

## Contents

<p><b>A. GENERAL..... 2</b></p> <p>A.1. Language..... 3</p> <p>A.2. Data protection and sub-contracting ..... 3</p> <p>A.3. Settlement of disputes and applicable law ..... 3</p> <p>A.4. Amendment of these General Terms and Conditions ..... 3</p> <p>A.5. Application of the General Terms and Conditions of the Bank and/or of LuxTrust and the Bank's tariff ..... 3</p> <p><b>B. INTERNET ACCESS SERVICE ..... 3</b></p> <p>B.1. Entitlement to Access ..... 3</p> <p>B.2. Extent of the Access..... 4</p> <p>B.3. Right to refuse Access ..... 4</p> <p>B.4. Withdrawal period..... 4</p> <p>B.5. Connection to the Access ..... 4</p> <p>B.6. Recommendations..... 4</p> <p>B.7. Safekeeping of Identification details ..... 5</p> <p>B.8. Description of the services provided ..... 5</p> <p>B.9. Information on the Website ..... 6</p> <p>B.10. Blocking and unblocking Access ..... 6</p>	<p>B.11. Execution of transactions ..... 6</p> <p>B.12. Revocation of a transaction ..... 7</p> <p>B.13. Posting of transactions ..... 7</p> <p>B.14. Delay applied to indexes and quotes ..... 7</p> <p>B.15. Regularisation, securities transaction, and other notices ..... 7</p> <p>B.16. Proof of transactions ..... 7</p> <p>B.17. Restrictions on use ..... 7</p> <p>B.18. Exclusion of liability ..... 7</p> <p>B.19. Mobile Access to the Internet service..... 8</p> <p>B.20. Intellectual property..... 9</p> <p>B.21. Tariffs ..... 9</p> <p>B.22. Termination or suspension ..... 9</p> <p><b>C. REMOTE SELLING ..... 9</b></p> <p>C.1. Request to open an account online..... 9</p> <p>C.2. Object of the sale ..... 9</p> <p>C.3. Essential features of products and services offered online ..... 9</p> <p>C.4. Tariff..... 9</p> <p>C.5. Right of withdrawal ..... 9</p>
---	---

\*\*\*\*\*

**These General Terms and Conditions- Internet and Remote Selling of the Bank apply for those Clients who subscribe to an Internet Access from 02 November 2022.**

**For the other Clients, these General Terms and Conditions- Internet and Remote Selling of the Bank will come into force as two months after notification to the Client by any means of the update to the General Terms and Conditions – Internet and Remote Selling of the Bank, except for Clients who specifically agreed that they could apply before that date.**

The use of the Internet Access which the Bank makes available to its Clients is governed by the following terms and conditions:

## A. GENERAL

### Definitions

The terms set out below are defined as follows for the purposes of these General Terms and Conditions - Internet and Remote Selling:

