

ING Banking Terms and Conditions

1st November 2020 – v1.4



Contents

1. General provisions	4
1.1 Purpose of the General Conditions	4
1.2 Definitions	4
2. Purpose of the ING Banking services	6
2.1 The ING Banking services	6
2.2 ING Banking Services	7
2.3 Payconiq In App Service	7
3. Legal framework applicable to ING Banking	8
3.1 Contract comprising the agreement	8
3.1.1. List of documents comprising the Agreement	8
3.1.2. Changes to the contractual framework on ING's initiative	9
3.2 Application of the agreement	9
3.3 Applicable legislation and competent courts	9
4. Subscription to the electronic services of ING and users of such services	9
4.1 Subscribing to the electronic services of ing	9
4.2 Users of the electronic services of ING	11
5. Access and use of the ING Banking	12
6. Obligations of the Client and the User with regard to security	13
7. ING's obligations as regards security	16
8. Liabilities of the Parties	16
8.1 General liability as regards the electronic services of ing	16
8.2 Special liability rules with regard to payment transactions	18
9. Ceilings of Transactions	21
10. Maintenance of the ING Banking services	22
11. Protection of privacy	23
11.1 General provisions	23
11.2 ING banking services	26
12. Proof of Transactions	26
12.1 Proof of transactions in general	26
12.2 ING banking services	27
13. Lists of charges – value dates	28
14. User licence for the ING Banking software and Home'Bank / Business'Bank / ING Banking database / Payconiq In App Services	29
15. Hypertext links for the ING Banking services	30
16. User messages	30
17. Chat	30
18. Availability of the ING Bankingservices	31
19. Duration of the ING Banking, Agreement - De-activation of the services and Termination of the Agreement	31
Appendix 1 : Cautionary advice for accessing and using the ING Banking services	33

**Appendix 2: The "ING Zoomit" service of the Home'Bank/Business'Bank/Smart Banking/ING Banking services
Regulation 35**

ING Banking Terms and Conditions

1. General provisions

1.1 Purpose of the General Conditions

The purpose of these ING Banking Terms and Conditions for ING Banking (hereafter the “General Conditions”) is to describe the electronic services offered by ING under the name ING Banking and to determine the rights and duties of the Client, the User and ING with regard to the provision by ING of ING Banking 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 the ING Banking electronic services, 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 or joint holder of the account(s) opened with ING and/or other companies of the ING Group and/or even with insurers outside the ING Group for which ING acts as an intermediary has concluded (a) contract(s), where such accounts or contracts are, in accordance with this Agreement once concluded, accessible via the ING Banking services 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, an insurance broker, registered with the FSMA under the code n° 12381 A, acting in its own name and on its own behalf as well as in the name and on behalf of the other companies of the ING Group and insurers outside the ING Group.

ING acts, in particular, as a service provider through the channel of electronic communications as well as a certification authority and issuer of ING Banking access and signature means, with the

other companies of the ING Group and insurers outside Europe on whose behalf ING acts as an intermediary using such services and means for secure electronic data transmission.

4° The other companies of the ING Group: the companies of the Group, with the exception of ING, which provide banking, financial and/or insurance services, which are established in a Member State of the European Union and whose services and products are available via ING Banking.

The up-to-date list of the ING Group companies in Belgium is available on the ING website (www.ing.be). The up-to-date list of the ING Group companies based in a Member State of the European Union can be obtained on simple request sent to ING.

5° The insurers outside the ING Group: the insurance companies for which ING acts as an intermediary, which are not part of the other companies of the ING Group, which are established in a Member State of the European Union and whose services and products are available through ING's electronic services.

The up-to-date list of the insurers outside the ING Group established in a Member State of the European Union can be obtained on simple request sent to ING.

6° Parties: ING and the Client as well as, where appropriate, the other companies of the ING Group or insurers outside the ING Group.

7° User: the individual(s) designated and authorised by the Client, in accordance with the provisions of point 4 below, to use the electronic services of ING according to the conditions laid down by this Agreement. If the Client is a natural person, he/she is also a User, unless he/she is under age or incapable (in which case he/she is only a User where duly authorised).

8° The ING Banking services, also designated as the electronic services of ING: all the electronic services offered by ING under the name ING Banking services and described in point 2 of these General Conditions.

9° Technical Documentation on the use of the electronic services of ING: any user manual of the ING Banking, and other technical documentation relating to the use of such services and concerning, in particular, communication and electronic signature procedures.

10° 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.

11° Transaction: any Transaction, whether a Payment Transaction, a Financial Instrument Transaction or any other banking, financial or insurance Transaction, or even any banking, financial or insurance product or service contract which can be the subject of an Instruction via the electronic services of ING.

12° Transaction on Financial Instruments: an act of buying, subscribing to, transferring or selling financial instruments, irrespective of any underlying obligations between the payer and the payee of the order.

13° Payment Transaction: an action consisting in transferring funds, irrespective of any underlying obligations between the payer and the payee of the Payment Order.

14° Payconiq Payment Transaction: a Payment Transaction given via the Payconiq In App Services .

15° Payconiq Payment Request: a personalised message requesting the recipient to transfer a specified amount by following the link included in the message and subsequently authorizing a payment instruction.

16° Payconiq In App Service: electronic payment service offered under the name "Payconiq" provided by the Payconiq Supplier, integrated as an ING Banking Service, allowing the user to transfer funds.

17° Payconiq Supplier: Payconiq International SA, rue Jean Fischbach, 7, L-3372 Leudelange, Grand Duchy of Luxembourg, registered with Luxembourg Trade Register under number B 169621, which is a company currently outside of the ING Group, or one or more third-party companies (information available on the website of Payconiq: www.payconiq.com)

18° BC/MC Mobile Payment Order: any Payment Order given through the operation of the Bancontact/Mister Cash (BC/MC) network linked to the ING debit card and included in the ING Banking service.

19° Payment Instruction: any instruction given through the ING Banking services, in the name and on behalf of the Client, requesting the execution of a Payment Transaction.

20° BC/MC mobile Payment Instruction: any Payment Order given through the operation of the Bancontact/Mister Cash (BC/MC) network linked to the ING debit card and included in the ING Banking service, in the name of and on behalf of the Client, requesting execution of a mobile BC/MC Payment Transaction to ING.

21° Consumer: a natural person who, in connection with the electronic services of ING, is acting for purposes other than his/her trade business or profession.

22° 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.

23° Value date: the reference date used to calculate the interest applicable to funds debited from or credited to an account.

24° Unique Identifier: the combination of letters, numbers or symbols used by the Client or the User to identify unambiguously the account used and/or payee of a Payment Transaction.

To the exclusion of any other element, the Unique Identifier consists of:

The IBAN (International Bank Account Number, consisting of a maximum of 34 alphanumeric characters and a set length in each country. It includes a country code (2 letters, a check digit (2 numbers) and a national bank account number).

For certain Payment Transactions, the IBAN must – where appropriate – be completed by the BIC (Bank Identifier Code, an international code which allows the unique identification of each bank. It designates the bank of the Payee; it consists of 8 or 11 alphanumerical characters and includes a bank code (4 characters), a country code (2 letters), a place code (2 characters), and for completeness's sake, for some banks, a branch code (3 characters)). Where the BIC is required, it is part of the Unique Identifier.

Conversely, neither the name of the payer or the payee of the Payment Order, nor their addresses, are part of the Unique Identifier even when such information is required, in particular for control purposes pursuant to public order national or international legal provisions.

25° 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.

26° 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 as a fingerprint or face recognition) 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

27° Personalised Security Credentials : personalised features provided to the User by ING for authentication purposes.

28° Payment Initiation Service: an online service allowing a payment service user to initiate a payment order involving a payment account held with another payment service provider;

29° Account Information Service: an online service that provides consolidated information concerning one or more payment accounts held by a payment service user, either with another payment service provider or with more than one payment service provider;

2. Purpose of the ING Banking services

2.1 The ING Banking services

2.1.1. According to the possibilities offered by ING, the electronic ING Banking services enable the User, via his mobile IT system

- To obtain general or personal banking, financial or insurance information (in particular, account information) from ING, other companies of the ING Group, account servicing financial institutions external to the ING Group or the Insurers external to the ING Group, and
- To send ING, or the other companies of the ING Group or the insurers external to the ING Group, Instructions relating to Payment Transactions, financial instrument transactions or any other banking, financial or insurance transactions with a view to their execution.

According to the possibilities offered by ING, the Client - if a User - and/or Users who can represent him/her can, also conclude or ask, subject to acceptance by ING or another company of the relevant ING Group or insurer external to the ING Group in question and by mutual agreement, to conclude contracts relating to banking, financial or insurance contracts with ING or insurer external to the ING Group in question (such as, for instance, opening accounts, taking out loans, making investments and taking out insurance, etc.).

According to the possibilities offered by ING, the User can receive information and carry out Transactions with regard to any account of which the Client is the holder or joint holder, open with ING and other companies of the ING Group. Similarly, the User can also receive information relating to all the accounts the Client is authorised to consult.

According to the possibilities offered by ING, the User can also receive information concerning accounts held with a third party account servicing financial institution and made available to the User online. ING only displays information relating to accounts for which the User has given his/her explicit consent.

According to the possibilities offered by ING, the Client – if a User – and/or Users who can represent him/her, can adjust the mandates on the accounts of which the Client is a holder or co-holder, opened with ING or the other companies in the ING Group.

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

2.1.3. The ING Banking services can be accessed at a distance, without the physical presence of an ING member of staff.

2.1.4. The banking, financial or insurance products and services available via the ING electronic services are intended only for residents of an EU Member State and who are nationals of an EU Member State, unless otherwise expressly stipulated or agreed. They are supplied either by ING, in which case the latter is the "vendor", or by a third-party company (including another ING Group company or an insurer external to the ING Group), in which case the capacity of the latter with regard to the banking, financial or insurance products and services it provides is mentioned in the ING Banking services and ING simply acts as an intermediary for and on behalf of the company concerned.

2.2 ING Banking Services

2.2.1. The ING Banking services are IT services available by means of electronic data transmission between ING and the User. They are provided by ING through its electronic systems (in particular its software, servers and network) and intended for any User with a compatible mobile IT system supplied by a third party, either an IT system (smartphone or tablet) with Android from Google or iOS from Apple (e.g. an Apple iPad, iPhone or iPod Touch, etc.), (hereafter "the mobile IT system" for the purposes of this Agreement). Such system must make it possible to use ING's electronic systems with a view to using the ING Banking services. To use the BC/MC mobile function linked to the ING debit card in the context of the ING Banking services with a view to executing BC/MC mobile payments, the Mobile IT system must in addition be equipped with a camera (with autofocus). To use the fingerprint recognition or face recognition function, supplied by a third party (e.g. the IOS Touch ID and Face ID from Apple or the Android Fingerprint), in the context of the ING Banking services with a view to securing access to the latter using the User's fingerprint or face recognition, the Mobile IT system must in addition be equipped with a fingerprint reader or a camera. Users must ensure that their Mobile IT system complies with the specifications stipulated in the Technical

Documentation on the use of the electronic services of ING.

2.2.2. The ING Banking services are provided by ING through IT programmes (hereafter the "ING Banking Software") and a database (hereafter the "ING Banking Database").

In particular, the ING Banking Software may include a security module (hereafter the "Security Module") and a security file for each User (hereafter the "Security File") with the ING Banking codes for a User in digital form which secures access to and use of the ING Banking services. When using the fingerprint recognition function (e.g. the IOS Touch ID from Apple or Android Fingerprint) or face recognition function (Face ID from Apple), recognition of a User's fingerprint or face replaces that of his/her authentication code to secure access to the ING Banking Services. The Security File is created by the User during the Security Module initialisation procedure. The ING Banking Software uses SSL v3 (encryption/decryption technology).

To access and use the ING Banking services, the User must download the ING Banking Software and the ING Banking Database (either the Phone or Tablet app) via the App Store or "Play Store" electronic application of his/her mobile IT System or via the iTunes "App Store" on the Apple website or "Play Store" on Google's website and install it on his/her/its mobile IT system. Access to the ING Banking services and use thereof also requires using the means of access and signature of the ING Banking services as defined in Articles 5 and 12 of these General Conditions.

2.2.3. The ING Banking services are services provided online requiring a direct connection between the User's mobile IT system and ING's electronic systems.

To use the ING Banking services, the User establishes a connection between his/her mobile IT system and ING's electronic systems through an electronic communications network, whether a telecommunications network, public or other, and/or a broadcasting network, in accordance with the specifications laid down by ING in the Technical Documentation on the use of ING's electronic services and communicated by the provider(s) of the electronic communications network concerned.

2.3 Payconiq In App Service

2.3.1 The Payconiq In App Service **allows** the User to

- (1) transfer funds to a merchant (P2M payment)
- (2) send Payconiq Payment Request

2.3.2 To access and use the Payconiq In App Service, the User must have a Payment Account denominated in Euros.

3. Legal framework applicable to ING Banking

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 Banking services and, where appropriate, its appendices signed for and on behalf of the Client (hereafter the /ING Banking/ Subscription Contract”)
- The Management Powers documents for general and/or specific Transactions and/or the authorisations accepted for and on behalf of the Client as well as the various aforementioned additional mandates, document amendments and authorisation forms, or any other similar document, electronic or otherwise, which ING provides or not to the Client (notably as appendix to the Phone’Bank/Home’Bank/Business’Bank/ING Banking/Extrabranh Mobility/e-ID for Branch, Belgian Mobile Identity, Payconiq for ING BE and/or Belgian Mobile Identity for ING BE services Subscription Contracts or via the Home’Bank/Business’Bank services), which are duly accepted by ING and by the Client or for and on behalf of the Client (hereafter “Management Powers” documents)
- Special agreements relating to certain functions of ING’s electronic services
- These General Conditions of ING's electronic services and, where appropriate, the appendices thereto
- The prices applicable for ING's electronic services
- Technical Documentation on the use of ING's electronic services.

