreaking" of the Mobile IT System carried out by the Client, the User or by third parties, and not approved by ING
    - Any upload of external account data by the Client; e.g. old Home'Bank Offline Database extracts.
    - Any upload of documents by the Client or the User.

- Legal or statutory obligations stipulated by domestic or community legislations; or
- Events beyond ING's control, such as action by authorities, war, riot, strike, default by its own suppliers, damage resulting from fire or natural causes (such as flooding, storm and lightning) or any event of force majeure.

Consequently, in the context of electronic services, ING cannot guarantee and provides no guarantee concerning:

- Access, availability as well as the access and response times for ING's electronic services via devices, networks, terminals or equipment not approved by ING and
    - The technical security and reliability of communications via devices, networks, terminals or equipment not approved by ING, in particular in the context of ING Multi Mandate, protection against viruses and other malware (e.g. spyware, etc.) despite the protective measures established by ING; and
    - Protection and confidentiality of communications via devices, networks or equipment not approved by ING.

Subject to the same reserve, ING is not liable, in particular, in the context of the e-ID services:

- For non-execution or incorrect execution, attributable to the Belgian public authorities in the context of their activity of providing services associated with Belgian electronic identity cards (in particular for the provision of the latter and the PINs linked to them or as a mere conduit) of IMM Payment Requests submitted using the means of access and signing of e-ID services, via devices, networks or equipment approved by the Belgian public authorities, whether they are placed under their control or not, and
- For IMM Payment Requests carried out without the User's authorisation arising from an action or omission attributable to the Belgian public authorities or any error or any irregularity in managing the Client's account attributable to the Belgian public authorities in the context of their activity of providing Belgian electronic identity card services (in particular the provision of the card and the PINs linked to it or as a mere conduit therefor).

Subject to the same reserve, ING is not liable, in particular in the context of the Belgian Mobile Identity for ING BE services:

- For non-execution or incorrect execution, attributable to Belgian Mobile ID in the context of its activity of providing Belgian Mobile Identity services (in particular, for the provision of the access and signing means for the Belgian Mobile Identity for ING BE services or as

a mere conduit therefor) for IMM Payment Requests submitted using the aforementioned access and signing means via devices, networks or equipment approved by Belgian Mobile ID, whether they are placed under their control or not,

- For IMM Payment Requests carried out without the User's authorisation arising from an action or omission attributable to Belgian Mobile ID or any error or any irregularity in managing the Client's account attributable to Belgian Mobile ID in the context of its activity of providing Belgian Mobile Identity services (in particular for the provision of the access and signing means for Belgian Mobile Identity for ING BE services or as a mere conduit therefor),

- For non-execution or incorrect execution, attributable to the Belgian public authorities in the context of their activity of providing services associated with Belgian electronic identity cards (in particular for the provision of the latter and the PINs linked to them or as a mere conduit therefor) of IMM Payment Requests submitted using the e-ID services means of access and signing, via devices, networks or equipment approved by the Belgian public authorities, whether they are placed under their control or not, and

- For IMM Payment Requests carried out without the User's authorisation arising from an action or omission attributable to the Belgian public authorities or any error or any irregularity in managing the Client's account attributable to the Belgian public authorities in the context of their activity of providing electronic identity card services (in particular for the provision of the cards and of the PINs linked to them, or as a mere conduit therefor).

In these cases, Belgian Mobile ID for the first two cases, and the Belgian public authorities for the last two are liable:

- In the case of Belgian Mobile ID, in accordance with the conditions laid down in the Belgian Mobile Identity Agreement and taking into account its capacity as a mere conduit and issuer of the means of access and signing for the Belgian Mobile Identity for ING BE services, or

- In the case of the Belgian public authorities, in accordance with the conditions laid down in the legal and regulatory provisions and taking into accounts their capacity as a mere conduit and issuer of the means of access and signing of the e-ID services.

**8.1.7.** The Client and, where appropriate, each of the Users, are responsible for ensuring that their computer, telephone or other equipment, software and configurations are compatible for accessing and using the ING Multi Mandate services.

**8.1.8.** ING ensures the User that ING Multi Mandate is free of any known virus

**8.2.** Liability of the Client

**8.2.1.** Until the notification stipulated in point 6.4 of these General Conditions, the Client shall bear all the losses resulting from the loss, theft, misappropriation or any unauthorised use of the IMM access means (including the Belgian Mobile Identity account) of the Client or the User, except for serious or deliberate error on the part of ING.

## 10. Maintenance of the ING Multi Mandate services

**10.1.** With regard to any technical, operational or functional incident or problem associated with ING Multi Mandate services (to the exclusion of the itsme services, in particular the network linked to these itsme services and its corresponding access and signing means), the User can call the ING Help Desk via the ING Client Services services.

The Help Desk can be accessed by calling ING Client Services services during business hours in accordance with the Technical Documentation on the use of electronic services of ING. The Help Desk can provide assistance in French, Dutch, English

Users scan also contact the Help Desk by e-mail (info@ing.be). When notifying the problem and subsequently, the User must provide all useful and necessary information likely to resolve the said problem.

**10.2.** In any event, corrective maintenance of the ING Multi Mandate services, associated mainly with correcting any faults or errors in the service, can only be carried out with ING's assistance. Users may not correct or modify the ING Multi Mandate services themselves.

**10.3.** ING shall endeavour to carry out maintenance tasks within a reasonable time. However, in carrying out its maintenance tasks, it is only bound by a best

effort obligation.

**10.4.** ING is not obliged to provide ongoing maintenance and, as a result, does not guarantee that the ING Multi Mandate services shall be adapted to the specific requirements and wishes of the Client or the User, in particular concerning adaptations to its computer or (mobile) telecommunications systems. The Client and the User are responsible for verifying that these systems match the specifications laid down in the Technical Documentation on use of the service.

## 11. Protection of privacy

**11.1.** General provisions

**11.1.1.** ING respects the privacy of any individual, including that of the User, that of the Client where appropriate, and that of any other individual concerned, in accordance with the legislation in force. The data processor for personal data on private individuals concerned is ING (e-mail: info@ing.be).

The personal data communicated or made available to ING is processed by the latter in accordance with the EU Regulation 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 (hereinafter referred to as the "EU Regulation") and with the Belgian legislation on the protection of privacy and its implementing decrees.

**11.1.2.** Besides the other data processed (from public or non-public external sources, where applicable) by ING mentioned in Article 6 (Protection of privacy) of ING's General Regulations, the personal data relating to individuals communicated to ING in the context of the conclusion or execution of the ING Multi Mandate Agreement (including the uploaded Homebank Offline data), particularly in the context of the use of the ING Multi Mandate services, is processed by ING for the purposes of centralising customer management,
the consultation of accounts and payments, generation of reporting,
marketing (i.e. surveys and statistics) of banking, financial (i.e. leasing) and/or insurance services ,unless the individual concerned objects,
a global overview of the client,
.
It is also processed by ING for the other (secondary, where applicable) processing purposes mentioned in Article 6 (Protection of privacy) of ING's General Regulations.