- **Bank:** ING Luxembourg, Société Anonyme, a credit establishment situated at 26, Place de la Gare at L-2965 Luxembourg, R.C.S. Luxembourg B.6041, VAT LU 11082217, tel. +352.44.99.1, fax. +352 44.99.2310, contactcenter@ing.lu, authorised and regulated by the Commission de Surveillance du Secteur Financier (CSSF), 283, route d'Arlon, L-2991 Luxembourg, [direction@cssf.lu](mailto:direction@cssf.lu), tel. +352.26.25.11,
- **LuxTrust:** LuxTrust S.A., a company incorporated under Luxembourg law, an IT company that in particular provides certification, authentication, and electronic signature services to the public and is regulated as a financial sector professional.
- **LuxTrust General Terms and Conditions:** LuxTrust's contractual conditions in force, such as regular updates by LuxTrust and available on LuxTrust's Website and/or on [www.ing.lu](http://www.ing.lu), which all persons accept when using one of LuxTrust's services (means of identification, registration, authentication, signature and validation) or a Certificate;
- **General Terms and Conditions of the Bank:** the general terms and conditions of the Bank in force, as applicable to the principal cardholder ("General Terms and Conditions of the Bank" for Retail and Private Banking customers, "General Terms and Conditions of Business Banking" for Business Banking customers, and "Wholesale Banking Terms and Conditions" for Wholesale Banking customers), and also applicable to the Cardholder by reference herein- **Client:** each person having an Internet Access or Mobile Access.
- **Internet Access:** the online Banking service via the transactional part of the Bank's Website, as part of an obligation of means, enabling the Client to perform various operations, particularly described in Article B.8. of these General Terms and Conditions - Internet and Remote Selling
- **Mobile Access:** the Online Banking service as part of an obligation of means via an App (iOS or Android) enabling the Client to perform various operations, particularly described in Article B.8. of these General Terms and Conditions - Internet and Remote Selling
- **Access:** Internet Access and Mobile Access
- **Mobile device:** tablets and portable devices compatible with the ING Mobile Application as described on the Website [www.ing.lu](http://www.ing.lu) and in the application stores in which the ING Mobile Application is available.
- **ING Mobile Application ("App"):** IT software enabling electronic transmission of data between the Bank and the Client. It is provided by the Bank in stores where applications can be downloaded, such as Apple Store, Google Play, and application stores officially recognised by the operating system of the Clients' Mobile devices.
- **Website:** ING Luxembourg, as part of an obligation of means, makes available, to the users who want it, the services appearing on the address of its Website. These services might be added to, amended, or withdrawn at any time and without prior notice, particularly depending on technological changes.
- **ing.lu (<http://www.ing.lu>):** the electronic address granting access to the Bank's Website on the worldwide web. The name "ING" is a protected trademark, registered by ING Groep N.V., a company incorporated under the laws of the Netherlands, having its registered office in the Netherlands at Bijlmerplein, 888, 1102 MG Amsterdam.
- **Identification details:** technical means enabling the Client to be identified, as described in Article B.7. of these General Terms and Conditions - Internet and Remote Selling.
- **One Time Password (OTP):** A one-time password generated by the LuxTrust product.
- **Contract number:** a number serving as one of the Client's Identification details containing three letters and three figures (e.g. ABC123) which is shown in the Internet Access Request.
- **Password:** a personal password serving as one of the Client's Identification that can be requested when logging into the transactional part of the Bank's Website.
- **Mobile PIN:** 5-digit PIN code defined by the Client when registering a Mobile device with a view towards securing his Mobile Access.
- **Token:** device (hardware or software) provided by LuxTrust, enabling LuxTrust to provide authentication services.
- **Smartcard:** smart card marketed by LuxTrust accompanied with two certificates (authentication, signature) to authenticate and/or make transactions using an electronic signature.
- **Certificate:** electronic file signed by LuxTrust that can be used for applications other than the Access and which contains information on the Client, in particular his public key.
- **LuxTrust Scan:** electronic device with a screen and a camera function. These makes it possible to scan a QR code containing an operation's data and enabling the generation of a One Time Password (OTP).
- **LuxTrust Mobile:** application can be downloaded on one's Mobile Device from application stores such as Apple store or Google Play. Once registered in the application, it provides authentication services or, as the case may be, it enables generating a One Time Password (OTP).
- **Fingerprint:** a process of fingerprint identification using the application provided by the manufacturer of the Mobile Device.
- **Face ID:** Facial recognition identification method using the application provided by the manufacturer of the Mobile Device.
- **Private certificate:** certificate issued in the name of the Client which may be revoked by the Client according to the procedures established by LuxTrust.
- **Consumer:** a natural person who, in relation to payment service contracts with the Bank, acts in a purpose other than that of his commercial or professional activity.
- **Bank working day:** a bank working day such as defined in the Bank's tariff in force;
- **Durable support:** any instrument which enables the Client to store information addressed personally to him in a way accessible for easy future reference for a period of time adequate for the purposes for which the information is intended and which allows the unchanged reproduction of the information stored, such as DVD-ROMs, CD-ROMs, hard drives of personal computers, etc. on which electronic mail can be stored.
- **Request:** a request for Access.
- **Remote Selling:** any sales contract for financial services and/or products entered into between the Bank and the Customer as part of an online contact, account application, and/or subscription to an online service and/or product offered by the Bank that, for this contract, exclusively relies on one or more distance communication techniques through to the conclusion of the contract, including the conclusion of the contract itself, in particular via it Website.