The order of priority of the documents making up the Agreement is governed according to the descending

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

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, the other companies of the ING Group or the insurers external to the ING Group concerned and those relating to the insurance, financial and banking products and services available via the /ING Banking/ services and, in particular, to the Transactions available via these services, apply in full to the /ING Banking/ services, whether they are provisions agreed or to be agreed between the Client and ING, notably those of the General Regulations of ING, of the Special Regulations for Trading in Financial Instruments, and the financial services covered by these Regulations, or the Special Regulations for Payment Transactions and the payment services covered by such Special Regulations¹, or the General Terms and Conditions of the ING debit card for the execution of BC/MC Mobile Payment Transactions covered by these General Terms and Conditions of the ING debit card, or those agreed or to be agreed between the Client and the other companies of the ING Group (e.g. those relating to the Payconiq services agreed or to be agreed with PayconiqSupplier) or insurers external to the ING Group.

Furthermore the documents referred to in this point 3.1.1.2, with the exception of those relating to the provisions agreed or to be agreed between the Client and the other companies of the ING Group, are available from any ING branch

3.1.1.2. The Client and the User can obtain all necessary information about the /ING Banking services/ by calling, browsing the ING website (www.ing.be) or, with respect to the /ING Banking services, the information broadcast through such services.

3.1.1.3. The Client and the User acknowledge that, prior to conclusion of the ING Banking contract, 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 Banking/ Agreement, they absolve ING from any liability in this respect and acknowledge that the electronic services of ING 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, email sent to the mailbox of the Client or the User and/ or messages displayed via the Home'Bank/Business'Bank Online or ING Banking services, without prejudice to mandatory or public order legal provisions. Such notification must take place at least two months or, if the Client is not a Consumer, 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 3.1.2. 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 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 the electronic services of ing

4.1.1. The electronic services of ING are provided to ING Clients who wish to use these services for private purposes.

4.1.2. The ING Banking Agreement is concluded with a Client by entering into ING Banking/ Subscription Contract and, as appropriate, its Annexes (in particular additional mandate forms) accepted for and on behalf of the Client, where appropriate by simply subscribing as stipulated in the following paragraph.

When opening an account, appointing an authorised user of the account or entering into a contract with ING, another ING Group company or insurers external to the ING Group, the Client automatically subscribes, by signing, electronically or otherwise, the relevant contractual documents (documents for opening an account, "Management Authority" documents, etc.) and unless specified to the contrary in these documents, to these ING Banking Terms and Conditions (including, notably, in the Appendix to ING's General Regulations), provided the relevant contractual documents refer to such subscription. By subscribing, the Client acknowledges that he/she/it has received a copy of these ING Banking Terms and

Conditions on paper or another durable medium in advance and has read the terms thereof. Such subscription implies acceptance of the ING Banking/ Subscription Contract and, likewise, conclusion of the / ING Banking Agreement.

Once the ING Banking Agreement has been concluded, where appropriate by means of the aforementioned subscription, any of the Client's Users is authorised to activate and deactivate the ING Banking/ services and to access and use them in accordance with the provisions of the Agreement.

4.1.3. If the Client and the User wish to activate the ING Banking services, they are bound to comply with the terms, conditions or procedures set out in the Technical Documentation on use of the electronic services of ING or any other form at ING's discretion. Once accepted by ING, activation of the ING Banking services is equivalent to the commencement of the subscription to the ING Banking services.

4.1.4. Subject to the possibilities offered by ING, the Client accepts that on concluding the /ING Banking/ Agreement, all the accounts with ING and the other banks of the ING Group in Europe of which he/she is the holder or joint holder shall be accessible via the ING Banking services for all of the Transactions he/she is authorised to carry out in relation to the management of such accounts, unless he/she expressly requests ING to exclude one or more specific accounts from the scope of the Agreement. Subject to the same reserve, the Client also accepts that all his/her representatives and agents referred to as such in the "Management Powers" documents (electronic or otherwise) for the account(s) with ING and other companies of the ING Group in Europe of which he/she is the holder or joint holder shall be considered automatically as Users of the ING Banking services.

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 or joint holder, as well as any changes made subsequently to such powers and limits, apply to Transactions submitted via the electronic services of ING.

The Client can, by completing the various mandate forms (electronic or otherwise) which ING provides to the latter (notably, as annexed to the Phone'Bank/Home'Bank/Business'Bank/ING Banking/Extrabranh Mobility/e-ID for Branch/Payconiq for ING BE and Belgian Mobile Identity for ING BE services or, subject to the possibilities offered by ING, via the Home'Bank/Business'Bank services), grant mandates by completing mandates and limits indicated on the Management Powers documents (electronic or otherwise) for general and/or specific Transactions for the account (jointly) held by the Client, to carry out the electronic Transactions via the electronic services of ING.

The "Management Powers" documents (electronic or otherwise) for the account(s) of which the Client is the holder or joint holder can, in particular in relation to the mandates, authority and the limits thereto, in the context of Transactions submitted via the electronic services of ING, be changed at the Client's request (at his/her ING branch or, subject to the possibilities offered by ING, via the Home'Bank/Business'Bank services) in accordance, with respect to ING, with the provisions of ING's General Regulations or, with respect to the other companies of the ING Group, with the provisions of their relevant regulations.

Without prejudice to specific provisions in this Agreement providing otherwise (in particular point 4.2.2.), ING shall, for the performance of this Agreement, take the "Management Powers" forms (electronic or otherwise) completed by the Client and/or the Client's change request for the "Power of Attorney" documents (electronic or otherwise) into account from the seventh bank business day at the latest after it has received them or from the thirtieth bank working day at the latest after they have been received by another bank of the ING Group. However, ING shall endeavour to implement it before such time if it is able to do so.

The provisions of this point 4.1.5. do not prejudice the setting of specific ceilings for Transactions submitted via the electronic services of ING in accordance with point 9 of these General Conditions.

4.1.5. Subject to the possibilities offered by ING, for the purpose of the ING Banking services, the Client agrees to receive all information relating to the banking, financial or insurance services and products

taken out in the name and on behalf of the Client with ING and other ING Group companies and insurers external to the ING Group, in particular with regard to accounts opened with ING and other ING Group companies of which the Client is the holder or joint holder or for which he/she is authorised to receive information.

He/she moreover explicitly agrees that all the Users may consult this information via the ING Banking/ services.

4.1.6. Upon conclusion of the Contract, the Client accepts that all insurance contracts concluded with ING and other ING Group companies or insurers external to the ING Group may be accessed by Users via the ING Banking services to carry out all the Transactions authorised in connection with the management of such contracts, subject however to the possibilities offered by ING.

4.2 Users of the electronic services of ING

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 the ING Banking services, including any information relating to banking, financial or insurance services and products taken out in the name of and on behalf of the Client with ING and other companies of the ING Group and insurers external to the ING Group (in particular information relating to accounts opened with ING and other companies of the ING Group, of which the Client is the holder or joint holder or for which the Client is authorised to receive information), subject however to the possibilities offered by ING and without prejudice to point 4.1. of the ING Banking Terms and Conditions.

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 orders for and on behalf of the Client requesting the execution of a Payment Transaction, a Financial Instrument Transaction or any other banking, financial or insurance transaction. Subject to the same reserves, the Client, if he/she is a User, and/or the Users who may act as his/her representatives, can also, using their electronic signature, conclude or

request (subject to acceptance by ING or another company of the ING Group or an insurer external to the ING Group concerned and to mutual agreement) to conclude insurance, financial or banking contracts, in accordance with their powers and within the limits of such powers, as defined in point 4.1 above.

Nevertheless, by way of a derogation from the above, Users with powers which are limited in terms of the authorised maximum amount of Transactions or the number of signatures required to carry out Transactions, may not enter and transmit orders requesting the execution of Transactions on Financial Instruments.

In addition, with regard to ING Banking the Client accepts, by derogation from the above, that only those users of ING Banking and services who are authorised to manage, alone and without restrictions (whether said restrictions are expressed in terms of the maximum authorised amount for Transactions, the number of signatures required to initiate Transactions and/or the types of Transaction authorised), the account(s) the Client holds solely or jointly with ING and other companies in the ING Group or insurer external to the ING Group may enter and transmit orders requesting the execution of a Payment Transaction, a financial instrument Transaction or any other transaction of a banking, financial or insurance nature, or otherwise enter into agreements or request (subject to acceptance by ING or by another company in the ING Group concerned, and by mutual consent) to enter into agreements of a banking, financial or insurance nature, in line with the above provisions, subject however to the possibilities offered by ING and without prejudice to point 4.1. of the ING Banking Terms and Conditions.

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 or another company of the ING Group or insurer external to the ING Group concerned, in particular, with respect to ING, in ING's General Regulations or, with respect to the other companies of the ING Group or insurers external to the ING Group, in the applicable regulations of the latter.

To block the means of access and signing the /ING Banking services, the Client or his/her/its Users must follow the procedures for blocking means of access and signing described in the provisions of point 6.4 of these General Conditions. However, Users duly mandated in the "Management Powers" documents

(electronic or otherwise) or in the various mandate forms (electronic or otherwise) provided by ING in Annex to ING Banking Subscription Contract, with the exception of duly authorised representatives and agents, may only block their own means of access and signature for the ING Banking services.

If the Client or his/her/its Users subsequently wish to reverse the block, he/she/it is obliged to confirm this to ING beforehand in accordance with the terms, conditions and procedures set out in the Technical Documentation on use of the electronic services of ING or in another way at ING's discretion.

If the Client asks ING to revoke a User's powers, ING shall endeavour to block the User's access to the electronic services of ING 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. If the Client wants such revocation to apply immediately in respect of use of the electronic services of ING, he/she/it must use the specific procedure for blocking means of access and signature referred to above in conjunction with the revocation procedure.

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 and signing 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 of the ING Banking

5.1. ING Banking

5.1.1 To access the ING Banking services for a given Mobile

IT system, the User must have set up a profile (hereafter the "Profile") beforehand based on the means of access provided by ING (such as the smart bank card with a card reader and/or his/her personal access numbers (ING ID and Card ID), according to the possibilities offered by ING) and those chosen by the User him/herself (such as the PIN linked to the smart bank card, the Home'Bank/Business'Bank password and/or any other confidential authentication code

known only to the User, according to the possibilities offered by ING).

ING Banking services are subsequently only accessible to the User after he/she has been identified by means of the "profile" set up as indicated above and by the means of access chosen by the User him/herself (such as a PIN and/or any other strictly confidential authentication code known only to the User and/or fingerprint of the latter where the fingerprint recognition function is used (e.g. iOS Touch ID of Apple or Android Fingerprint) and/or face recognition function (e.g.: the iOS Face ID) available on some Mobile IT systems equipped with fingerprint reader or a camera, according to the possibilities offered by ING). To use the aforementioned fingerprint recognition function or face recognition function for a given "profile", the User must first activate such function for the "profile" in question. Such activation is itself done by the User in connection with the ING Banking services used for such "profile".

5.1.2. By entering into the ING Banking Agreement and, where appropriate, pursuant to the signature of the "Management Powers" documents (electronic or otherwise) or the various mandate forms (electronic or otherwise) ING provides as an Annex to Subscription Contract, the Client and Users agree to the provision of the electronic services of ING means of access and signature.

Upon receipt of the means of access and signature, 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 and signature, in accordance with the provisions of these General Conditions.

Until then ING shall accept the risk associated with sending the means of access and signature to the User.

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 Payconiq Agreement or the Belgian Mobile Identity Agreement.

5.2.2. Once the User has accessed the ING Banking services and has been identified in accordance with point 5.1.1., the User may send Orders via the ING

Banking automated services by entering data on the keyboard of his/her Mobile IT system.

5.2.3. With regard to access to the ING Banking services, without prejudice to the provisions of this point 5. and 8 of these ING Banking Terms and Conditions, the Client accepts that the entering and validation by someone of the User's "profile" and the personal and confidential means of access chosen by the User constitute valid and sufficient proof of the identity of such person as a User of ING Banking services who is the holder of the ING Banking Software for the relevant profile, provided such means of access have been authenticated by the relevant ING Banking Software and, where appropriate, by the fingerprint recognition function or the face recognition function. Through this validation, the means of access used are, in particular, recognised by the relevant ING Banking Software and, where appropriate, by the fingerprint recognition function or the face recognition function as originating from the User.

5.2. Payconiq In App Service

5.2.1 In order to make a payment the User must authenticate himself and authorize the Payment Instruction using the available ING Banking Access and Signature means.

5.2.1 A Payconiq Transaction is processed in Euros via Sepa Credit Transfer from the payment account of the user to the payment account of the beneficiary, or from another person to a Payconiq User.