**11.1.3.** Such data is not intended to be communicated to third parties other than:
- those designated by the individual concerned;
- the independent agents of ING, acting for and on its behalf;
- the companies whose intervention is necessary or useful in order to carry out ING's purposes mentioned in point 11.1.2., in particular:
  - for the provision of the ING Multi Mandate interface and transmission of the IMM Payment Requests to ING Business'Bank, HCL Technologies
  - for the hosting of the ING Multi Mandate platform, Microsoft Inc. via the Azure Cloud platform
  - for marketing activities: Selligent SA, Bisnode Belgium SA and Social Seeder SPRL (all established in Belgium) as well as, where applicable, external call centres (in particular, in connection with surveys);
  - for means of access provided by Belgian Mobile Identity payment Transactions, Belgian Mobile ID;
  - competent authorities,

in accordance with the following provisions.

The data of the Client and of the other people concerned may also be transferred to non-EU countries which may or may not provide an adequate level of personal data protection (for example, SWIFT SCRL/bvba archives US payment data, which is subject to US legislation, data which is communicated to the companies of the ING Group which are not established in another Member State of the European Union, etc.). The data of the Client and of the other private individuals concerned is exchanged between – existing or future – companies of the banking, financial and insurance group ING whether established or not in a Member State of the European Union.

The ING Group in the EU is a group of companies with activities in banking, insurance, leasing, asset management and/or an activity following on from those activities. Any private individual may ask ING for an updated list of the updated list of the ING Group companies established in Belgium, or in another Member State of the European Union or in another country and which participate in the exchange of data about the Client and the other people concerned. These companies have given an undertaking to guarantee a high level of protection of any data of a personal nature exchanged and are bound, as far as such data is concerned, by an

undertaking of discretion.

Such exchange of data is intended to allow the companies of the ING Group established in another Member State of the European Union participating in it to centralise customer management, obtain a global overview of Clients, to undertake surveys, statistics or marketing campaigns (except e-mail advertising, except with the consent of the person concerned, and unless the individual concerned objects), to offer and/or provide the services mentioned above, and to control the regularity of Transactions (including the prevention of irregularities). These companies may also pursue the same compatible secondary purposes as those mentioned for ING in Article 6.1.4. of ING's General Regulations.

Consequently, the private individual data required for the companies of the ING Group established or not in another Member State of the European Union to respect the legal or statutory provisions (including those stemming from a competent supervisory authority circular) relating to the duty of vigilance towards clients, to the prevention of the use of the financial system for the purposes of money laundering and the funding of terrorism, and the prevention of the funding of the proliferation of weapons of massive destruction, is also exchanged between such companies for these purposes. ING Bank NV (Bijlmerplein 888, 1102 MG, Amsterdam Zuidoost, The Netherlands), acting as the joint processing manager, manages the exchange of data within the companies of the ING Group which participate in the exchange of data relating to private individuals for the aforementioned purposes.

The judicial (police, prosecution, examining magistrate, courts and tribunals) or administrative authorities, including the banking and financial supervisory bodies (National Bank of Belgium/FSMA), whether Belgian or international, e.g. American may, in certain cases stipulated by law or local regulations (in particular with a view to preventing terrorism) demand from ING Belgium or a company to which data may have been transferred in accordance with the above provisions, communication of all or part of the personal data of private individuals (e.g. the data relating to Payment Transactions). Certain data is, for instance, communicated to the central point of contact held by the National Bank of Belgium and to the credit services of the National Bank of Belgium, in accordance with Article 5 of the General Regulations of ING.

However, ING only transfers data to a country that is not a Member State of the European Union not providing an appropriate level of protection in the cases laid down by the legislation applicable to protection of privacy, for example by specifying adapted contractual provisions as laid down in Article 46.2 of the EU Regulation. A copy of the conventions may be obtained by contacting the data protection officer of ING mentioned in point 11.1.6.

**11.1.4.** Any private individual may access the data relating to him/her, processed by ING or another company of the ING Group established or not in a Member State of the European Union or insurers external to the ING Group, and, where appropriate, request the rectification of erroneous data. They may also request the deletion of such data or limitation on the processing as well as object to the processing thereof. Finally, they have the right to data portability.

The relevant private individual may, at any time, object, on request and free of charge:
- to the processing of the data relating to him/her for the purposes of direct marketing;
- object to his/her data being exchanged between companies of the ING Group established in a Member State of the European Union for the purposes of direct marketing;

- for reasons relating to their own specific situation, to the processing of their personal data for statistical purposes,

without ING or the other ING Group company concerned being able to challenge the exercise of such right.

**11.1.5.** Personal data relating to the individual concerned is processed by ING and the other ING Group companies established or not in an EU Member State with the utmost confidentiality. However, as electronic communications networks, particularly the Internet, do not offer total security, the respect of privacy can only be guaranteed if the personal data is sent via the communication channels expressly indicated by ING as being protected.

**11.1.6.** For any further information about the processing of personal data by ING as well as, in particular, about the automated individual decision-making by ING (including profiling), the data recipients, the lawfulness of the processing, the processing of sensitive data, the protection of premises by surveillance cameras, the requirement

to provide personal data, the terms and conditions for exercising the rights afforded to any person concerned and the retention of data by ING, the person concerned may consult:

- Article 6 (Protection of privacy) of ING's General Regulations, and
- "ING's Declaration of Confidentiality for the Protection of Privacy" appended to the aforementioned Regulations.

For any question regarding the processing of personal data by ING, any person concerned may contact ING via ING's usual communication channels:

- by logging into the ING Home'Bank/Business'Bank or ING Smart Banking services and, where applicable, by sending a message via these services with the reference "Privacy",
- by contacting their ING branch or their contact person at ING,
- by telephoning the following number: +32 2 464 60 02,
- by sending an e-mail to info@ing.be with the reference "Privacy".

In the event of a complaint concerning the processing of their personal data by ING, the person concerned may contact ING's Complaint Management department by sending their request with the reference "Privacy", together with a copy of their identity card or passport:
- by post to the following address:
ING Belgium, Complaint Management, Cours Saint Michel 60, B-1040 Brussels
- by e-mail to the following address: plaintes@ing.be

If they do not obtain satisfaction or require further information about protection of privacy, the person concerned may contact the data protection officer (also referred to as "Data Protection Officer" or "DPO") of ING:

- by post at the following address: ING Privacy Office, Cours Saint Michel 60, 1040 Brussels.
- by e-mail at the following address: ing-be-PrivacyOffice@ing.com.

Any person concerned also has the right to complain to the competent supervisory authority regarding protection of privacy, namely, for Belgium, the Data Protection Authority (Rue de la Presse, 35, 1000 Brussels; www.dataprotectionauthority.be).

**11.2.** ING Multi Mandate services

**11.2.1. Cookies**

"Cookies" are used in some places of the Business'Bank/ING Multi Mandate services to provide Users with a better service. The applicable cookie policy can be found on https://www.ing.be/en/retail/my-news/online-security/cookie-use.

**11.2.2.** Environment variables

When the User uses the ING Multi Mandate services, the following personal data, called "environment variables", is sent to ING Multi Mandate Service and recorded via the User's navigation software:

- The User's TCP/IP address (identification number of the User's computer system on the Internet network),
- The makes and versions of his/her navigation software and operating system,
- The language used by the User,
- The preferred means of access,
- All information about the ING Multi Mandate services pages visited by the User and those of other websites through which the User accessed the ING Multi Mandate Online services.
- The date and time when the User logged to ING Multi Mandate for the last time

Such data is processed by ING with a view to taking into account the specific configuration of the User's IT System and to being able to send him/her the web pages requested in a suitable format. It is also processed to compile statistics for the ING Multi Mandate services and to ensure that the contents of such services are improved.