### A.1. Language

Anyone wishing to subscribe to the Bank's products or services via the website [www.ing.lu](http://www.ing.lu) declares being fluent in at least one of the languages proposed by this site. The languages offered by this site are French, German, and English. The language of the contractual and communication conditions is the language chosen by the Customer from among the languages proposed. In case of any divergence between the French version and the other languages, the French version alone will be taken into consideration.

### A.2. Data protection and sub-contracting

As part of its online banking services, ING carries out personal data processing. This processing is subject to the Bank's General Terms & Conditions.

Without prejudice of the Bank's General Terms and Conditions applicable to the Client, the information transmitted is recorded by ING Bank in an automated file. This is processed for the purpose of identifying and managing access to the e-banking service, account management, account operations, and securities accounts, as well as controlling their consistency.

Access and use of the online banking services also implies transmitting the Customer's personal data to LuxTrust. LuxTrust shall also process the data as the data controller, in accordance with the information on its website [www.luxtrust.lu](http://www.luxtrust.lu).

By the simple fact of authorising the Bank to order authentication material from Luxtrust on behalf of the Client, the Client authorises the Bank to communicate his personal data to LuxTrust who will process them in accordance with LuxTrust's General Terms and Conditions.

In order to offer a high quality internet service and to take advantage of the ING Group's shared infrastructures, the Bank sub-contracts out the infrastructures related to Internet Access and Mobile Access to ING Bank NV, its branches and/or subsidiaries.

In this context certain information concerning the Client or his transactions may be made accessible in a confidential manner to ING Bank NV and/or to its sub-contractors in the Netherlands, Belgium or Poland. For other matters, the Client is referred to the Bank's General Terms and Conditions in force (and in particular, article A. 9 bis "Outsourcing" for Retail Banking, Private Banking and Business Banking clients, and to articles 7 and 8 of the Appendix specific to "Luxembourg" in the "Wholesale Banking Terms and Conditions" for Wholesale Banking clients), and to the appendix on outsourcing services in force.

Depending on the situation, the personal data of the Customer's shareholders and/or agents, as well as the beneficial owners, having access to the online banking service, may be collected and processed by both the Bank and LuxTrust for the purposes outlined above.

The Customer has the right to request access, rectification, deletion, and portability of his personal data. He has the right to oppose their processing or to request a limitation. The Customer may consult and/or modify some of his personal data via his Access.

The Bank may retain personal data for a period not exceeding that necessary for its defined purposes and in accordance with the Terms and Conditions of the Bank applicable to the Client.

For the rest, personal data is processed in accordance with the current Privacy Statement available on the website at [www.ing.lu](http://www.ing.lu) or in the branch offices.

### A.3. Settlement of disputes and applicable law

This contract and the online subscription procedure are governed by Luxembourg law. All existing or future disputes arising as a result of this contract or subscription procedure shall be exclusively heard by the Luxembourg courts in the said geographical jurisdiction.

For out-of-court procedures relating to the settlement of complaints and the existence of guarantee funds, see the Bank's general conditions in force.

### A.4. Amendment of these General Terms and Conditions

Without prejudice to the Bank's right to add a new service at any time, or to bring the Access service or these General Terms and Conditions - Internet and Remote Selling in compliance with any new legislation or regulations, the Bank may not amend these General Terms and Conditions - Internet and Remote Selling except by giving the Client notification of the amendments at least two months before those amendments take effect.

The Client will be notified of amendments by notice provided via the Access service, notices enclosed with bank statements, or by any other form of correspondence (postal and/or electronic) addressed by the Bank to the Client.

These current General Terms and Conditions - Internet and Remote Selling are also available for consultation on the Bank's Website.

If the Client does not wish to abide by the amendments, he must, before those amendments take effect, cancel in writing his Contract of Access to the Internet Service, current account/ and/or financial products and services subscribed to online. Except if otherwise stipulated, the termination shall be free of charge and with immediate effect.

If the Client does not use the right of termination, this shall be taken as the Client's acceptance in full of the amendments.

The new provisions shall apply to future operations as well as to operations commenced before the amendments take effect.