5.2.2 Notwithstanding Clause 5.2.1 , a beneficiary /merchant may use us or another payment service provider ("PSP") to collect payments on his behalf. In that case, the amount of your payment will be transferred to the payment account of the Payconiq Supplier or the payment account of the PSP used by the Merchant to collect payments on his behalf.

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 the ING Banking stipulated in the 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 Banking services can be accessed.

In particular, the Client and Users undertake only to use the ING Banking/ 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 Banking services access and signature means in accordance with the provisions of this Agreement which come into effect upon the issuing or use of said services, within the limits of use agreed on with ING the other companies of the ING Group and the insurers external to the ING Group.

The User undertakes to respect the cautionary advice in order to avoid any risk of misuse of its means of access and signing the electronic services of ING:

Such cautionary advice includes:

- Make sure no one is watching when you carry out your transactions, especially when entering your PIN.
- Use a security code to turn on your mobile device.
- Choose a secure profile code - avoid using your date of birth.
- Do not leave your mobile device in a public place or your car.
- If your mobile device is lost or stolen, call our help desk on +32 2 464 60 04 (you will also find this number on the back of your ING bank card).
- Perform a factory reset on your mobile device if you sell it.
- Always install the latest version of this app and the software for your mobile device (iOS or Android). Never use jailbreak software.
- When making a transfer, always check the account details and amount.
- ING will never ask you for your banking details by e-mail. If you receive such an email, do not reply but instead call our helpdesk on +32 2 464 60 04 (you will also find this number on the back of your ING bank card).

- If you notice anything unusual when using the app, do not make any further transfers and call our helpdesk immediately on +32 2 464 60 04 (you will also find this number on the back of your ING bank card).

The User shall take all reasonable precautions to ensure that his/her ING Banking services means of access and signature are secure. The means of access and signature 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 Banking, access and signature means to a third party (including, but not limited to, a spouse, a family member and/or a friend) 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.

Furthermore, in the context of the ING Banking services, the User may only activate, in accordance with point 5.4.1. of these general conditions, the fingerprint recognition function (e.g. the IOS Touch ID or Android Fingerprint) or the face recognition function (e.g.: the iOS Face ID) for a given “profile” on a Mobile electronic system of which he/she is the sole user. In addition, he/she may only record his/her own fingerprints or face for the fingerprint or facial recognition function on such same Mobile electronic system.

6.4. The Client and/or User is/are obliged to immediately notify ING as soon as he/she becomes aware of:

1. the loss, theft, misappropriation or any unauthorised use of his/her/their ING Banking services means of access and signing (except in case of use of an electronic pen as means of signing of the latter services). “Loss” or “theft”, within the meaning of these ING Banking Terms and Conditions, refers to any involuntary dispossession of the ING Banking services means of access and signature (excepted in

case of use of an electronic pen as means of signing of the latter services). “Misappropriation” or any “unauthorised use” means any illegitimate or unauthorised use of the ING Banking services means of access and signature (except in case of use of an electronic pen as means of signing of the latter services);

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

ING provides each Client or User with the appropriate means to enable him/her to make such notification at any time. The Client and/or the User undertake to block, in the aforementioned cases, his/her/its means of access and signing the ING Banking/ services by following, for instance, the blocking procedures as described in the Technical Documentation relating to the use of the electronic services of ING (in particular by calling **Card Stop (070 344 344** or +32 70 344 344 from abroad) to block cards or the **ING Help Desk (02 464 60 00** or +32 2 464 60 00 from abroad) to block only the Phone’Bank/Home’Bank/Business’Bank/ING Banking/Extrabranche Mobility/ e-ID Branch/Payconiq for ING BE and/or Belgian Mobile Identity for ING BE services).

The Client or the User receives a written or electronic confirmation or an identification means (such as a number) enabling him/her to prove their notification. **The call to Card Stop or the ING Help Desk shall be recorded by an automated system. The data recorded in this way has probative value in the event of a dispute and is saved in accordance with Article 14 (protection of privacy), without prejudice to Articles VI.83 and VII.2, § 4 of the Code of Economic Law.** The data recorded in this way constitutes proof in the event of a dispute and is saved in accordance with Article 12.

In the event of theft, misappropriation or unauthorised use of the ING Banking means of access and signature, 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. Without prejudice to the special provisions applicable to Payment Transactions, in particular the provisions of the Special Payment Transaction Regulations, and the Transactions on Financial

Instruments, in particular the provisions of the Special Regulations for Trading in Financial Instruments, neither the Client nor the User may revoke a Transaction which the User has carried out using his/her access or signature means of the electronic services of ING.

Using information which the Client receives, in accordance with point 7.3 of these General Conditions, with regard to the Transactions carried out in the connection with the electronic services of ING (in particular, using account statements or breakdowns), the Client or the User is required to regularly, and at least once a month, verify the correct receipt, acceptance or not and possibly correct execution of Orders given via the ING Banking services by means of the User's access or signature means. Similarly, the Client is also required to regularly verify the regularity of entries booked in the context of the electronic services of ING. Moreover Clients or Users who subscribe to the ING Banking services are required to read regularly, and at least once a month, the notices provided by ING via the Home'Bank/Business'Bank services, in particular for the application of point 3.1.2.

The Client or the User is obliged to notify ING or, if the relevant Transaction involves another company of the ING Group (e.g. if the relevant account(s) is (are) involved by the Transaction is (are) held at another bank of the ING Group) or an insurer external to the ING Group, the company of the ING Group or the insurer external to the ING Group concerned by the Transaction:

1. of any Transaction carried out without their agreement which appears on their bank or account statements or any other document on a Durable medium upon receipt, acceptance or execution of the Transactions in accordance with point 7.3 of these General Conditions; or
2. of any error or irregularity noticed on their bank or account statements or any other document on a Durable Medium received following the receipt, acceptance or execution of their Transactions in

accordance with point 7.3 of these General Conditions.

Such notification must be confirmed by the Client or the User in writing to ING or, if the relevant Transaction relates to another company of the ING Group or an insurer external to the ING Group, to the company of the ING Group or an insurer external to the ING Group concerned by the Transaction.

Without prejudice to the special provisions stipulated below and relating to the deadline for disputing Payment Transactions, any complaint relating to a Transaction carried out through the /ING Banking services 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.

By way of a derogation from the above provisions, the following rules apply to complaints relating to Payment Transactions.

Once the information relating to the Payment Transaction has been made available to the Client or the User – or, in the absence of such availability, supplied to the Client or the User – the Client or the User does not obtain the correction of a Payment transaction immediately notified to ING of an unauthorised Payment Transaction, or a Payment Transaction not executed or not executed correctly and giving rise to a claim, and at the latest within thirteen months following the date of the debit or the credit, unless - where appropriate - ING has not provided or made available information relating to such Payment Transaction in accordance with these ING Banking Terms and Conditions. If such notification was not made in writing, the Client or the User can confirm it in writing, as stipulated in this point, after the aforementioned deadlines have elapsed.

Where the Client is not a Consumer, the abovementioned period of thirteen months is reduced to two months. After such deadline, the Payment Transaction shall be deemed to be correct and exact and can no longer be disputed.

6.7. The electronic services of ING access and signature means which are provided to Users by ING, with the exception of the access and signature means selected by the User him/herself (such as a password, PIN and/or any other confidential authentication code known only to the User), remain the exclusive property of ING or, accordingly unless otherwise provided for in this Agreement or expressly agreed with the Client or the User.

The smart card readers offered free of charge by ING or bought by the Client or the User to replace smart card readers offered free of charge by ING remain the exclusive property of ING, unless stipulated otherwise in this Agreement or expressly agreed with the Client or the User. However, card readers bought by the Client or the User, with the exception of those acquired to replace smart card readers offered free of charge are, from the time of their purchase, the exclusive property of the relevant Client or User.

Users undertake to return to ING or Another company of the ING Group accordingly, at the first request of ING, or Another company of the ING Group, the ING Banking services his/her access and signature means Furthermore, the User undertakes to return to ING his/her ING Banking access and signature means, in the event the access and signature means are no longer used following termination of this Agreement or revocation of the User's powers.

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 and signature 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. ING shall refrain from providing any unsolicited access and signature means of ING's electronic services, except to replace such means.

7.3. At the very least ING shall ensure that the User is sent electronic (where appropriate, by e-mail), telephone or written confirmation of receipt of his/her Order requesting execution of a Payment Transaction, Transaction on Financial Instruments or any other banking, financial or insurance Transaction or request to conclude or accept a banking, financial or insurance contract placed via ING Banking services. Depending on whether it is an Order or an application to conclude or accept a contract, ING, the other

company of the ING Group or the insurer external to the ING Group in question, shall also or, instead of the aforementioned written confirmation, ensure that the User or Client is sent electronic (where appropriate, by e-mail) or written confirmation that the Order has or has not been accepted and, if accepted, whether the Order has been carried out or not, or whether the contract has been concluded or the application to conclude a contract has been accepted or not.

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, ING or the other company of the ING Group where the account in question is held shall provide or make available to the Client or the User, regularly and at least once a month following the receipt, acceptance of execution of Orders relating to Transactions transmitted in connection with the /ING Banking 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.

Without prejudice to the foregoing, ING shall provide the Client with confirmation of the execution of a Transaction involving financial instruments on the day following the execution of the relevant Transaction, at the latest, in accordance with Article 118 of the Special Regulations for Trading on Financial Instruments.

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 ING Banking access and signature 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 General liability as regards the electronic services 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 Payment Transaction obligations stipulated in points 6.4., 7.1., 7.4 and 12.1.1. of these ING Banking 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, the other companies of the ING Group or insurers external to the ING Group concerned as regards banking, financial or insurance products and services available via the electronic services of ING and, more specifically, the Transactions available via these services, 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 and the Special Regulations for Trading on Financial Instruments, or with regard to the other companies of the ING Group or insurers external to the ING Group, the applicable regulations of such companies. These Transactions are proposed as such via the /ING Banking services, 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 Banking Software or ING Banking Database provided it designed them, or in the choice of the ING Banking Software or ING Banking Database 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 installing, accessing, downloading or using the ING Banking Software and ING Banking Database 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 Banking services 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.

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, for other companies of the ING Group, for insurers external to the ING Group or for third parties, from any use, whether improper or otherwise, of the ING Banking by third parties using access and signature means of a User. This provision does not prejudice point 8.2. of these General Conditions.

8.1.6. Except in the event of serious or deliberate transgression of duty on its part or that of its subcontractors 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 Banking, services 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, terminals or computer, telecommunications or broadcasting equipment not approved by ING.

For this point 8, devices, networks, terminals 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 subcontractors (unlike, for instance, the Card Reader supplied by ING), and
- Which are not specifically designated by ING as approved by it, or

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 Banking services 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 Banking Software of ING or "jailbreaking" of the Mobile IT System carried out by the Client, the User or by third parties, and not approved by ING
- 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 the ING Banking services, 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, terminals or equipment not approved by ING.

8.1.7. Unless otherwise provided in the Agreement, when ING has to call on third parties to carry out Orders, it undertakes to send them the Orders as quickly as possible. ING cannot under any circumstances be held liable for the detrimental

consequences of any negligence or error by the third parties in question.

ING cannot be held liable in the event of the sending or execution of the Client's Orders is delayed or hindered by circumstances beyond its control.

8.1.8. 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, downloading, activating, installing and using the ING Banking services, in particular the ING Banking Software /ING Banking Database provided by ING.

8.1.9. ING ensures the User that ING Banking Software and Database are free of any known virus on the installation date of ING Banking services.

8.1.10. As they are not issuers of access and signature means of the electronic services of ING, the other companies of the ING Group and the insurers external to the ING Group refuse any liability with regard to the consequences associated with the loss or theft of such means, except in the event of serious or deliberate fault on their part.

8.2 Special liability rules with regard to payment transactions

In derogation from points 5.1.2, 8.1.1 to 8.1.3 and 8.1.5 of these General Conditions, but without prejudice to the latter's other provisions describing the obligations and liabilities of the Parties, in particular points 5, 6 and 7 as well as points 8.1.4 and 8.1.6 to 8.1.10, the liability of the Parties in the event of non-execution or incorrect execution of a Payment Transaction or in the event of an unauthorised Payment Transaction is determined in accordance with the following provisions.

8.2.1. Liability in the event of a Payment Transaction not executed, improperly executed or delayed

8.2.1.1. Payment Transactions covered by the Special Regulations for Payment Transactions (with exceptions, the Special Regulations for Payment Transactions apply to the following Payment Transactions : 1) Payment Transactions in euros or in the currency of a Member State of the European Economic Area (hereafter the

'EEAA²'), and carried out within the EEA³); 2) Payment Transactions carried out within the EEA in the currency of States which are not part of the EEA; 3) Payment Transactions – in any currency – originating from or destined for a State located outside of the EEA, but only with regard to the parts of the Payment Transaction which are carried out within the EEA)

The respective liability of the Parties in the event of non-execution, incorrect execution or delayed execution of the Payment Transactions covered by this provision is determined in accordance with Articles 16 to 18 of the Special Regulations for Payment Transactions. For the application of these provisions, a Payment Order is only considered to have been given by the User once the latter has received electronic, written or telephone confirmation from ING of the receipt of his/her Order sent via the ING Banking services.

Furthermore the previous provisions do not prejudice Article 2.2 of the Special Regulations for Payment Transactions.