**11.2.3** The Client acknowledges having the possibility to upload data into the ING Multi Mandate Service and being solely responsible for the imported data, including accuracy.

**11.2.4** The data archived in the ING Multi Mandate Service are retained for the duration of the ING Multi Mandate agreement. Upon termination of the ING Multi Mandate Agreement, Client will have the possibility extract the data for a period of 30 calendar days.

## 12. Proof of Transactions

The provisions of this point 12 do not prejudice the Client's right to provide proof to the contrary through any legal channel, nor the system of liability stipulated in points 5 and 8 of these General Conditions.

Furthermore, they do not prejudice the mandatory or public order legal provisions which may stipulate special rules on the authentication, recording and/or booking of Transactions.

**12.1.** Proof of Transactions in general

**12.1.1.** Without prejudice to point 6.6 of these General Conditions, in the event of a dispute concerning a Transaction resulting from an IMM Payment Request carried out by a User using his/her ING Multi Mandate services access means, ING undertakes to provide proof that the IMM Payment Request was authenticated and recorded and booked correctly and was not affected by a technical incident or other failure.

For all Transactions resulting from an IMM Payment Request given via the ING Multi Mandate services, such proof shall be provided by producing an excerpt of the log tape or recordings on a data medium of all the Transactions recorded, established by ING's electronic systems or any sub-contractors called on by ING (including itsme services).

The Parties recognise that the aforementioned log file and recordings on a data or computerised medium have evidential value. The contents of such log file and recordings may be copied onto paper, microfiche or microfilm, magnetic or optical disc, or onto any other data medium. For the Parties such reproduction shall have the same binding value as an original document. The Client may request that a reproduction invoked as proof by ING be certified as a true copy by the latter.

**12.1.2.** ING keeps an internal list of the Transactions resulting from an Order submitted using the means of access and signing of ING's electronic services for a period of at least five years from when the Transactions are executed, without prejudice to other legal or statutory provisions with regard to the provision of supporting documents.

**12.1.3.** Without prejudice to imperative legal, statutory or public order provisions, any notification by ING in the context of the Agreement may, in particular, be validly carried out by letter or e-mail, by a notice included in account statements and, in the context of the Home'Bank/Business'Bank or Smart Banking services, by electronic message.

**12.2.** ING Multi Mandate

**12.2.1.**IMM Payment Request executed using ING Multi Mandate services, the Client acknowledges that simple validation of the request, without recourse at such time to other signature means, by a person duly authenticated beforehand as a User, in accordance with point 5.2 of these General Conditions, via his/her means of access when accessing ING Multi Mandate services, constitutes the electronic signature of this User, provided such means of access are validated by ING's electronic systems, and more specifically, they are recognised by such systems as originating from the User, and that said means of access are valid and have not been revoked or, where appropriate, have not expired.

The Payment Order following from the IMM Payment Request remains to be authorised using the Business'Bank Signature means in accordance with the Business'Bank Terms and Conditions.

**12.2.2.** For all IMM Payment Request carried out in the context of ING Multi Mandate services, the Client accepts that the electronic signature as defined in points 12.2.1 of these General Conditions, of each User – validated by the ING electronic systems and recognised as originating from said User – satisfies the conditions of imputability and content integrity attached to a signature within the meaning of Article 1322, paragraph 2, of the Civil Code and that an electronic document with such electronic signature has the same evidential value as a written document with the written signature of the User, and binds the Client as such. The Client accepts that, provided the User's electronic signature is validated by ING's electronic systems and recognised as originating from the User, all IMM Payment Request validated with the electronic signature of the User and received by ING via ING Multi Mandate and transferred to Business'Bank services constitute valid and sufficient proof of his/her agreement on the existence and content of the IMM Payment Request concerned, as well as the consistency between the content of the ING Multi Mandate as transmitted by the User and the content of the Payment Request, visualised as an Order in Business'Bank.

## 13. Lists of charges

**13.1.** The charges for using the ING Multi Mandate services are indicated in the lists of charges applied to the main banking operations published by ING and are available, in particular, from any ING branch and via the ING Client Services, Home'Bank/Business'Bank/Smart Banking/ING Multi Mandate services. They are also provided to the Client prior to the conclusion of the ING Multi Mandate Agreement. Such lists of charges are only valid as from the date they are published.

They do not constitute a binding offer on ING, unless they are communicated to the Client in a ING Multi Mandate services subscription form or refer to the contractual documents mentioned in point 4.1.2. in these General Terms and Conditions.

These lists of charges may stipulate, for the use of ING's electronic services, the payment of annual fees, which can be demanded (at the request of the Client or the User) upon the activation of the service and, then, on each anniversary date of the Agreement.

**13.2.** The Client authorises ING to automatically debit the reference account designated in the ING Multi Mandate Agreement with all the fees applicable under the charging policy in effect, for the use of the service. If the Reference Account is closed, the Client is required to inform ING Belgium of another Reference Account. Otherwise, another reference account from which the aforementioned fees are to be debited automatically shall be automatically designated by ING, as it deems appropriate. In the latter case, if ING is not informed through a statement incorporated with the account statements within a deadline of fifteen calendar days after the provision of the message included with the account statements to indicate another reference account to ING Belgium. If ING is not informed of such other account within the aforementioned deadline, the aforementioned charges shall be automatically debited from the reference account designated by ING as a matter of course after the end of such deadline, without prejudice to the Client's right to subsequently request a change of reference account.

Furthermore, in the case of Transactions carried out in connection with the use of ING Multi Mandate Service, the Client authorises the automatic debiting, unless ING expresses makes another method of payment available at the choice of the Client, of any charges applicable to such Transactions from the account over which the Transaction is carried out.

In both of the above cases, the Client undertakes to fund his/her sufficiently or, if a credit line or overdraft facility is given on this account, to provide for sufficient disposable sums to be deducted, for the debit date.

**13.3.** The costs of telephone communications (including those associated with calling the Help Desk of ING's call centre) and, where appropriate, the costs associated with the acquisition, installation and operation of computer, telephone or other equipment and software, as well as access to and use the electronic communications networks to access and use the ING Multi Mandate services are at the Client's or User's expense.

## 14. User licence for the ING Multi Mandate software and database

Without prejudice to the provision of the ING Multi Mandate services to the User as provided in the Agreement, either ING or the person who has conferred the rights of use on ING reserves all of the property rights and all of the intellectual property rights (including the rights of use) for both ING Multi Mandate Software and Database, as well as all its components, in particular, but not limited to, texts, illustrations and other elements appearing in the Software and/or in the Database.

### 14.1. ING Multi Mandate Software

**14.1.1.** For the duration of this Agreement, the User is granted a strictly personal, non-exclusive and non-transferable licence to use the ING Multi Mandate Software in its directly readable object code version in the User's (Mobile) IT System. However, no property rights or intellectual rights are transferred to the User. This license provides only the right to access the ING Multi Mandate Software with all the (Mobile) computer systems to which the User has access and to operate it in accordance with the purpose determined in the Agreement.

**14.1.2.** Any permanent or temporary reproduction of the ING Multi Mandate Software, in part or in whole, by any means and in any form, any translation, adaptation, arrangement, any other transformation and any correction of the ING Multi Mandate Software, as well as reproduction of the computer program resulting therefrom, are subject to prior written authorisation from ING.
However, the User is entitled to carry out Transactions to load, display, transfer the ING Multi Mandate Banking Software required to enable the User to use the Software in accordance with its

purpose. Copying the code and translating the form of the code for the ING Multi Mandate Software are subject to prior written permission from ING, even if such acts are essential to obtain the information required for interoperability between the ING Multi Mandate Software and third-party Software, as the said information is accessible to the User from ING. Without prejudice to the above, the source codes for the ING Multi Mandate Software shall not be communicated to the User.

**14.1.3.** The provisions of this point 14.1 apply not only to the ING Multi Mandate Software in its entirety, but also to all of its components.

**14.2.** ING Multi Mandate Database

**14.2.1.** For the duration of this Agreement, the User has a strictly personal non-exclusive, non-transferable license for use of the ING Multi Mandate database.

However, no property rights or intellectual rights are transferred to the User. This license provides only the right to use the ING Multi Mandate Software for all the computers to which the User has access and to operate it in accordance with the purpose determined in the Agreement.

**14.2.2.** Any extraction and/or reuse of the entirety or a qualitatively or quantitatively substantial portion of the content of the ING Multi Mandate database is strictly prohibited.
Similarly, repeated and systematic extractions and/or reuse of insubstantial portions of the content of the ING Multi Mandate database are not authorised when they are contrary to normal use of the ING Multi Mandate database or cause unjustified damage to the legitimate interests of ING.

**14.3.** Trademarks, names and logos
The registered or non-registered brands, names and logos contained in the ING Multi Mandate Software and database are the exclusive property of ING or the other companies of the ING Group and may not be reproduced, without the express prior agreement of ING.

## 15. Hypertext links for the ING Multi Mandate

Except in the event of gross negligence or intentional misconduct on their part, ING and the other companies of the ING Group do not provide any guarantee or accept any liability for the hypertext links created from the ING Multi Mandate to third-party websites, nor with regard to the contents of such websites. Such websites are accessed solely at the risk of the User, as he/she is well aware that such websites may be subject to other conditions of use, other provisions with regard to the protection of privacy and/or in a general manner other rules than those which apply to the ING Multi Mandate. ING and the other companies of the ING Group are not liable for these websites' compliance with the legislation and regulations in force.

## 16. User messages

Any message from the User containing data, questions, comments, ideas and suggestions, sent to ING by e-mail (to the following address: info@ing.be) or by any other means, shall not be considered as confidential, subject to ING's duty of discretion in the context of its banking activity and of respect of the User's rights as recognised by law, in particular those deriving from the law on the protection of privacy. Subject to respect of the same reservations, within five years from when it is sent and without any compensation whatsoever, any message may be reused, copied in whole or in part, amended and transmitted by ING, in any form whatsoever, by any means and for any purposes in the European Union.

## 17. Availability of the ING Multi Mandate services

**17.1.** Insofar as it is able, and in accordance with the limits laid down in this Agreement, ING shall endeavour to make the ING Multi Mandate services accessible 24 hours a day, 7 days a week.

**17.2.** However, ING does not undertake to provide continuous, uninterrupted and secured access to ING Multi Mandate services.

Moreover, ING reserves the right, without being obliged to compensate the Client, to interrupt access to all or some of the ING Multi Mandate Solution services temporarily at any time and, in emergencies, without prior notice, to any User in order to carry out maintenance operations, to make improvements or changes or to resolve any technical incidents or failures in ING's electronic (including the telecommunications systems).

ING shall inform the Client by any means it deems appropriate of such suspension and the reasons therefore, if possible before the suspension, otherwise immediately thereafter, unless providing

such information is prevented by security reasons adequately explained or prohibited under applicable legislation.

ING shall endeavour to limit the duration of such interruptions and to inform Users of their duration through any means ING deems appropriate.

Moreover, each Party shall take all necessary measures, within its capabilities and means, to stop any technical incident or failure as soon as possible.

Without prejudice to its right to additional compensation for any loss, ING also reserves the right to block at any time access to all or part of ING Multi Mandate services to any User for objectively motivated reasons relating to the security of the services and/or the access and signature means for these services, or in the case of a presumed unauthorised or fraudulent use of the services and/or access and signature means for these services.

When ING exercises its right to blockthe User of the service, it shall inform the Client or the User by letter, through an account statement or any other way it deems appropriate according to the circumstances and, if possible before the access is blocked, otherwise immediately after, unless the provision of such information is contradicted by objectively motivated security reasons or if it is prohibited pursuant to another applicable legislation. ING shall restore access to the blocked service(s) when the reasons for the block cease to apply.

## 18. Duration of the ING Multi Mandate Agreement

### - De-activation of the services and Termination of the Agreement

**18.1.** The ING Multi Mandate Service Agreement is signed by the Parties in accordance with point 4.1.2. of these General Terms and Conditions and is concluded for an indefinite period until its termination.

Once activated in accordance with point 4.1.3. of these General Terms and Conditions, the ING Multi Mandate shall remain activated for an indefinite period until deactivation, i.e. closing of the access to such services which is deemed as closing of the subscription to such services.

**18.2.** The Client may terminate and or deactivate the ING Multi Mandate Agreement and/or deactivate the ING Multi Mandate , for him/herself and/or his/her Users, at any time, free of charge and without providing any justification.

The Client must send written notification of termination of the agreement to ING, which shall endeavour to take it into account as soon as it is received, without accepting any liability in this regard, however, before the end of the second bank working day following receipt of the written termination notice signed by the Client.

If the Client wishes such termination or deactivation to have immediate effect with regard to use of ING's electronic services, he/she must unsubscribe from the service in an ING Branch or via ING Call Centre. .

However, the Agreement may also be terminated subject to simultaneous closure of the relevant accounts and termination of the contracts with ING that may be accessed via ING's electronic services and which, where appropriate, may be managed via these services. If the client deactivates the ING Business'Bank services for the Client him/herself, ING Multi Mandate services will be automatically terminated accordingly .

If the Client or his/her Users subsequently wish to reactivate the ING Multi Mandate, he/she is obliged to subcribe again to the service via Business'Bank or an ING Branch

**18.3.** ING may terminate the ING Multi Mandate Agreement and/or deactivate the ING Multi Mandate at any time, for the Client him/herself and/or his/her Users, at any time and without providing any justification, subject to two months' notice by post or on any other durable medium. Termination by ING ends this Agreement with regard not only to its relationship with the Client.

Likewise, without prejudice to any applicable public order or imperative legal provisions, ING, at any time and without notice, terminate ING Multi Mandate Agreement or suspend execution of all or part and/or deactivate, for him/herself and or his/her Users, the ING Multi Mandate if the Client and his/her Users seriously fail to honour their commitments with respect to ING or is in a state of insolvency, goes bankrupt, enters into an arrangement with creditors, is put into receivership or is subject to similar proceedings.

ING can also, at any time and without notice, terminate the Agreement and/or deactivate for the Client him/herself and or his/her Users the ING Multi Mandate services in the event of an end to the

contractual relationship relating to their respective products and services available via the ING Multi Mandate services.
In this case, the ING Multi Mandate Agreement may only be entirely terminated by ING subject to simultaneous closure of the accounts and termination of the contracts with ING and other ING Group companies or insurance companies external to the ING Group that may be accessed via the ING Client Services/Home'Bank/Business'Bank/Smart Banking/Extrabranch Mobility/e-ID for Branch/Payconiq for ING BE and/or Belgian Mobile Identity for ING BE services and which, where appropriate, may be managed via these services.