8.2.1.2. Payment Transactions not covered by the Special Regulations for Payment Transactions

In the event of non-execution or incorrect execution of Payment Transactions not covered by the Special Regulations for Payment Transactions ING can only be held liable in the case of serious or deliberate transgression of duty on its part.

If any information (e.g. the name and/or address of the payee of the Payment Transaction) is not supplied in addition to the Unique Identifier defined in point 1.2, 29°, ING is only liable for the execution of the Payment Transaction according to the Unique Identifier indicated, without having to take into account any discrepancies between such additional information and the Unique Identifier indicated.

For the application of the above provisions, a Payment Order is only considered to have been given by the User once the latter has received electronic or telephone confirmation from ING of the receipt of

his/her Order transmitted via the ING Banking services.

Whatever the case, ING can only be held liable for the direct loss established by the Client, to the exclusion of any indirect loss such as, but without restriction, the loss of data, loss of earnings, loss of profit, projected opportunity, clients or savings, the costs for procuring an equivalent service or product or loss of reputation.

8.2.1.3 BC/MC Mobile Payment Transactions covered by the ING debit card General Terms and Conditions

The respective liability of the Parties in the event of non-execution or incorrect execution of BC/MC Mobile Payment Transactions is determined in accordance with Articles 9 and 10 of the General Terms and Conditions of the ING debit card.

For the application of these provisions, a BC/MC Mobile Payment Order is only considered to have been given by the User once the latter has received electronic confirmation of the receipt of his/her Order sent via the BC/MC Mobile function included in the ING Banking services.

8.2.2. Liability in the case of unauthorised Payment Transactions through the ING Banking services

8.2.2.1. Whatever the currency of the Payment Transaction, the liability of the Parties with regard to unauthorised Payment Transactions through the ING Banking services is determined in accordance with the following provisions, whether the Payment Transaction is carried out within or outside the EEA.

8.2.2.2 Liability of the Client

8.2.2.2.1. The Client shall be liable for losses arising from the loss, theft, misappropriation or any unauthorised use of the ING Banking, access and signature means (except when an electronic pen is used as means to sign for the latter services) of the Client or the User until notification by the Client or the User as stipulated in point 6.4, sub-paragraphs 1 and 2 of these General Conditions.

However, his/her liability is limited to a maximum amount of 50 euros for all Payment Transactions

² On 1 September 2018, the EEA included, in addition to the Member States of the European Union, Norway, Iceland and Liechtenstein.

³ Both the payment service provider of the principal and the payment service provider of the beneficiary must be located in the EEA.

carried out prior to the said notification, unless such losses result from the fact that the Client and/or the User did not meet, deliberately or due to serious negligence, one or several obligations incumbent upon him/her pursuant to these General Conditions. In that case, the ceiling of 50 euros does not apply. Gross negligence is considered in particular as:

1° the fact, for the User, of writing down his/her password, PIN and/or any other strictly personal and confidential authentication code, including the PIN code for, in an easily recognisable form, in particular near his/her (Mobile) computer system, or smart card, on his/her smart card reader, on his/her telephone or even on an item or document the User keeps and takes with him/her;

2° the fact the Client or the User fails to notify ING immediately, as soon as he/she is aware of the loss, theft, misappropriation or any unauthorised use of the ING Banking services access and signature means (except when an electronic pen is used as means to sign for the latter services), in accordance with point 6.4 § 1 and 2 of these General Conditions.

3° the fact the Client or the User fails to notify ING immediately as soon as he/she is aware of the loss, theft, misappropriation or any unauthorised use of his/her Belgian Mobile Identity account as a means of access and signing for the Home'Bank/Business'Bank services, in accordance with point 6.4, § 1 and 2 of these General Conditions.

Furthermore ING wishes to draw the Client's attention to the fact that other actions or behaviour, whether or not they result from non-observance by the Client and/or the User of his/her obligations under these Regulations, could be qualified as gross negligence, according to all the circumstances under which they occurred or happened, as decided the courts and tribunals in the final instance.

For instance, the following could be qualified as gross negligence, according to the circumstances and without prejudice to the assessment of the courts and tribunals:

- The fact, for the User, of not using his/her ING Banking services access and signature means in accordance with the conditions for access and use of the /ING Banking services which are stipulated in the Agreement and within the utilisation limits

agreed with ING, the other companies of the ING Group and the insurers external to the ING Group. Nonetheless, non-observance by the Client or the User of Article 6.4, § 4 or 5 of these General Conditions relating to the obligation to confirm the notification in writing and the obligation to report or file a complaint cannot be automatically qualified as gross negligence per se

- The fact that the User fails to abide by the cautionary advice appended to these General Conditions
- The fact that the User fails to keep his/her ING Banking services access and signature means safe to prevent any misuse by third parties and, for instance, leaves them in a vehicle or place accessible to the public, except, in the latter case, if they are in a locked cupboard or safe. A place accessible to the public is considered to be any place to which others have access, although not necessarily a place open to the public without prejudice to the right of the User to use the services of a payment initiation or account information service provider, the fact that the User allows a third party (including, without any restrictions, his/her spouse, a relative or friend) knowledge of his/her password, PIN and/or any confidential and strictly personal authentication code or to use ING Banking services access and signature means.

8.2.2.2.2. When the Client and/or the User acted fraudulently, the Client shall bear all the losses resulting from unauthorised Payment Transactions carried out both before and after the notification stipulated in point 6.4 of these General Conditions (notwithstanding ING's obligation to do its utmost to prevent any other use of the ING Banking, services access and signature means).

8.2.2.2.3. By way of a derogation from the above provisions, the Client shall not bear any loss in the following cases:

1°The loss, theft or misappropriation of the means of access and signature for the ING Banking, Services could not be detected by the User before payment (referring in particular to cases of forgery of the card, hacking, skimming, etc. of the personalised security credentials, particularly the means of access and signature for the ING Banking Services); however, this exception does not apply if it is established that the Customer and/or User acted fraudulently .

2° The loss was caused by acts or lack of action of an employee or agent of ING or of another ING Group company.

8.2.2.2.4. If the Client is not a Consumer, the upper limit of 50 euros referred to in Article 8.2.2.2.1 does not apply. Consequently, 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 Phone'Bank, Home'Bank/Business'Bank, ING Banking, Extrabranche Mobility and/or e-ID for Branch services access and signature means (including the Belgian Mobile Identity account) (except when an electronic pen is used as means to sign for the latter services) of the Client or the User, except for serious or deliberate error on the part of ING.

8.2.2.3. ING's liability

8.2.2.3.1. Except in the case of fraud, gross negligence or deliberate breach on the part of the Client and/or User of one or more obligations incumbent upon him/her pursuant to these General Conditions, and without prejudice to point 8.2.2.2.4 when the Client is not a Consumer, ING shall cover, above the amount of 50 euros to be borne by the Client, the losses linked to unauthorised Payment Transactions prior to the notification stipulated in point 6.4 of these General Conditions.

8.2.2.3.2. Except in the case of fraud by the Client and/or User, ING shall bear the losses associated with unauthorised Payment Transactions before the notification stipulated in point 6.4 of these General Conditions.

8.2.2.3.3. ING shall bear the losses associated with unauthorised Payment Transactions in the following cases:

1° if the loss, theft or misappropriation of the means of access and signature for ING Banking, Services could not be detected by the User before payment (referring in particular to cases of forgery of the card, hacking, skimming, etc. of the personalised security credentials, particularly the means of access and signature for the ING Banking Services); however, this exception does not apply if it is established that the Customer and/or User acted fraudulently ;

2° if the loss was caused by acts or lack of action of an employee or agent of ING or of another ING Group company.

8.2.2.3.4. In the case of an unauthorised Payment Transaction, ING shall refund the Client without delay with the amount of the unauthorised transaction, by restoring the account debited to the state it would have been in if the unauthorised Payment Transaction had not occurred. The value date of the crediting shall correspond to the value date of the debiting of the initial Transaction. This provision does not prejudice the obligations and liabilities of the Client and User as described in point 6 and point 8.2.2.2.

Similarly, in the cases mentioned in point 8.2.2.3.3 and unless the Client and/or User acted fraudulently, it shall refund the Client with the amount required to restore the account debited to the state it was in prior to the use of the access and signature means forged, hacked or skimmed within the meaning of this provision, under the correct value date. In addition, ING shall refund the Client for any other financial consequences, in particular the amount of expenses borne by the Client to determine the losses repayable, provided the amounts claimed under its liability are established using documentary evidence.

The above provisions do not prejudice point 8.2.2.2.4 when the Client is not a Consumer.

8.2.3. Force majeure

By way of a derogation from the provisions of articles 8.2.1, 8.2.2 8.2.3 and 8.2.4 ING cannot be held liable in the event of force majeure, or when it is bound by other legal obligations stipulated by domestic legislations or the European Union

9. Ceilings of Transactions

9.1. In the context of the electronic services of ING, execution of Transactions is limited to the available account balance (including, where appropriate, the available credits linked to the account) and, where appropriate, to one or more maximum amounts per Transaction type and/or period of time determined jointly by the Client, the User and ING and/or the other companies of the ING Group. These limits may vary according to ING Banking services chosen for

issuing Orders relating to Transactions according to the means of signature itself chosen to that end – in relation to the aforementioned services.

9.2. Within the minimum and maximum amounts set by ING and/or the other companies of the ING Group and communicated to the User, certain applicable ceilings can, at the request of the User or the Client, and in agreement with ING or the other companies of the ING Group, be changed to suit the Client or the User's own requirements. Information in this regard is available from any ING branch or registered offices or, if the account(s) concerned is (are) held at another ING Group company, at the bank where the account(s) concerned is (are) held.

Furthermore, the Client or the User can, within the limit of the above-mentioned minimum and maximum amounts, apply to change certain applicable ceilings in the following cases:

- Following the loss, theft, misappropriation or any unauthorised use of ING Banking services access and signature means.
- In the case of charging up to the account statements of any Transaction carried out without his/her agreement.

Nonetheless, if the Client is a legal entity, the account agents designated as such in the "Management Powers" documents for the relevant account or in the various mandate forms provided by ING as an appendix to the ING Banking Agreement and who are not representatives or agents duly authorised by the Client may only adjust their own ceilings.

9.3. The following ceilings apply to Orders relating to Payment Transactions given via ING Banking services, from accounts opened with ING, unless otherwise agreed upon with ING, in accordance with point 9.2 of these ING Banking Terms and Conditions, those published in the document relating to Transaction limits available on ING's website ("<http://www.ing.be/limits>) or from any ING branch.

9.4. The ceilings applied to other Orders are communicated to the User in connection with the ING Banking Agreement.

Users can always access the ceilings applicable to Orders via the ING Banking. In addition, Users are

always notified if a Transaction cannot be carried out if a ceiling is exceeded.

9.5. ING Banking services offer the possibility of entering Payment Orders which must be signed by one or more additional Users (where the User who

enters the Payment Order does not have powers to sign it alone). In this case, the ceilings set out in this Article 9 do not apply to the Home'Bank/Business'Bank services (including the Belgian Mobile Identity for ING BE services). For the ING Banking services, the ceilings set out in this Article 9 only apply at the time of the first signature of the Payment Order carried out in connection with the ING Banking services, to the exclusion of subsequent signatures.

10. Maintenance of the ING Banking services

10.1. With regard to any technical, operational or functional incident or problem associated with the ING Banking services, in particular those associated with the installation and use of the ING Banking Software and/or ING Banking Database, or with the use of the, ING Banking access and signature means or which might jeopardise the security of such services, the User can call the ING Help Desk .

The Help Desk can be accessed by calling 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 or German.

Users can 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 Banking/ services, associated mainly with correcting any faults or errors in the ING Banking Software, can only be carried out with ING's assistance. Users may not correct or modify ING Banking 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, ING Banking 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 ING Banking services.

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 Banking Agreement, particularly in the context of the use of the ING Banking services, is processed by ING for the purposes of centralising customer management, the management of accounts and payments, granting and managing credits, asset management (investments), brokerage services (in particular insurance and/or leasing), 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, controlling the regularity of Transactions and preventing irregularities.

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.

Data relating to individuals managed by ING intermediaries (independent agents or brokers), including that relating to their financial Transactions, is also processed by ING to ensure compliance by such intermediaries with their legal and statutory (including resulting from a FSMA/BNB circular) or contractual obligations, including any duty of exclusivity towards ING.

Data communicated to other ING Group companies established or not established in an EU Member State, or insurers external to the ING Group on the initiative of individuals, is processed by such companies in accordance with the information on the protection of privacy supplied by such companies.

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 management of payment transactions, in particular: the company equensWorldline SA (Belgium), Swift SCRL (in Belgium), as well as the clearing and settlement institutions for payments (Centre d’Echange et de Compensation ASBL (“CEC”), Systèmes technologiques d’échange et de traitement SA (“STET”));
- for the provision of the card reader (Card Reader): Gemalto SA (established in France);
- for archiving your data in “paper” or electronic format: OASIS Group (in Belgium);
- for payment and account-related Transactions: ING Business Shared Services Bratislava, Slovakia;
- for payment, credit and financial Transactions: ING Business Shared Services Manila, in Manila, the Philippines; - for IT/electronic management (including security): ICT suppliers such as Unisys Belgium SA (established in Belgium), IBM Belgium SPRL (established in Belgium), 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 (established in Belgium and India), HCL Belgium SA (established in Belgium), Cognizant Technology Solutions Belgium SA (established in Belgium), Getronics BV (established in the Netherlands), ING Tech Poland (established in Poland);

- 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 Payconiq payment Transactions, the Payconiq Supplier;
- for Belgian Mobile Identity payment Transactions, Belgian Mobile ID;

- the companies of the ING Group established or not in a Member State of the European Union;
- affiliated insurers outside of the ING Group;
- 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.