Furthermore, the above provisions do not prejudice the procedure for blocking the ING Multi Mandate means of access and signature in accordance with point 7.4 of the General Terms and Conditions, and interrupting access to ING Multi Mandate services in accordance with point 17.2. of the General Terms and Conditions, and the legal provisions requiring the Bank to take special measures in the event of exceptional circumstances.

**Appendix: Cautionary advice for accessing and using the ING Multi Mandate services**

**General security advice:**

- Always check your bank account statements and breakdowns. Notify your bank immediately of any anomalies.
- When using ING Multi Mandate, make sure you use the latest firewall, spyware and antivirus software, have them permanently switched on, and update them regularly.
- Make sure not to jailbreak your Mobile IT system (device with Android of Google or iPad, iPhone, iPod Touch of Apple).

**Specific advice concerning the secret code for the ING Client Services services, the Home'Bank/Business'Bank Online / Extrabranch Mobility password (and/or smart (bank or electronic identity) card PIN) or the PIN code for Home'Bank/Business'Bank Online / Extrabranch Mobility Services or the Smart Banking/ Payconiq for ING BE/Belgian Mobile Identity for ING BE services:**

- Also memorise your PIN code for itsme services as soon as it has been generated, and do not write it down anywhere.

No-one has the right to ask you for your PIN code for ING Client Services, your password (and/or smart card PIN) for Home'Bank/ Business'Bank/ Extrabranch Mobility/e-ID for Branch services and/or Smart Banking/Payconiq for ING BE/Belgian Mobile Identity for ING BE PIN. This includes your bank (except for requests for encryption via the electronic services of ING), the police and insurance departments, in any form whatsoever.

Therefore, never give your secret code/password (and/or PIN) via e-mail, over the Internet (where requested by e-mail) or telephone, for example, without being certain of sending them to your bank via the electronic services of ING. However, this does not affect your right to choose the services of a payment initiation or account information service provider who is duly authorised for this activity.

Be on your guard and inform your bank immediately if you notice unusual circumstances.

- Do not write your PIN code for ING Client Services and/or your password for Home'Bank/ Business'Bank/ Extrabranch Mobility/e-ID for Branch services (and/or smart card PIN) and/or your Smart Banking/ Payconiq for ING BE/Belgian Mobile Identity for ING BE PIN anywhere, even in code form, for example, by disguising it (them) as a fake phone number.
- Use the ING Multi Mandate services in places where discretion is guaranteed. Always enter your PIN away from prying eyes.
- Always ensure that you cannot be observed unwittingly, for example, by using your hand to shield the telephone, iPad, iPhone or iPod, or computer keyboard. Do not allow anyone to distract you and, if this is the case, never enter your PIN. If you become aware of unusual circumstances, inform your bank immediately in accordance with Article 6.4 of the General Terms and Conditions.
- If you have good reason to believe that your PIN code is (are) no longer confidential, change it (them) immediately. If you are not able to change your PIN, alert your bank immediately in accordance with Article 6.4 of the General Terms and Conditions.

## Appendix 1: ING Belgium Declaration of Confidentiality for the Protection of Privacy

### Contents

## 1. About this Privacy Statement

This Privacy Statement of ING Belgium nv/sa (hereafter referred to as ING) aims to explain in a simple and transparent way what personal data we gather about you and how we process it. It applies to the following people:

- All past, present and prospective ING customers;
- Anyone involved in any transaction with ING, whether it's in your personal capacity or as a representative of a legal entity (for example, a company manager, agent, legal representative, operational staff, etc.);
- Non-ING customers such as payees or the contact persons of corporate clients.

**Personal data** refers to any information that tells us something about you or that we can link to you. This includes your name, address, date of birth, account number, IP address or information about payments you've made from your bank account.
By **processing** we mean everything we can do with this data such as collection, recording, organisation, storage, adaptation, use, disclosure, transfer or erasure.

You share personal data with us when you:
- Become a customer;
- Register with our (online) services;
- Complete an (online) form;
- Sign a contract;
- Use our products and services; or
- Contact us through one of our channels.

We also use data that is legally available from public sources such as the Central Individual Credit Register of the National Bank of Belgium (NBB), commercial registers, media, or is legitimately provided by other companies within the ING Group or third parties such as Thomson Reuters that provides World-Check risk detection services.

## 2. The types of data we process about you

The personal data we process includes:
- **Identification data**, such as your name, surname, date and place of birth, ID number, e-mail address and the IP address of your computer or mobile device.
- **Transaction data,** such as your bank account number, deposits, withdrawals and transfers related to your account.
- **Financial data,** such as invoices, credit notes, payslips, payment behaviour, the value of your property or other assets, your credit history, your credit capacity, financial products you have with ING, whether you are registered with a credit register of the BNB, payment arrears and information on your income.
- **Socio-demographic data**, such as whether you are married and have children.
- **Your online behaviour and preferences data,** such as the IP address of your mobile device or computer and the pages you visit on ING websites and apps.
- **Data about your interests and needs** that you share with us, for example when you contact our ING branches, call centre or fill in an online survey.
- **Audio-visual data,** such as surveillance videos at ING branches or recordings of phone calls to our customer service centres.

### Sensitive data

We do not record sensitive data relating to your health, ethnicity, philosophical, political opinion, religion or beliefs, trade union membership unless it is strictly necessary. When we do it is limited to specific circumstances, for example if you instruct us to pay a membership fee to a political party.

### Children´s data

We know how important it is for our customers that we protect their children´s data. We only collect data about children if they have an ING product or if you provide us with information about children in relation to a product you buy.
In relation to the offer of information society services (for example, ING Smart Banking) directly to a child under the age of 13, we would do so only if and to the extent that we have received authorization from the person holding parental responsibility.
Furthermore, we do not do direct marketing to children that are below the age of 12.

## 3. What we do with your personal data

We only use your personal data under one of the following legal grounds:
- To conclude and carry out our contract with you;
- To comply with our legal obligations;
- For our legitimate business interests. This data processing may be necessary to maintain good commercial relations with all our customers and other concerned parties.

We may also process your data to prevent and combat fraud and to maintain the security of your transactions and of the operations made by ING;
- When we have your consent. In this case, you may withdraw your consent at any time.

We may process your data for the following purposes:
- **Administration.** For example, when you open an ING account we are legally obliged to collect personal data that verifies your identity (such as a copy of your ID card or passport) and to assess whether we can accept you as a customer. We also need to know your postal, e-mail address or phone number to contact you.
- **Product and service delivery.** We use information about you to assess whether you are eligible for certain products and services such as a current or savings account, mortgage, loan or investment.
- **Managing customer relationships.** We may ask you for feedback about our products and services and share this with certain members of our staff to improve our offering. We might also use notes from conversations we have with you online, by telephone or in person to customise products and services for you.
- **Credit risk and behaviour analysis.** For example, to assess your ability to repay a loan we apply specific statistical risk models based on your personal data.
- **Personalised marketing based on profiling**. With your consent, we may send you letters, e-mails, or text messages offering you a product or service based on your personal profile (payment data or other similar details) or show you such an offer when you log in to our website or mobile apps. You may at any time unsubscribe from such personalised offers.
- **Providing you with the best-suited products and services.** When you visit our website, call our customer service centre or visit a branch we gather information about you. We analyse this information to identify your potential needs and assess the suitability of products or services. For example, we may suggest investment opportunities suited to your profile. We analyse your payment behaviour, such as large amounts entering or leaving your account. We assess your needs in relation to key moments when a specific financial product or service may be relevant for you, such as starting your first job or buying a home. We assess your interests based on simulations you participate in on our website.
- **Improving and developing products and services**: Analysing how you use our products and services helps us understand more about you and shows us where we can improve. For instance,
    - We use transactional data to gain understanding on how you use our services to improve them. When you open an account, we measure the time it takes until your first transaction to understand how quickly you are able to use your account.
    - We analyse data on transactions between you and our corporate customers to offer information services to our corporate customers or provide them advice on how they can make better use of ING's products and services. When ING processes personal data for this purpose, aggregated data may be made available to the corporate customer. A corporate customer cannot identify you from these aggregated data.
    - We analyse the results of our marketing activities to measure their effectiveness and the relevance of our campaigns.
    - Sometimes we may use automated processes to analyse your personal data, for example we use an algorithm to speed up credit decisions for loans and mortgages.
- **Preventing and detecting fraud and data security:** We have a duty to protect your personal data and to prevent, detect and contain data breaches. We are also obliged to screen your transactions, for example to comply with regulations against money laundering, terrorism financing and tax fraud.
    - We may process your personal information to **protect you and your assets** from fraudulent activities, for example if you are the victim of identity theft, if your personal data was disclosed or if you are hacked.
    - We may use certain information about you for profiling (e.g. name, account number, age, nationality, IP address, etc.) to quickly and

efficiently detect a particular crime and the person behind it.
    - We use contact and security data (such as card readers or passwords) to secure transactions and communications made via remote channels. We could use this data to alert you, for example when your debit or credit card is used in a non-typical location.
- **Internal and external reporting:** We process your data for our banking, credit and financial operations and to help our management make better decisions about our operations and services. We as well process your data to comply with a range of legal obligations and statutory requirements (for example credit, anti-money laundering and tax legislations).

## 4. Who we share your data with and why

To be able to offer you the best possible services and remain competitive in our business, we share certain data internally and outside of ING. This includes:

### ING entities

We transfer data across entities of ING Group for operational, regulatory or reporting purposes, for example to screen new customers, comply with certain laws, secure IT systems or provide certain services. (See section 'What we do with your personal data' for more details). We may also transfer data to centralised storage systems or to process it globally for more efficiency.

### Self-employed agents and brokers

We share information with self-employed agents and brokers who act on our behalf. These agents and brokers are registered in line with local legislation and operate with due permission of regulatory bodies.

### Government authorities and regulated professions

To comply with our regulatory obligations we may disclose data to the relevant authorities, for example to counter terrorism and prevent money laundering or to prevent excessive indebtedness.
In some cases, we are **obliged by law** to share your data with external parties, including:

- **Public authorities, regulators** and **supervisory bodies** such as the central banks of the countries where we operate.
- **Tax authorities** may require us to report your assets (e.g. balances of deposits, payment or savings accounts or holdings on an investment account). We may process your social security number or Tax Identification Number for this.
- **Judicial/investigative authorities** such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request.
- **Lawyers,** for example, in case of bankruptcy, **notaries,** for example, when granting a mortgage, **trustees** who take care of other parties' interests, and **company auditors.**

### Financial institutions

When you withdraw cash, pay with your debit card or make a payment to an account at another bank, the transaction always involves another bank or a specialised financial company. To process payments we have to share information about you with the other bank or specialised financial company, such as your name and account number. We also share information with financial sector specialists who assist us with financial services like:

- Exchanging secure financial transaction messages;
- Payments and credit transactions worldwide;
- Processing electronic transactions worldwide;
- Settling domestic and cross-border security transactions and payment transactions.

Sometimes we share information with banks or financial institutions in other countries, for example when you make or receive a foreign payment. And we share information with business partners whose financial products we sell, such as insurance companies.

### Service providers

When we use other service providers we only share personal data that is required for a particular assignment for the benefit of ING. Service providers support us with activities like:

- Designing and maintenance of internet-based tools and applications;
- Marketing activities or events and managing customer communications;
- Preparing reports and statistics, printing materials and designing products;
- Placing advertisements on apps, websites and social media.

### Partnerships for innovation

We are always looking for new insights to help you get ahead in life and in business. For this, we may exchange personal data with partners like universities, who use it in their research, and innovators. The researchers we engage must satisfy the same strict requirements as ING employees. This personal data is shared at an aggregated level and the results of the research are anonymous.
In all of these cases, we ensure the third parties can only access personal data that is necessary for their specific tasks.

### Communication of personal data in other countries

Whenever we share your personal data internally or with third parties in other countries, we ensure the necessary safeguards are in place to protect it. In case of transfer to a country outside the European Economic Area whose local regime is considered as inadequate by the European Commission, ING relies amongst others on:

- The conclusion or the execution of an agreement, one of your transactions or a third-party transaction in your favour;
- EU Model clauses, which are standardised contractual clauses used in agreements with service providers to ensure personal data transferred outside of the European Economic Area complies with EU data protection law. We may provide you with a copy of these clauses upon request;
- Data transfer that are necessary for reasons of public interests;
- Your explicit consent;
- Privacy Shield framework that protects personal data transferred to the United States.

## 5. Your rights and how we respect them

We respect your individual rights to determine how your personal information is used. These rights include :

### Right to access information

You have the right to ask us for an overview of your personal data that we process.

### Right to rectification

If your personal data is incorrect, you have the right to ask us to rectify it. If we shared data about you with a third party and those data are later corrected, we will also notify that party.

### Right to object to processing

You can object to ING using your personal data for its own legitimate interests (for example, marketing). We will consider your objection and stop processing your data unless we assess that we have legitimate and imperious reasons that justify processing your data.

You can also object to receiving commercial messages from us (by e-mail, mail and phone) or for statistical purposes. When you become an ING customer, we may ask you whether you want to receive personalised offers (based on your payment data and other similar details). Should you later change your mind, you can choose to opt out of receiving these messages by, amongst others::

- Using the 'unsubscribe' button at the bottom of each commercial e-mail;
- Adapting your privacy settings in your ING Home'Bank / Business'Bank/Smart Banking / Smart Banking;
- Filling in our contact form on www.ing.be ;
- Calling ING +32.2.464.60.04;
- Visiting http://www.robinsonlist.be/index.html and https://www.dncm.be/fr/ subscribing to Robinson Mail and the "Do Not Call Me List".

Even if you have opted out of receiving commercial messages, you cannot object to us processing your personal data:

- If we are legally required to do so;
- If it is necessary to fulfil a contract with you;
- If there are security issues with your account, such as when your card is blocked.

### Right to object to automated decisions

You have the right not to be subject to decisions which may legally or significantly affect you and that were based solely on automated processing using your personal information. In such cases you may ask to have a person to make the decision instead. Some of our decisions are the result of automated processes for which you gave us explicit consent or these decisions are necessary to perform or fulfil a contract with you. In both cases, you may ask for

human intervention and contest the resulting decision (e.g. automatic refusal of an online credit application).
Your right to object and to contest may be impeded if automated decisions are made for legal reasons.