In addition, the data collated by ING in its capacity as insurance broker is also communicated to the relevant insurers external to the ING Group involved which are external to the ING Group and are established in a Member State of the European Union (in particular, NN Non-Life Insurance nv, NN Insurance Belgium SA, Aon Belgium SPRL, Inter Partner Assurance SA, AXA Belgium SA, Cardif Assurance Vie SA and Cardif Assurances Risques Divers SA) and any representatives they may have in Belgium (in particular, NN Insurance Services Belgium SA for NN Non-Life Insurance nv) (list available upon

request), provided it is necessary for the purposes of assessing the risk insured and, where appropriate, concluding and managing the insurance contract, marketing their insurance products (except for the sending of advertisements by e-mail), centralising customer management and controlling the regularity of transactions (including the prevention of irregularities). Any private individual may request a list of the relevant insurers external to the ING Group and their representatives in Belgium. Similarly, it may also be communicated to insurance brokers acting as insurance intermediaries for ING.

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; - to the communication of data relating to them which is gathered by ING as an insurance broker for the relevant insurers external to the ING Group and their representatives in Belgium, for the purpose of commercial canvassing ("direct marketing") by such companies; - 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 decisionmaking 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 ING 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-bePrivacyOffice@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.privacycommission.be).

11.2 ING banking services

When the User uses the ING Banking services, the following personal data, called "environment variables", is sent to ING and recorded by ING via the User's browser software:

- The User's TCP/IP address (identification number of the User's computer system on the Internet network),
- The makes and versions of the Mobile IT system used (Android device, iPad, iPhone, iPod Touch, etc.) and his/her operating system,
- The serial number of the Mobile IT system used (UDID),
- The type of Home'Bank services used by the User (Home'Bank or Business'Bank),

- The language used by the User,
- The pages of the ING Banking services viewed by the User.

Such data is processed by ING with a view to taking into account the specific configuration of the User's Mobile 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 Banking services and to ensure that the contents of such services are improved.

If the User uses the fingerprint recognition function (e.g. the IOS Touch ID or Android Fingerprint) or or the face recognition function (e.g.: the iOS Face ID), his/her fingerprint or face is scanned by the Mobile IT system's fingerprint reader or camera and only a confirmation or non-confirmation of validation of the User's fingerprint or face by the fingerprint recognition function or the face recognition function is communicated to ING in the context of the ING Banking services. ING does not therefore see the User's fingerprint or the face itself, or the representation of it recorded by the fingerprint recognition function or the face recognition function. Furthermore, only a request for confirmation of the validation of the User's fingerprint or face, without personal data concerning him/her, is made by ING to the fingerprint or face recognition function. ING does not therefore communicate any of the User's personal data to the fingerprint recognition function or face recognition function.

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 ING Banking 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 Order

carried out by a User using his/her ING Banking, services access and signature means, ING undertakes to provide proof that the Order was authenticated, recorded and booked correctly and was not affected by a technical incident or other failure.

For all Transactions resulting from an Order given via the ING Banking, 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 subcontractors called on by ING .

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 ING Banking services, by electronic message.

12.2 ING banking services

12.2.1. In the context of the ING Banking services, each Order is signed electronically by a User using the signature means possibly provided by ING (such as a Security module; according to the possibilities offered by ING) and by those selected by the User him/herself according to the possibilities offered by ING (such as a secret code, biometrics covering fingerprint and face recognition and/or any other confidential authentication code known only to the

User, according to the possibilities offered by ING) hereafter "the ING Banking Signature Means".

12.2.2. When the Security Module is used for the purpose of electronically signing an Order, the private key contained in the Security File the User created during the initialisation procedure of Security Module is activated by using the ING Banking Signature Means. The result of such activation is recorded in a single file. The Client acknowledges that this file resulting from the use by a person of the signature means in the aforementioned manner constitutes the electronic signature of one of his/her Users who is a holder of the Security File concerned or, if he/she is a User and holder of the Security File concerned, provided such electronic signature is validated by ING's electronic systems and recognised by such systems as originating from the User and that his/her certificate is valid and has not expired or been revoked.

12.2.3. In derogation from points 12.4.1 and 12.4.2 of these ING Banking Terms and Conditions, for certain orders executed using ING Banking services and specified in the Technical Documentation relating to the use of ING Banking (for instance, Payment Orders in favour of other accounts of which the Client is the holder and/or of agent), the Client acknowledges that simple validation of the order, without recourse at such time to the ING Banking Signature Means, by a person duly authenticated beforehand as a User, in accordance with point 5.4 of these ING Banking Terms and Conditions, via his/her means of access when accessing ING Banking services, constitutes the electronic signature of this User who is the holder of the relevant Security File or if he/she is the User and the holder of the relevant Security File, 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 his/her certificate is valid and had not been revoked.

12.2.4. For all Transactions carried out in the context of ING Banking services, the Client accepts that the electronic signature, as defined in points 12.2.2. or 12.2.3 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 signed document by the civil the Civil Code and that an electronic Transaction with such electronic signature has the same evidential value as

a written Transaction 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 Transactions signed electronically by the User and received by ING via ING Banking services constitute valid and sufficient proof of his/her agreement on the existence and content of the Transaction concerned, as well as the consistency between the content of the Transaction as transmitted by the User and the content of the Transaction as received by ING.

13. Lists of charges – value dates

13.1. The charges for using the /ING Banking/ 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 Banking services.

They are also provided to the Client prior to the conclusion of the ING Banking, 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 Banking services subscription form or refer to the contractual documents mentioned in point 4.1.2. in these ING Banking 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 ING Banking services and, then, on each anniversary date of the Agreement.

13.2. The lists of charges for banking or insurance products and services available via the ING Banking services and, in particular, the lists of charges for Payment Transactions and Transactions on Financial Instruments available via these services are indicated either, with regard to products and services provided by ING, in the lists of charges and rates (Lists of Charges applied to the main banking operations for private individuals or companies, the main securities Transactions, interest rates on ING savings certificates, etc.) published by ING and available, notably, at any ING branch and/or via the ING Banking services, or, with regard to the products and services provided by another company of the ING Group, in the lists of charges published by the latter

and available, notably, from such company and/or via the ING Banking services. Such lists of charges and rates are only valid as from the date they are published. They do not constitute an offer to enter into a contract from ING or other ING Group companies unless they are communicated to the Client in a subscription form for the product or service concerned

13.3. Subject to any application of a separate charge for automated Transactions, the execution of Transactions resulting from Orders submitted via ING's electronic services is subject to the charging policy applicable to such Transactions.

13.4. The Client authorises ING to automatically debit the reference account designated in the ING Banking/ Agreement with all the fees applicable under the charging policy in effect, for the use of ING's electronic services.

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 a minimum of two months or, if the Client is not a Consumer, a minimum 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's electronic services, 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.

13.5. 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 Banking services are at the Client's or User's expense.

13.6. When the Client is the Payee of a Payment Transaction, the credit value date shall correspond to the bank working day during which the amount of the Payment Transaction is received by ING. If the funds are received on a non-bank working day, the value date shall correspond to the next bank working day.

When the Client or the User acts as the payer of a Payment Transaction, the value date of the debit shall correspond to the time when the Transaction amount is debited from the account.

14. User licence for the ING Banking software and Home'Bank / Business'Bank / ING Banking database / Payconiq In App Services

Without prejudice to the provision of the /ING Banking 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 the / ING Banking Software and the ING Banking Database, as well as all its components, in particular, but not limited to, texts, illustrations and other elements appearing in the ING Banking Software and/or in the ING Banking Database.

14.1 ING banking software

14.1.1. For the duration of this Agreement, the User is granted a strictly personal, non-exclusive and nontransferable licence to use the ING Banking 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 install the ING Banking Software for 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 Banking 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 Banking 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, transmit or store the ING Banking Software required to enable the User to use the ING Banking Software in accordance with its purpose. Copying the code and translating the form of the code for the /ING Banking 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 Banking 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 Banking Software shall not be communicated to the User.

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

14.2. ING banking database

14.2.1. For the duration of this Agreement, the User has a strictly personal non-exclusive, nontransferable license for use of the /ING Banking database.

However, no property rights or intellectual rights are transferred to the User. This license provides only the right to install the ING Banking 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 Banking database is strictly prohibited.

Similarly, repeated and systematic extractions and/or reuse of insubstantial portions of the content of the ING Banking database are not authorised when they are contrary to normal use of the ING Banking 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 Banking Software and /ING Banking 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 or the concerned insurers external to the ING Group.

14.4 Payconiq In App service

Notwithstanding article 14.1 and 14.3. , the user is granted a limited, strictly personal, revocable, non-exclusive, non-sublicensable and non-transferable licence to use Payconiq in app services, including future updates, and use it in accordance with these Terms and Conditions.

The User may not alter, copy, distribute, transfer, display, publish, sell or grant a licence to use Payconiq In app Services . No license or rights are granted

to the user by implication or otherwise, except for the license and rights expressly granted to you.

If you do not comply with any of the above requirements and/or restrictions, or if you delete your account, all

rights granted to you in relation to the licence cease to have effect.

All intellectual property rights regarding Payconiq In App Services are

exclusively owned by the Payconiq Supplier and/or our the Bank.

15. Hypertext links for the ING Banking services

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 Banking services to thirdparty 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 Banking services. 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. Chat

ING provides ING Banking users the possibility to send message via 'Chat' within certain timeframe based on technical and human capabilities, all defined by ING. ING can use artificial intelligence (chatbot) to automatically respond to some request sent via 'Chat'.

Users should never divulge their card number or access credentials (whether online banking credentials or debit card PIN) when using the 'Chat' feature. ING will never ask you to provide these details.

This 'Chat' functionality can be used for support on ING products or ING online channels.

Users bear responsibilities and consequences of :

- their usage of the 'Chat' feature through the questions asked or the request sent.
- the security and improper use of the device on which the 'Chat' feature is used

ING can end the 'Chat' session at any moment if

- Messages sent from user are considered as disrespectful or inappropriate
- For security reason

Users have no right of action against ING for any adverse consequences or loss/damage they might suffer as a result of using the 'Chat' feature or information received through that service.

'Chat' conversations are saved and can be used for training and quality purposes and in case of a legal dispute.

18. Availability of the ING Bankingservices

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

18.2. However, ING does not undertake to provide continuous, uninterrupted and secured access to the, ING Banking, services.

Moreover, ING reserves the right, without being obliged to compensate the Client, to interrupt access to all or some of the ING Banking 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 to ING Banking services, 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 in ING Banking services 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 the ING Banking services, including integrated 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 block the use of the card or to withdraw it, 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.

19. Duration of the ING Banking, Agreement - De-activation of the services and Termination of the Agreement

19.1. The ING Banking Agreement comes into force on the day the ING Banking Agreement is signed by the Parties in accordance with point 4.1.2. of these ING Banking Terms and Conditions and is concluded for an indefinite period until its termination. Once activated in accordance with point 4.1.3. of these ING Banking Terms and Conditions, the ING Banking services 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.

19.2. The Client may terminate the ING Banking Agreement and/or deactivate the ING Banking services, for him/herself and/or his/her Users, at any time, free of charge and without providing any justification. Users designated as agents in the "Management Powers" documents (electronic or otherwise) or in the various mandate forms (electronic or otherwise) ING provides as an Annex to the ING Banking Subscription Contract, with the exception of duly authorised representatives and agents, may also deactivate only their own ING Banking services 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 follow the special procedure for blocking the means of access and signature set out in these ING Banking Terms and Conditions at the same time as the termination and deactivation procedure.

However, the Agreement may only be terminated subject to simultaneous closure of the accounts and termination of the contracts with ING and other ING Group companies that may be accessed via ING's electronic services and which, where appropriate, may be managed via these services. Otherwise, it is only possible to deactivate the ING Banking/ services for the Client him/herself and/or his/her Users, without prejudice to the requirement to follow the procedure for blocking ING's electronic services means of access and signature in accordance with the provisions of point 6.4 or 6.6. of these ING Banking Terms and Conditions.

The Technical Documentation on use of ING's electronic services may, where appropriate, specify other terms, conditions or procedures for deactivating the ING Banking services. The Client undertakes to comply with these terms, conditions and procedures in any event.

Deactivation of the ING Banking services also implies cancellation of the subscription to the ING Banking services concerned, accordingly. In addition, deactivation of the Home'Bank/ Business'Bank services or cancellation of the Home'Bank/ Business'Bank subscription shall automatically result in deactivation of ING Banking but not vice versa.

If the Client or his/her Users subsequently wish to reactivate the ING Banking/ services, he/she is obliged to notify ING in advance in accordance with the terms, conditions and procedures specified in the Technical Documentation on use of ING's electronic services or in another way, at ING's discretion.