### Right to restrict processing

You have the right to ask us to restrict using your personal data for the period necessary to ING for its verifications if:

- You believe the information is inaccurate or we are processing the data unlawfully;
- You have objected to us processing your data for our own legitimate interests.

You have the same right if ING no longer needs the data, but you want us to keep it for use in a legal claim.

### Right to data portability

You have the right to ask us to transfer some of your personal data directly to you or to another company. This applies to personal data we process by electronic means and with your consent or on the basis of a contract with you. Where technically feasible, we will transfer your personal data.

### Right to erasure

Unless required by law, you may ask us to erase your personal data if:

- We no longer need it for its original purpose;
- You withdraw your consent for processing it;
- You object to us processing your data for our own legitimate interests (except for legitimate and compelling interests) or for commercial messages;
- ING unlawfully processes your personal data; or
- A law of the European Union or a member state of the European Union requires ING to erase your personal data.

### Right to complain

Should you not be satisfied with the way we have responded to your concerns you have the right to submit a complaint to us. If you are still unhappy with our reaction to your complaint, you can escalate it to the Data Protection Officer (DPO) of ING Belgium. You can also contact the Belgian data protection authority.

### Exercising your rights

If you want to exercise your rights, you can already access and amend some of your personal data when you log in on ING Home'Bank / Business'Bank/Smart Banking / Smart Banking.
You can also exercise your rights by contacting us (see section 10).
We aim to respond to your request as quickly as possible. In some instances this could take up to one month. Should we require more time to complete your request, we will let you know how much longer we need and provide reasons for the delay.
In certain legal cases, we may deny your request. If it's legally permitted, we will let you know in due course why we denied it.

## 6. Your duty to provide data

There is certain information that we must know about you so that we can commence and execute our duties as a Bank, Lender or Insurance Intermediary and fulfil our associated contractual duties. There is also information that we are legally obliged to collect. Without this data we may not be able to open an account for you or perform certain banking, credit, financial and insurance activities.

## 7. How we protect your personal data

We apply an internal framework of policies and minimum standards across all our business to keep your data safe. These policies and standards are periodically updated to keep them up to date with regulations and market developments. More specifically and in accordance with the law, we take appropriate technical and organisational measures (policies and procedures, IT security etc.) to ensure the confidentiality and integrity of your personal data and the way it's processed.

In addition, ING employees are subject to confidentiality and may not disclose your personal data unlawfully or unnecessarily.

## 8. What you can do to help us keep your data safe

We do our utmost best to protect your data, but there are certain things you can do as well:

- Install anti-virus software, anti-spyware software and a firewall. Keep them updated.

- Do not leave equipment and tokens (e.g. bank card) unattended.
- Report the loss of a bank card to ING and cancel the lost card immediately.
- Log off from online banking when you are not using it.
- Keep your passwords strictly confidential and use strong passwords, i.e. avoid obvious combinations of letters and figures.
- Be alert online and learn how to spot unusual activity, such as a new website address or phishing e-mails requesting personal information.

## 9. How long we keep your personal data

We are only allowed to keep your personal data for as long as it's still necessary for the purpose we initially required it. After this we look for feasible solutions, like archiving it.
When assessing how long to keep personal data, retention requirements might be stipulated by other applicable laws (e.g. anti-money laundering law).
Kept personal data can serve as legal evidence in litigation, but we will not use such personal data actively.
Retention periods may depend on circumstances. For example, your data may be archived for up to 10 years after your bank account has been closed or even up to 30 years for your mortgage loan data.
Other data, collected by surveillance cameras or call recordings are kept for shorter periods as required by law.

## 10. Contact us

If you have questions, want to know more about ING's data policies and how we use your personal data, you can **primarily contact us through our usual channels** by:

- Connecting to your ING Home'Bank, Business'Bank or Smart Banking (app) and sending us a message with a reference to "Privacy",
- Visiting your local branch, contacting your relationship manager, your personal or private banker,
- Calling us +32.2.464.60.04, or
- Sending us an e-mail to info@ing.be referencing "Privacy".

**In case of disagreement or complaints** related to the processing of your personal data, you can send us a request with "Privacy" as reference via:

- E-mail: plaintes@ing.be / klachten@ing.be
- Letter: ING Complaint Management, Cours Saint Michel 60/Sint-Michielswarande 60, B-1040 Brussels

If you did not obtain a satisfactory resolution of your case or if you would like to receive further information about this Privacy Statement, you can submit a written request to the ING Data Protection Officer via:

- E-mail: ing-be-PrivacyOffice@ing.com
- Letter: ING Privacy Office, Cours Saint Michel 60/Sint-Michielswarande 60, B-1040 Brussels.

When you contact us we will have to identify you before carrying out your request. We may for example ask you to an ING branch to identify you correctly. You may be asked to provide us with a valid ID or passport.

You will find below a list of contact information for this Privacy Statement, as well as a list of data protection authorities in each country where ING operates.

## 11. Scope of this Privacy Statement

This is the Privacy Statement of ING Belgium n.v./s.a. acting as data controller, ING Belgium n.v/s.a. - Bank/Lender - Avenue Marnix 24, B-1000 Brussels - Brussels RPM/RPR – VAT BE 0403.200.393 - BIC: BBRUBEBB – IBAN: BE45 3109 1560 2789 – Insurance broker registered with the FSMA under the code number 0403200393. - www.ing.be - Publisher: Marie-Noëlle De Greef - Cours Saint-Michel 60, B-1040 Brussels. 10/18.

We may amend this Privacy Statement to remain compliant with any changes in law and/or to reflect how our business processes personal data. This version was created in November 2018 and enters into force in January 2019. The most recent version is available at ing.be.

## 12. Supplement to the Privacy Statement of ING Belgium S.A.

### Competent authorities

The following competent authorities receive personal data :

- Legal communications to **judicial or administrative authorities**,
- Legal communications at the **Central Point of Contact** of the National Bank of Belgium (NBB),
- Legal communications to the **Central Individual and Corporate Credit Register** of the NBB,
- Communications to the **File of non-regulated registrations** of the NBB.

## Financial sector specialists

Financial sector specialists who also have a legal obligation to treat personal data with all due care are:

- **SWIFT SCRL/CVBA** (established in Belgium) for secure financial transaction message exchange whose data are stored in the United States and are subject to US law,
- **MasterCard Europe SPRL/BVBA** (established in Belgium) **et VISA Europe Limited** (established in the United Kingdom) for payments and credit transactions worldwide,
- **Card Stop** (service of Worldline) to block your bank card,
- **Atos Worldline / EquensWorldline** (established in Belgium) for global credit transactions and Atos Group companies in Morocco and India, which operate as subcontractors,
- **Euroclear** (established in Belgium) for settlement / delivery of securities worldwide, for domestic and international bond and equity transactions,
- **Gemalto** (established in France) for the personalisation of bank cards,
- The **Payconiq** (established in Luxembourg) to facilitate payments with smartphone,
- **Isabel** (established in Belgium) for services via the Internet and the Zoomit service of Isabel,
- **INGenico** (established in Belgium) for the provision of payment terminals to professionals,
- **SIA** (established in Italy) for the authorization of transactions and the provision of credit card statement information,
- Correspondent banking/financial institutions in foreign countries

Please read the specific data protection policies/privacy statements of these specialists on their respective websites.

## Service providers

Some specific personal data may be shared with service providers, including:

- The risk detection service World-Check of **Thomson Reuters Ltd.** (established in the United Kingdom that collects data in and outside the European Union) or **Regulatory DataCorp Ltd.** (established in the United Kingdom collecting data in and outside the European Union);
- The services of **Graydon Belgium SA/NV, Dun & Bradstreet, Swift SCRL/CVBA**, Internet search engines, press and other reliable sources on counter-terrorism and anti-money laundering,
- The financial information services of **Graydon Belgium SA/NV**, Bel-first of **Bureau van Dijk Electronic Publishing SA/NV** (information on companies and their representatives) and the postal address identification services of Bisnode Belgium SA (all established in Belgium), the research services of Fondation OpenStreetMap Ltd. (established in the United Kingdom) and other search engines in connection with marketing ,
- The financial and commercial information service of **Coface SA/NV** (established in France), **Roularta Media Group SA/NV** (Belgium) and the service of **Bloomberg Ltd** (established in the United States) and **Fitch Ratings Ltd** (established in the United Kingdom) for the identification of company representatives,
- The service of **ING Business Shared Services Bratislava** in Slovakia for payment and account-related transactions,
- The service of **ING Business Shared Services Manila** in Manila, Philippines for payment, credit and financial transactions,
- IT services of suppliers such as **Unisys Belgium SA/NV**, **IBM Belgium SPRL/BVBA**, **Adobe** (established in Ireland), **Contraste Europe VBR** (established in Belgium), **Salesforce Inc.** (established in the US), **Ricoh Nederland BV** (established in the Netherlands), **Fujitsu BV** (established in the Netherlands), **Tata Consultancy Services Belgium SA/NV** (established in Belgium and India), **HCL Belgium SA/NV**, **Cognizant Technology Solutions Belgium SA/NV**, **Getronics BV** (established in the Netherlands), **ING Tech Poland** (established in Poland),
- The service of **Selligent SA/NV, Bisnode Belgium SA/NV et Social Seeder SPRL/BVBA** (all established in Belgium) and, where applicable, **external call centers** (in particular, as part of surveys) for marketing activities,
- The security service of funds and securities of **G4S SA/NV / Loomis Belgium SA/NV** (established in Belgium),

- The archiving service of your banking, financial or insurance data in paper or electronic form from **OASIS Group** in Thurnhout in Belgium,
- The service of management of the consumer credit and mortgage credit agreements of **Stater Belgium SA/NV** (established in Belgium),
- The custody service of foreign financial instruments and the management of their "corporate actions": custodians, in particular **Clearstream** (in Luxembourg), the National Bank of Belgium, **Euroclear** (in Belgium), **BNP Paribas SA/NV** (in France), **ING Luxembourg SA/NV** (in Luxembourg).

### Insurances

Personal data may be transmitted as part of the conclusion or execution of an insurance contract to entities outside the ING Group which are established in a Member State of the European Union and in particular:

- **NN Non-Life Insurance S.A./N.V.,**
- **NN Insurance Belgium S.A./N.V.,**
- **Aon Belgium S.P.R.L./B.V.B.A.,**
- **Inter Partner Assurance S.A./N.V.,**
- **AXA Belgium S.A./N.V.,**
- **Cardif Assurance Vie S.A./N.V.** et **Cardif Assurances Risques Divers S.A./N.V.**,
- And to their potential representatives in Belgium (in particular **NN Insurance Services Belgium SA/NV for NN Non-Life Insurance sa/nv**) (list on request).

**For further details, please refer to the General Regulations on the ING Belgium S.A./N.V.**
https://www.ing.be/static/legacy/SiteCollectionDocuments/GeneralRegulationsNewEN.pdf

| Country | Contact details for Data Protection Officer | Data Protection Authority |
|---|---|---|
| Australia | customer.service@ing.com.au | Office of the Australian Information Commissioner (OAIC)<br>https://oaic.gov.au/ |
| Belgium | ing-be-PrivacyOffice@ing.com<br>or<br>**ING Privacy Office,**<br>**Cours Saint Michel 60/Sint-Michielswarande 60,**<br>**B-1040 Brussels** | **Belgian Privacy Authority**<br>**Rue de la Presse 35 / Drukpersstraat 35,**<br>**1000 Brussels**<br>http://www.privacycommission.be |
| France | dpo.privacy.france@ing.com | Commission Nationale Informatique et Libertés<br>https://www.cnil.fr/fr |
| Germany | datenschutz@ing-diba.de | Der Hessische Datenschutzbeauftragte<br>https://datenschutz.hessen.de/ |
| Hungary | communications.hu@ingbank.com | Hungarian National Authority for Data Protection and Freedom of Information<br>http://www.naih.hu/ |
| Italy | privacy@ingdirect.it | Garante per la protezione dei dati personali<br>www.gpdp.it<br>www.garanteprivacy.it<br>www.dataprotection.org |
| Luxembourg | dpo@ing.lu | CNPD - Commission Nationale pour la Protection des Données<br>https://cnpd.public.lu |
| Netherlands | privacyloket@ing.nl | Autoriteit Persoonsgegevens<br>https://autoriteitpersoonsgegevens.nl/ |
| Philippines | dpomanila@asia.ing.com | National Privacy Commission<br>https://privacy.gov.ph/ |
| Poland | abi@ingbank.pl | Generalny Inspektor Ochrony Danych Osobowych<br>http://www.giodo.gov.pl/ |
| Portugal | dpo@ing.es | Comissão Nacional de Protecção de Dados<br>https://www.cnpd.pt |
| Romania | protectiadatelor@ing.ro | National Supervisory Authority for Personal Data Processing (ANSPDCP)<br>http://www.dataprotection.ro/ |
| Russia | mail.russia@ingbank.com | The Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor)<br>https://rkn.gov.ru |
| Slovakia | dpo@ing.sk | Úrad na ochranu osobných údajov Slovenskej republiky<br>https://dataprotection.gov.sk/uoou/ |
| Spain | dpo@ing.es | Agencia Española de Protección de Datos<br>https://www.agpd.es |
| Tchèquie | dpo-cz@ing.com | Úřad pro ochranu osobních údajů<br>https://www.uoou.cz |

| Country | Contact details for Data Protection Officer | Data Protection Authority |
|---|---|---|
| Australia | customer.service@ing.com.au | Office of the Australian Information Commissioner (OAIC)<br>https://oaic.gov.au/ |
| Belgium | ing-be-PrivacyOffice@ing.com<br>or<br>**ING Privacy Office,**<br>**Cours Saint Michel 60/Sint-Michielswarande 60,**<br>**B-1040 Brussels** | **Belgian Privacy Authority**<br>**Rue de la Presse 35 / Drukpersstraat 35,**<br>**1000 Brussels**<br>http://www.privacycommission.be |
| Ukraine | dpe.office@ing.com | Personal Data Protection department of Ombudsman<br>http://www.ombudsman.gov.ua |

ING Belgium SA/nv - Bank/Lender - Avenue Marnix 24, B-1000 Brussels
VAT BE 0403 200 393 – Brussels RPM/RPR – BIC: BBRUBEBB – IBAN: BE45 3109 1560 2789 – www.ing.be – info@ing.be. Insurance broker registered with the FSMA under the code number 0403200393
Publisher: Marie-Noëlle De Greef - Cours Saint-Michel 60, B-1040 Brussels. 10/18.