19.3. Both ING and any other ING Group company or insurer external to the ING Group may terminate the ING Banking Agreement and/or deactivate the ING Banking services 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, but also in the context of the relationships between the Client and the Other ING Group companies and/or Insurers external to the ING Group, whereby ING acts for and on behalf of such companies. Termination by Another ING Group company ends the ING Banking Agreement with regard only to its relationship with the Client, but not with regard to relationships between the Client and ING and between the Client

and the other ING Group companies and/or the other insurers external to the ING Group not concerned.

Likewise, without prejudice to any applicable public order or imperative legal provisions, ING or any Other company of the ING Group may, at any time and without notice, terminate the ING Banking/ Agreement or suspend execution of all or part and/or deactivate, for him/herself and or his/her Users, ING Banking services if the Client and his/her Users seriously fail to honour their commitments with respect to ING or any other company of the ING Group or insurer external to the ING Group 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, as well as any other ING Group company or insurance company external to the ING Group, can also, at any time and without notice, terminate the Phone'Bank/Home'Bank/Business'Bank/ING Banking services Agreement and/or deactivate for the Client him/herself and or his/her Users the ING Banking services in the event of an end to the contractual relationship relating to their respective products and services available via the ING Banking services. In this case, the ING Banking Agreement may only be entirely terminated by ING or any Other companies of the ING Group or Insurance companies external to the ING Group 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 Banking services and which, where appropriate, may be managed via these services. Otherwise, termination by ING, Another ING Group company or an Insurer external to the ING Group terminates the ING Banking Agreement as regards only its relations with the Client, but not for the purpose of the other relations between the Client and ING and between the Client and other ING Group companies and/or the other insurers external to the ING Group which are not involved. In this case again, deactivation for the Client him/herself and/or his/her Users of the ING Banking services by ING, another ING Group company or an insurance company external to the ING Group only concerns its own relations with the Client, and not other relations between the Client and ING and between the Client and other ING Group companies and/or other insurers external to the ING Group which are not involved.

Furthermore, the above provisions do not prejudice the procedure for blocking the ING Banking services

means of access and signature in accordance with point 7.4 of the ING Banking Terms and Conditions, and interrupting access to ING Banking services in accordance with point 17.3. of the ING Banking Terms and Conditions, and the legal provisions requiring the Bank to take special measures in the event of exceptional circumstances.

19.4. In the event of termination of the ING Banking Agreement or deactivation of the ING Banking services, the Client acting in his/her capacity as a Consumer is entitled to a refund of the annual fee

mentioned in point 13.1 in proportion to the time left to run, from the month following that during which the Agreement was terminated or the services were deactivated.

19.5. In the event of termination of the ING Banking Agreement, suspension of the execution thereof or deactivation of the ING Banking services, the Client remains obliged to honour Transactions resulting from an Order given via the ING Banking services before the termination of the Agreement.

Appendix 1 : Cautionary advice for accessing and using the ING Banking services

General security advice ING banking

- Print out or request a print-out or, if the possibility is offered, communication through electronic channels of confirmations of the Transactions you carry out via ING Banking services and keep them. Also keep the electronic or written confirmations of the execution or non-execution of your Transactions.
- Always check your bank account statements and breakdowns. Notify your bank immediately of any anomalies.
- When using ING Banking services, 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 for the PIN code for ING Banking

- Memorise your PIN code for the ING Banking services as soon as it has been generated, and do not write it down anywhere.
- When you choose your ING Banking Pin, avoid combinations which are too obvious (for example, part of your birth date, your town's postcode, the first four digits of your phone number, your

surname or first name or that of a family member, etc.).

- Choosing the same PIN for all of your cards and/or all of your access and signature means involves obvious risks.
- Your ING Banking PIN must remain secret: without prejudice to your right to use the services of a payment initiation or account information service provider who is duly authorised for this activity, do not divulge it (them) to anyone, not even a family member or friend, and certainly not to a supposedly well-intentioned third party.
- No-one has the right to ask you for your PIN code for ING Banking services. 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 Banking anywhere, even in code form, for example, by disguising it (them) as a fake phone number.
- Use the ING Banking services in places where discretion is guaranteed away from prying eyes. Likewise, always create and/or enter your ING Banking 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, card reader keypad or computer keyboard. Do not allow anyone to distract you and, if this is the case, never enter your PIN for ING Banking. If you become aware of unusual circumstances, inform your bank immediately in accordance with Article 6.4 of the ING Banking Terms and Conditions.
- If you have good reason to believe that your PIN code for ING Banking is no longer confidential, change it (them) immediately. If you are not able to change your ING Banking PIN, alert your bank immediately in accordance with Article 6.4 of the ING Banking Terms and Conditions.
- Only activate the fingerprint recognition function or face recognition function for the ING Banking services on a Mobile electronic system of which you are the sole user and only record your own fingerprints or face on this same Mobile electronic system.

Specific guidance relating to the fingerprint recognition function (e.g. the IOS Touch ID from Apple or Android Fingerprint) or the face recognition function (e.g.: the iOS Face ID) for the ING Banking services:

Appendix 2: The "ING Zoomit" service of the Home'Bank/Business'Bank/Smart Banking/ING Banking services Regulation

1. Purpose of the "ING Zoomit service" Regulations

The purpose of the ING Zoomit service of the Home'Bank/ Business'Bank/Smart Banking/ ING'Banking (hereafter the "Regulations") is to describe the Codabox Zoomit service offered by ING, within the scope of ING's Home'Bank/ Business'Bank/Smart Banking/ ING'Banking, under the name "ING Zoomit", as well as to determine the rights and obligations of the Client, the User and ING within the scope of such service.

2. Terminology used in these Regulations

1. The **definitions** summarised in Article 1.2 of the General Terms and Conditions of Home'Bank/ Business'Bank/Smart Banking/ING'Banking (included as an appendix to the General Regulations governing ING Transactions) are applicable to these Regulations.

For the application of these Regulations, the term "Transaction", defined in Article 1.2 of the "Terms and Conditions" of Home'Bank/ Business'Bank/Smart Banking/ING'Banking service, must be understood as the consultation of Electronic Documents using the ING Zoomit service.

2. In addition to these definitions, the following **terminology** is used in these Regulations:

The ING Zoomit service: all services offered by ING using the name ING Zoomit and described in Article 4 of these Regulations.

An Electronic Document: any electronic document, which may or may not contain financial data (e.g. invoices, credit notes, payslips, direct debit instructions, etc.) issued by an Issuer and made available via the ING Zoomit service, in whole or in part, to the Main Recipient and, where applicable, the Secondary Recipient according to the provisions laid down in these Regulations.

Electronic Documents contain, in some cases, standing orders for which the execution request (by transfer), filled in previously by ING with data from Electronic Documents sent by the Issuer, may be actioned via the ING Zoomit service.

The Sender: the legal entity or individual person which has agreed an 'Sender' contract with Codabox

for the Codabox Zoomit service, which is the Issuer of Electronic Documents and which makes these available, in whole or in part, to

the Main Recipient, and where applicable, the Secondary Recipient via the ING Zoomit service.

The full list of senders is available at the website www.zoomit.be/en/senders/

The Main Recipient: the User (individual person) of Home'Bank/ Business'Bank/Smart Banking/ING'Banking services,

- who acts and subscribes to the ING Zoomit service as a Customer, in their own name and on their own behalf,
- And/or who acts for, and subscribes to, the ING Zoomit service, if applicable, as a body or agent, acting in the name of and on behalf of the (Customer) individual person(s) or legal entity(ies), who may designate it as a User, according to the Terms and Conditions for Home'Bank/Business'Bank/Smart Banking ING'Banking services, and who may have authorised it to use Home'Bank/Business'Bank/Smart Banking ING'Banking services in their name and on their behalf,
- And for whom the Electronic Documents available via the ING Zoomit service are intended following a successful Compliance Test, according to the provisions of these Regulations.

The Secondary Recipient: the User (the User (individual person) of Home'Bank/ Business'Bank/Smart Banking/ING'Banking services who accesses and uses the ING Zoomit service in the name of and on behalf of the Customer who is authorized by the Main Recipient, in accordance with Article 6.1 of these Regulations, to consult and to manage via the ING Zoomit service, the Issuer's Electronic Documents intended for the Main Recipient and made available via the ING Zoomit service in accordance with the provisions of these Regulations.

Codabox: Codabox SA/NV, Diestsepoort 1, 3000 Leuven, Brussels Trade Register (RPM/RPR), VAT BE 0840.559.537. Codabox is a third company, acting as an Internet service provider and the Codabox Zoomit

service (including as regards the execution of the Compliance Test), which the Parties call on to supply the ING Zoomit service and, within this framework, transmit secure electronic data. Codabox acts as a subcontractor both in the name of and on behalf of the Issuers and ING.

Full Compliance Test: the comparison carried out by Codabox between, on the one hand, ING Customer's first names, last names and account numbers of the individual persons or legal entities sent to Codabox by the Issuers of the Electronic Documents, with a view to making available to the Main Recipient and, where appropriate, the Secondary Recipient via the ING Zoomit service, those Electronic Documents concerning the Main Recipient in the event of compliance between first names, last names and account numbers, in accordance with the provisions of these Regulations.

The Full Compliance Test is carried out by Codabox when a User wishes to consult an Electronic Document made available via the ING Zoomit service.

The Basic Compliance Test: the comparison carried out by Codabox between, firstly, ING Customer account numbers sent to Codabox by ING and, secondly, the account numbers of those individual persons or legal entities sent to Codabox by the Senders of the Electronic Documents.

The Basic Compliance Test is carried out systematically by Codabox at all times when a User accesses the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services, even in the absence of a request by said User to consult an Electronic Document made available via the ING Zoomit service.

3. Applicable legal framework

1. These Regulations exist in addition to ING's "General Transaction Regulations" and ING's General conditions of the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services (appended to ING's General Regulations), as well as the "Special Regulations for Payment Transactions" and are an integral part of the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services agreement signed in the name of and on behalf of the Customer.

Moreover, the technical documentation relating to the use of ING Zoomit comes in addition to the Technical Documentation relating to the use of the Home'Bank/ Business'Bank/Smart

Banking/ING'Banking services and is an integral part of the ING General Conditions Agreement signed in the name of and on behalf of the Client.

2. Except insofar as these Regulations expressly override this, the provisions of the "General Terms and Conditions of the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services, ING's "General Regulations" wholly in application as regards the ING Zoomit service.

Accordingly, unless an express provision is made to the contrary in these Regulations, the Main Recipient or, where applicable, the Secondary Recipient may access and use the Zoomit ING service under the same conditions and according to the same procedures as those defined in the General Terms and Conditions of the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services. Furthermore, unless an express provision is made to the contrary in these Regulations, the rights and duties of each party (particularly in terms of security) as well as their responsibilities with regard to access and use of the Zoomit ING service, specifically in the event of theft, loss or abusive use of the means of access and use of Home'Bank/ Business'Bank/Smart Banking/ING'Banking services, proof of consultation, maintenance and availability of the Zoomit service remain governed by the General Terms and Conditions of the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services.

3. Except insofar as the technical documentation relating to the use of Zoomit ING expressly overrides this, the provisions of these Regulations, of the technical documentation relating to the use of Home'Bank/ Business'Bank/Smart Banking/ING'Banking services, of the "General Terms and Conditions of Home'Bank/ Business'Bank/Smart Banking/ING'Banking services" and ING's "General transaction Regulations" remain wholly applicable to the Zoomit ING service.

4. Purpose of the ING Zoomit Service and liability of the parties

1. The ING Zoomit service is an integral part of ING's the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services as defined in Article 2.3 of the General conditions of Home'Bank/ Business'Bank/Smart Banking/ING'Banking services.

With the Zoomit ING service, the Main Recipient and, where applicable, the Secondary Recipient, when necessary, consult in a secure manner and in line

with the provisions of these Regulations, all or part of the Electronic Documents made available by Issuers which are linked to the financial data of the Main Recipient as held by ING. Electronic Documents are stored on the Issuers' server or on that of a third party designated by the Issuer. These are made available, in full or in part, to the Main Recipient and, where applicable, to the Secondary Recipient, through the Zoomit ING service by automatic inclusion, following the successful conclusion of the Basic Compliance Test, of a note on the account in question to which the Electronic Document in question is linked via a secure hyperlink. Through the ING Zoomit service, the Main Recipient and, where applicable, the Secondary Recipient can additionally request the execution of standing orders linked to the Electronic Documents made available to them by the Zoomit ING service, in line with the provisions in these Regulations. Standing order execution requests are filled out, in this case, beforehand by ING using data from the Electronic Documents sent by the Issuer. ING only accepts an obligation of diligence which is strictly limited to making Electronic Documents available through the Zoomit ING service (including as regards the execution of the Full Compliance Test) and to the prior completion of 3 standing order execution requests.

ING can consequently only guarantee that the Electronic Documents will be available in a continuous, secure and uninterrupted manner through the Zoomit ING service. ING calls on the services of Codabox to offer the Zoomit ING service, whereby Codabox acts as ING's subcontractor.

ING does not represent Issuers in any way and does not guarantee either their solvency or their honourable nature.

More information concerning the Zoomit ING service (including as regards the Full Compliance Test) can be obtained online at the www.ing.be/Zoomit website.

2. All Issuers other than ING or Codabox remain solely responsible, with the exception of ING or Codabox, for the decision to make available Electronic Documents which they have issued and which are made available through the Zoomit ING service, as well as the time, the form, the frequency and the duration for which said Electronic Documents are made available, along with their content (including accuracy, precision error-free nature, exhaustive nature, quality, and updating), unless gross negligence or wilful misconduct occurs on the part of ING or Codabox.

They alone are free, with the exception of ING or Codabox, to change the time, form, frequency, duration and content of those in Electronic Documents which they have issued, even after they have been made available through the Zoomit ING service, where applicable according to the procedures defined in the contract agreed between the Recipient and the Issuer according to Article 5 of these Regulations.

Any disputes or claims relating to the time, form, frequency, duration of availability, and contents of the Electronic Document as well as any lack of availability of said Electronic Documents must be handled directly with the Issuer in question.

3. Electronic Documents coming from any sources which are external to ING and Codabox, i.e. coming from Issuers other than ING or Isabel, are made available, in whole or in part, to the Main Recipient and, where applicable, the Secondary Recipient, by ING faithfully through the Zoomit ING service, without appraisal or checking on the part of ING or Codabox. They are made available via the Zoomit ING service by hyperlinks which are sent to the User faithfully by ING with the data sent by the Issuer, without appraisal or checking on the part of ING or Codabox. In the same way, any standing order execution requests linked to these Electronic Documents are faithfully completed beforehand by ING via the Zoomit ING service with data sent by the Issuer, without appraisal or checking on the part of ING or Codabox.

Any Electronic Document from Issuers other than ING or Codabox, including data from standing orders linked to these Electronic Documents which are completed beforehand in standing order execution requests, along with hyperlinks to which the Electronic Documents are linked, are made available without any guarantee on the part of ING or Codabox, nor any responsibility for the aforesaid, except in the event of gross negligence or wilful misconduct on their part.

In particular, the accuracy, precision, error-free nature, exhaustive nature, quality and updating of the Electronic Documents, including the aforementioned data for standing orders linked to be Electronic Documents and hyperlinks to which the Electronic Documents are linked cannot be guaranteed by ING or by Codabox, nor can the consequences of any errors that they may include be attributed to them, except in the event of gross negligence or wilful misconduct on their part.

Neither ING nor Codabox can provide any guarantee

whatsoever, nor can they commit to any responsibility except in the case of gross negligence or wilful misconduct on their part, as regards the hyperlinks via which the Electronic Documents sent by Issuers other than ING or Codabox, and in terms of servers and/or websites, in particular their content or their security, to which said hyperlinks are associated and on which these Electronic Documents are stored. Accessing and using these websites and/or servers belonging to Issuers other than ING or Codabox or third parties designated by them, is performed solely at the risk of the User. The User is well aware that these websites and/or servers may offer a level of security which is different to that of Home'Bank/ Business'Bank/Smart Banking/ING'Banking services and which is subject to other usage conditions, to other provisions in terms of privacy and/or generally speaking, other rules than those which are applicable to Home'Bank/ Business'Bank/Smart Banking/ING'Banking services. Neither ING nor Codabox is responsible for the respect by Issuers other than ING or Codabox of the legislation and Regulations in force, unless gross negligence or wilful misconduct occurs on their part. In this respect, they are specifically not responsible for the content of Electronic Documents insofar as they have no effective knowledge of any illicit information or activity relating to said Electronic Documents or with respect to civil damages proceedings, deeds or circumstances which could highlight the illicit content of the activity or information. ING commits to act promptly as soon as it becomes aware of such knowledge or as soon as it is contacted by an administrative or legal authority, in order to remove the hyperlink to which the Electronic Documents concerned are linked or to make access to said Document impossible. ING also commits to tell the public prosecutor immediately about any activity or illicit information, as soon as ING becomes effectively aware of such activity or illicit information relating to an Electronic Document.

The Main Recipient and where applicable the Secondary Recipient, each remains wholly responsible for the use they make freely of Electronic Documents and the consequences of such use. In the same way, they each remain wholly responsible for the use that they make freely of standing order execution requests which are completed beforehand by ING with data from the Electronic Documents sent by the Issuer. It is down to each of them to check the aforementioned data, and if need be to rectify it.

5. The recipient is obliged to notify ING as soon as he becomes aware of any use whether abusive or not

by an unauthorised third party (including the Main Recipient, the Secondary Recipient of the Zoomit ING service, in particular in the event of consultation of Electronic Documents by a third party who is not authorised to do so by the recipient (e.g. in the event of a compliance failure to the extent agreed upon in line with Article 7) or by the Main Recipient or in the event of consultation by the Main Recipient, the Secondary Recipient of an Electronic Document which is not intended for them. Likewise, the Main Recipient along with, where applicable, the Secondary Recipient, are all obliged to notify ING as soon as they become aware of any use whether abusive or not by an unauthorised third party (including the Main Recipient, the Secondary Recipient, of the Zoomit ING service, in particular in the event of consultation of Electronic Documents by a third party who is not authorised by the recipient or the Main Recipient to do so, or in the event of consultation by the Main Recipient, the Secondary Recipient of an Electronic Document which is not intended for them.

6. The Main Recipient and, where applicable, the Secondary Recipient accept that the Electronic Documents may appear markedly different from those which are sent in paper form, particularly in terms of colours, contrasts or clarity, and generally speaking, quality. Article 9 headed "Information and advice" in the ING general transaction Regulations, is not applicable to Electronic Documents. **7.** The ING Zoomit service of Home'Bank/ Business'Bank/Smart Banking/ING'Banking services is limited and does not offer all the functionalities available in the Home'Bank/Business'Bank services.

5. ING Zoomit Service subscription or membership

Any access or use of the Zoomit ING service by a User is subject to subscription or membership to ING's Home'Bank/ Business'Bank/Smart Banking/ING'Banking services by this User, as a Customer himself who is the recipient of Electronic Documents or in the name of and on behalf of a Customer who is the recipient of Electronic Documents, or by the Customer who is the recipient of Electronic Documents in the name of and on behalf the entity for whom the User acts. Any subscription or membership of ING's Home'Bank/ Business'Bank/Smart Banking/ING'Banking services presupposes subscription or membership of the Zoomit ING service, including these Regulations. Pursuant to these Regulations, the Customer who is a Recipient of Electronic Documents, authorises access

and use of Zoomit services by any User that he designates (namely the Main Recipient and where applicable, the Secondary Recipient with a view to consulting all or part of these Electronic Documents, according to the provisions laid down in these Regulations.

It is not possible to input a request for access and use of the Zoomit ING service in any other way than the one given previously.

2. Every Issuer has concluded a specific, separate "Issuer" contract with Codabox for the Codabox Zoomit service, if need be on the basis of a contract agreed between the Recipient and the Issuer, in order that the Main Recipient and, where applicable, the Secondary Recipient may consult all or part of the Electronic Documents made available by each of the Issuers concerned via the Zoomit ING service.

Codabox remains free to conclude such an "Issuer" contract with the persons of its choice and for the Document of its choice. Conversely, every person remains free to conclude such an "Issuer" contract with Codabox of their choice and for the Document of their choice.

3. In addition to adherence to these Regulations, the recipient must agree, via the other Home'Bank/ Business'Bank/Smart Banking/ING'Banking services, a separate individual contract with each of the Issuers in order that the Main Recipient, and where applicable, the Secondary Recipient may consult all or part of the Electronic Documents made available by each of the Issuers via the Zoomit ING service. The recipient remains free to conclude such a contract with the Issuers of his choice and for the Electronic Documents of his choice. However, the Main Recipient and, where applicable, the Secondary Recipient or the Main Recipient and, where applicable, the Secondary Recipient, the Authorised User or another User may not consult Issuers' Electronic Documents via the Zoomit ING service until this has been agreed with the Issuers, with the exception of data from the Electronic Documents mentioned in Article 7.5.

Issuers also remain free to make the Electronic Documents available via the Zoomit ING service, and to enter into a contract with the recipient to this end if they wish. They take sole responsibility for this. **4.** The Issuer determines with Codabox, the time from which the fact of making Electronic Documents available via the Zoomit ING service, may or may not replace paper-based communication, insofar as the Main Recipient agreed beforehand that Electronic

Documents could be consulted via the Zoomit service by requesting to consult an Electronic Document from the same Issuer, of the same type and bearing the same Customer number. **5.** Unless it commits gross negligence or wilful misconduct, ING does not bear any responsibility as regards contractual relations concluded between the Issuer and Codabox and, where applicable between the recipient and the Issuers.

6. Appointment of the secondary recipient

1. Only the Main Recipient can designate as a "Secondary Recipient", within the bounds of the possibilities offered by ING, the User of the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services who will be authorised to consult Electronic Documents from Issuers via the Zoomit ING service, intended for the Main Recipient and made available via the Zoomit ING service in line with the provisions contained in these Regulations. The Main Recipient determines for each Electronic Document Issuer, for each Customer number held by each Issuer and for each type of Electronic Document, whether the User of the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services is authorised, as a "Secondary Recipient" to consult the Electronic Documents via the Zoomit service. He determines accordingly the Electronic Documents from which Issuers, the Electronic Documents linked to which Customer number with each Issuer and the Electronic Documents of which type are made available to the Secondary Recipient that he designates through the Zoomit ING service.

2. In the same way, only the Main Recipient can also refuse that the other Users who are authorised to consult the accounts referred to in Electronic Documents, via the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services, be designated as "Secondary Recipients" in such a way that they will not be authorised to consult Electronic Documents from Issuers intended for the Main Recipient via the Zoomit ING service and made available via the Zoomit ING service, subject to Article 7.5. of these Regulations, however.

7. Compliance Test

1. When a User wishes to consult an Electronic Document made available through the Zoomit ING service, a Full Compliance Test is executed by Codabox in the name of and on behalf of ING and the Issuers, on the basis of data sent by the Issuers, in order to ensure that unauthorised

persons cannot consult Electronic Documents. ING is not responsible in the event of a Full Compliance Test failure following incorrect or incomplete transmission of data on the part of an Issuer, of Isabel, of a Customer or of a User.

2. The Main Recipient of an Electronic Document is designated following a successful Full Compliance Test.

The Main Recipient of an Electronic Document thus designated is the User whose last name, first name and account number with ING which he is authorised to consult via the the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services, correspond, according to the agreed level of compliance, to the last name, first name and account number of an individual person sense to Codabox by the Electronic Document Issuers. in the event of compliance between the aforementioned data (that is to say in the event of a successful Full Compliance Test), the Main Recipient thus designated is authorised to consult Electronic Documents from Issuers, via the Zoomit ING service, intended for the Main Recipient and made available via the Zoomit ING service.

The Issuer determines with Codabox in line with Article 5 of these Regulations, where applicable according to the contract agreed between the Issuer and the recipient, the level of compliance applied for the test designed to make the Issuer's Electronic Documents available. Depending on the agreed extent of compliance, the recipient accepts that the Electronic Documents may be consulted through the Zoomit ING service by a Main Recipient and, where applicable, a Secondary Recipient other than him. The Issuer determines with Codabox in line with Article 5 of these Regulations, where necessary according to the contract agreed between the Issuer and the Main Recipient, those Electronic Documents which may or may not be closely linked to their private sphere, or which may or may not be sensitive.

3. The Main Recipient accepts that the Secondary Recipient whom he has designated in line with Article 6 of these Regulations may, following a successful Basic Compliance Test and in the absence of a successful Full Compliance Test (that is to say that there is compliance only between the account numbers, and not between the last and first names), consult, through the Zoomit ING service, the Electronic Documents of Issuers intended for the Main Recipient and made available through the Zoomit ING service, insofar as he has received authorisation, in line with Article 6 previously mentioned, for the Electronic Document Issuer in

question, for the Customer number in question linked to this Issuer and the type of Electronic Document in question.

4. When, in respect of Electronic Documents which are not considered as closely linked to the private sphere (for example water, gas and electricity bills) or which are intended for a legal entity and are not sensitive, a Basic Compliance Test is successful but not the Full Compliance Test in its own right, then the recipient of the Electronic Document accepts, insofar as the Main Recipient did not refuse the designation of other Users as Secondary Recipients in line with Article 6.2., that a User - authorised to consult the accounts referred to in the Electronic Documents via the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services - may in their capacity as an Authorised User, consult in full or in part the Issuers' Electronic Documents, through the Zoomit ING service, intended for the Main Recipient and made available via the Zoomit ING service. insofar as this User enters the "Zoomit" code corresponding to the Electronic Document in question and sent by the Issuer.

A User who acts and subscribes to the Zoomit ING service as a person authorised by another individual or individuals, or a legal entity or entities (Customer(s)) only to consult their accounts, via the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services, in line with the general conditions of the the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services, cannot consult Electronic Documents which are linked to the aforementioned accounts as an "Authorised User".

5. Furthermore, the recipient accepts that all Users who are authorised by him to consult the accounts referred to in the Electronic Documents, through the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services (including (joint) holders or agents for the accounts in question), may, following a successful Basic Compliance Test and in the absence of a successful full Full Compliance Test, still consult the following data from the Issuer's Electronic Documents, via the Zoomit ING service, intended for the Main Recipient and made available via the Zoomit ING service:

- The Issuer's name
- The type of Electronic Document (bill, direct debit, payslip, etc.)
- The date of receipt of Electronic Documents
- Any expiry date of the Electronic Documents

- The status of Electronic Documents (document consulted, new document, document downloaded, etc.)
- Any amount linked to the Electronic Documents
- Where appropriate, the fact that any amounts linked to the Electronic Documents have been paid or not.

These Users may consult this data even if the Main Recipient refused to designate them as Secondary Recipients in line with Article 6.2.

8. Protection of privacy and duty of discretion

1. By subscribing to or becoming a member of the Zoomit ING service, in line with Article 5, the User, in his capacity as a Customer in his own right, or acting in the name of and on behalf of a Customer, and/or the Customer in whose name and on behalf of whom he acts, consents to the exchange and processing of the following data between ING, Codabox and the Issuers within the scope of the Zoomit ING service, in line with these Regulations:

- a) the request made by the Main Recipient, the Secondary Recipient to access and use the ING Zoomit service in line with these Regulations;
- b) data required for the execution of the Full Compliance Test: the last name, first name and account number of the Customer along with,
- c) consultation or non-consultation by the Main Recipient, Secondary Recipient of the Electronic Documents in line with these Regulations;
- d) Electronic Documents, including data relating to direct debits with ING and any payments linked to the Electronic Documents.

2. The above-mentioned Electronic Documents referred to at point 1, c), of this Article 8 are processed by ING and by Codabox acting as a subcontractor for the Issuers of these Electronic Documents, only in the event of a successful Basic Compliance Test and with the sole purpose of making available all or part of the Electronic Documents, via the Zoomit ING services, to the Main Recipient, and where applicable, to the Secondary Recipient, (including the execution of the Full Compliance Test) as well as, where applicable, the execution of standing orders, to the exclusion of all other purposes (for example marketing). Electronic Documents are accordingly processed by ING or by Codabox without either party becoming aware of the content of the data in the Electronic Documents, apart from with regard to the following data:

- the name and account number of the Issuer;
- the last name, first name and account number of the recipients of the Electronic Documents;
- the type of Electronic Document (bill, direct debit, payslip, etc.);
- the date of receipt of the Electronic Documents;
- any expiry date for direct debits with ING and any standing orders linked to the Electronic Documents;
- the status of Electronic Documents (document consulted, new document, document downloaded, etc.);
- any amount linked to the Electronic Documents;
- if applicable, the fact that any amounts linked to the Electronic Documents have been paid or not;
- other data relating to direct debits with ING and any standing orders linked to the Electronic Documents (in particular, data relating to structured communications or free-standing communications from the Issuer).

The data listed in the previous paragraph as well as the data mentioned above in point 1, a), b), c) and e) in Article 8 is processed by ING, who is responsible for processing within the scope of its end-management of accounts and payments, and by Codabox, as an ING subcontractor, with the sole purpose of making available, through the Zoomit ING service, all or part of the Electronic Documents to the Main Recipient and, where applicable, to the Secondary Recipient, (including the execution of the Full Compliance Test) as well as, where applicable, the execution of standing orders, to the exclusion of all other ends (for example marketing).

This data is not communicated to third parties except for the persons designated in point 1 above, and where applicable, companies whose intervention is necessary (in particular, for payment transactions: Swift SCRL, MasterCard Europe SPRL, and so on) in order to undertake the objectives mentioned previously.

3. Any individual person is entitled to inspect the information relating to him/herself.
4. For additional information regarding the data processing undertaken by ING Belgium, all individuals can refer to Article 11 (Protection of privacy) of the

General Regulations for ING's Home'Bank/
Business'Bank/Smart Banking/ING'Banking services.

9. Access and use of the ING Zoomit Service

1. Whenever the User subscribes to or becomes a member of the Zoomit ING service, as a Customer himself, or in the name of and on behalf of all of our Customer, and/or by the Customer in whose name and on behalf of whom key aspects hand, the Main Recipient and, where applicable, the Secondary Recipient, in line with these Regulations, consult all or part of the Electronic Documents made available by the Zoomit ING service by the Issuers and intended for the Main Recipient pursuant to the Full Compliance Test.

Only these persons can consult all or part of the Electronic Documents, with the exception of all other persons.

2. The means of accessing and signing required by the Main Recipient or, where applicable, the Secondary Recipient to access and use the Zoomit ING service, including those necessary to approve electronic signature, are identical to those required in order to access and use ING's Home'Bank/
Business'Bank/Smart Banking/ING'Banking services.

3. The Bank may refuse to process a Zoomit ING service consultation request, with no obligation to give any grounds for said refusal, in particular if the Main Recipient, the Secondary Recipient submits several successive requests which do not fall within the boundaries mentioned in these Regulations or, generally speaking, makes improper use of the Zoomit ING service. All complaints in this regard will be rejected, unless it can be shown that the Bank has been guilty of gross negligence or wilful misconduct.

10. Availability of Electronic Documents

Each Electronic Document is made available via the Zoomit ING service for a minimum timeframe of six (6) months and a maximum of (18) months from the date it is made available by its Issuer through the Zoomit ING service. The aforementioned timeframe is determined, depending on the type of Electronic Document in question, by the Issuer with Isabel in line with Article 5 of these Regulations, where applicable according to the contract agreed between the Issuer and the recipient, on the understanding that this timeframe cannot, under any circumstances, be less than 6 months or greater than 18 months.

The Main Recipient and, where applicable, the Secondary Recipient recognise and accept that: •

the Main Recipient and, where applicable, the Secondary Recipient are themselves responsible for the safeguarding of each Electronic Document, and they commit to this end, to download (save) and/or print out each Electronic Document within the agreed availability timeframe;

- the Electronic Documents will no longer be available after the agreed availability timeframe has expired or as from the effective date of any termination of the Zoomit ING service in whole or in part (with regard to the Issuers concerned), regardless of the reason for termination;
- any Electronic Documents which have not yet been made available during the agreed availability timeframe, will no longer be available as from the effective date of any termination of the Zoomit ING service;
- the availability of Electronic Documents via the Zoomit ING service may have the consequence, according to the contract agreed by the Issuer with Codabox in line with Article 5 of these Regulations, that all or part of these will no longer be sent by other channels (for example, in paper format by post or by fax, or in electronic format by e-mail). Unless it commits gross negligence or wilful misconduct, ING does not take any responsibility as regards the contractual relationships agreed between the recipient and the Issuers.

11. Charges for the ING Zoomit Service

The possible rates applicable to the subscription, membership and/or use of the Zoomit ING service are mentioned in the rates for primary banking transactions published by ING and available, among other places, at all of the ING branches and 8 via the information services of the Home'Bank/
Business'Bank/Smart Banking/ING'Banking services. In addition, they are communicated to the User prior to subscription. These published rates are only valid on the date they are provided. They do not constitute a contract offer from ING unless they are sent to the User in a subscription.

Though rates are applicable to subscription, membership and/or use of the Zoomit ING service, they apply to the Main Recipient in the event of use of the Zoomit ING service by them, or in the event of use of the Zoomit ING service by the Secondary Recipient that he designates. These rates may stipulate, for subscription or membership to the Zoomit ING service, the payment of an annual fee which is then payable and applied to the Main Recipient, as soon as subscription or membership to the Zoomit ING service by the Customer or in his

name and on his behalf, and then, on all anniversary dates of the subscription or membership. The possible rates for the Zoomit ING service are independent of the pricing of the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services.

12. Intellectual Property

1. Without prejudice to the availability of the Zoomit ING service from Codabox within the scope of the Zoomit ING service for the Main Recipient and, where applicable, the Secondary Recipient exclusively for their personal needs as laid down in the Regulations, Codabox reserves all rights in terms of property as well as all intellectual property rights (including usage rights) both in terms of the Codabox software and the Codabox database relating to the Isabel Zoomit service, as well as regarding all the elements which make it up, in particular and not limited to texts, illustrations, brands and other items which can be found in the Codabox software package and/or in the Codabox database.
2. For the duration of subscription or membership to the Zoomit ING service, the User is granted a strictly personal, non-exclusive and non-transferable licence to use the Codabox software relating to Isabel's Zoomit service, in its computer-readable object code version, and to use the Codabox database relating to Codabox's Zoomit service. However, no property rights or intellectual rights are transferred to the User. This licence only grants the right to use the Isabel software and the Codabox database within the scope of the Zoomit ING service in line with its purpose as determined in these Regulations, in particular the consultation of Electronic Documents.
3. It is strictly forbidden for Users to make even the slightest modification to the Isabel software package or to the Codabox database relating to the Codabox Zoomit service.
4. Codabox is the sole holder of the brands and logos linked to the Codabox Zoomit service.

13. Duration and end of the ING Zoomit Service

1. Subscription or membership to the Zoomit ING service by a Customer or on his own behalf comes into force on the day of the subscription or membership and is valid for an indefinite period.
2. Both the User, the Customer and ING may terminate the Zoomit ING service at any time without charge and without justification. The Zoomit ING service is an integral part of ING's Home'Bank services, and the complete termination of the Zoomit ING service is only possible by terminating ING's the Home'Bank/

Business'Bank/Smart Banking/ING'Banking services. Accordingly, without prejudice to the provisions contained in these Regulations, both the User, the Customer and ING may only completely terminate the Zoomit ING service in the same conditions and according to the same procedures as those defined for the termination of the Home'Bank Agreement within the General Terms and Conditions for the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services. At any time, without charge and without justification, the Main Recipient may terminate availability of Electronic Documents via the Zoomit ING service for some or all of the Issuers, by sending a request to this end to the Issuers in question, where applicable according to the contract agreed between the Issuers and the Recipient in line with Article 5 of these Regulations. Each Issuer in question will take such a demand into account according to the conditions and procedures agreed between itself and the Recipient, without ING's responsibility ever being committed in this area, unless there has been gross negligence or wilful misconduct on its part. At any time, without charge and without justification, ING may also terminate with immediate effect, the availability of the Electronic Documents via the Zoomit ING service for some or all of the Issuers. Furthermore, ING may, at any time and without notice, terminate the subscription or membership to the Zoomit ING service or suspend its execution in whole or in part if the User or the Customer fails to honour their commitments in respect of ING or finds themselves in a situation where they are unable to pay, if they are declared bankrupt or put into liquidation or receivership, or they are the subject of similar procedures, without prejudice to any additional damages.

3. Any closure of accounts with ING or termination of ING's the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services agreements to which the Zoomit ING service is linked will immediately terminate use of the Zoomit ING service for the accounts and the ING's the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services agreements in question. If all the accounts held with ING to which the Zoomit ING service is linked are closed, or if all the Home'Bank Agreements to which the Zoomit ING service is linked are terminated, then subscription or membership of the Zoomit ING service will terminate with immediate effect.
4. Except in the event of force majeure or serious failure by the User or the Customer to respect

their commitments in respect of ING, the termination of Zoomit ING services or the withdrawal of the Electronic Documents made available via the Zoomit ING service by ING in line with Article 13.2. will not prejudice the right of the Customer or User to be compensated for any prejudice which may result for them due to this termination as demonstrated by them. Similarly, the User or the Customer can invoke this right if the subscription or membership is terminated by him due to ING changing the contractual framework unilaterally in accordance with Article 14 or due to gross negligence or wilful misconduct on the part of ING, as demonstrated by him.

5. In the event of termination of the subscription or membership of the Zoomit ING service due to a serious failure on the part of the User or the Customer to respect their commitments in respect of ING or termination of the subscription or membership of the Zoomit ING service by the User or the Customer, then ING will not be obliged to reimburse, even partially, the annual fee which may be applicable in line with Article 11 of the Regulations. **6.** If use of the Zoomit ING service is partially terminated with regard to the making available of all or part of the Electronic Documents for some or all Issuers, or if use of the Zoomit ING service is completely terminated, then the Main Recipient and, where applicable, the Secondary Recipient of the Electronic Documents concerned which were made available via the Zoomit ING service are obliged to inform the Issuer concerned of this and to find a solution with them as soon as possible for another mode of communication or method of availability for the future of the Document in question. According to the same conditions, the Issuers concerned by the withdrawal of the Electronic Documents made available via the Zoomit ING service or via the complete termination of the subscription or membership to the Zoomit ING service are not obliged, unless there is a provision to the contrary in any contract agreed between the recipient and the Issuer in line with Article 5 of these Regulations, to communicate or make available in another way after the termination occurs, those Electronic Documents which have already been made available via the Zoomit ING service.

14. Changes to these Rules

1. The Bank reserves the right to change these Rules by giving one month's notice. To this end, ING will inform the User or the Customer, at least one two (2) month before the application of the changes in

question, of the availability of the new Regulations. ING will inform the User or the Customer by mail (electronic or traditional), by a message featured in the account statements or by a notice displayed in ING branches or through the the Home'Bank/ Business'Bank/Smart Banking/ING'Banking services. **2.** The User or the Customer may refuse these changes and, in this case, exercise their right to terminate the subscription or membership to the Zoomit ING service in line with Article 12 of these Regulations. Failure of use, by the User or the client, within a month of the communication stipulated above, of their right to terminate the subscription or membership to the Zoomit ING service, will be deemed as tacit agreement of the User or Customer to adopt the proposed changes.

ING Belgium SA/nv Bank/Lender- Avenue Marnix 24, B1000 Brussels
VAT BE 0403200 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 12381A
Publisher:Philippe Wallez- Cours SaintMichel 60, B1040 Brussels.01/19.