The Bank may also and at any time change all or part of the technical requirements for Access, in particular the Identification elements, with the aim of improving security of the Access service or adapting it to new technological changes. The Client shall be informed of the changes in the manner set out in this article.

The cancellation or invalidity of one of the clauses of these General Terms and Conditions - Internet and Remote Selling shall not under any circumstances cause the cancellation of the other clauses, which remain fully valid.

### A.5. Application of the General Terms and Conditions of the Bank and/or of LuxTrust and the Bank's tariff

For remaining matters, see the Bank's general terms and conditions in force and tariffs applicable to the Client, which are applicable to the extent that there is no exemption in these General Terms and Conditions - Internet and Remote Selling.

The same applies to LuxTrust's products and services, which remain governed only by the LuxTrust General Terms and Conditions in force.

## B. INTERNET ACCESS SERVICE

### B.1. Entitlement to Access

The Client shall in the Request specify the client number(s) to which he wishes to have Access.

A Client may have Access in his capacity as an individual account holder of the client number(s), as a joint account holder, a mandate holder, the client number's account holder's legal representative, or as a holder of a VISA card.

#### B.1.1. Account holder

As an account holder, the Client has Access to all of his accounts, of any kind (cash accounts, securities accounts, deposit, and credit accounts etc.) referenced under the client number(s) indicated in the Request.

### **B.1.2. Joint account holder**

As joint account holder, the Client may on his own request Access in respect of the client number(s) under which he is a joint account holder.

Each joint account holder must sign their own Request and shall have their own Identification details. **The joint account holder who requests Access must inform the other joint account holder(s) and shall hold the Bank harmless from any loss or damage arising out of any claim for liability as a result of failure to inform the other joint account holder(s).**

### **B.1.3. Mandate holder**

As mandate holder, the Client may only request Access with the express written consent of the account holder / a joint account holder of the client number(s) indicated in the Request.

**The (joint) account holder who authorises Access to the mandate holder acknowledges and accepts that the latter has the right to view, unlimited in time, all information concerning the client number(s) indicated in the Request, in particular in relation to the account history and the card statements.**

**A joint account holder who authorises Access to the mandate holder must inform the other joint account holder(s) and shall hold the Bank harmless from any loss or damage arising out of any claim for liability as a result of failure to inform the other joint account holder(s).**

The account holder or joint account holder who authorises Access shall be liable for the operations executed by his mandate holder.

The foregoing authorisation may be revoked at any time by any account holder. It shall however remain valid until revocation in writing, either notified by registered letter or delivered to the Bank against acknowledgement of receipt. Unless agreed otherwise, however, the Bank shall only be held liable on expiry of the fifth banking day following receipt of the written revocation.

The authorisation shall cease to have effect vis-à-vis the Bank on the occurrence of any of the grounds referred to in Article 2003 of the Civil Code (death, unless agreed otherwise, statutory lack of capacity, insolvency or any other similar procedure), on the fifth working day after the Bank becomes aware of its occurrence, without the Bank being required to make inquiries.

### **B.1.4. Legal representative**

As a legal representative, the Client may request access for the client number(s) indicated in the Request belonging to an account holder over whom the Client exercises parental authority.

Without prejudice to article B.2. of these General Terms and Conditions - Internet and Remote Selling, the Access shall be granted to the legal representative until the titleholder has reached the age of 18, except in the case of emancipation of the latter or forfeiture of parental authority on the part of the legal representative.

In those eventualities, Access shall be withdrawn and the Bank shall only be held liable from the fifth bank working day after the Bank has been informed, either by registered letter or by presentation to the Bank against a receipt of the document setting out emancipation, or forfeiture of parental authority.

### **B.1.5. VISA cardholder**

As the holder of a VISA card issued by the Bank, the Client may not request an Access to consult the VISA statement of his/her VISA card number as indicated in the Request, except with the express written agreement of the account holder / a joint account holder of the client number(s) indicated in the Request.

## **B.2. Extent of the Access**

**The range of the operations available to the Client using the Access depends on the kind of access granted to the Client (consultation or transactional), on the type of accounts to which the Access relates, the type of authority or management associated with those accounts (signatory powers over the accounts, whether or not there is a management mandate, limits on the accounts, etc.), and the**

**capacity under which the Access is granted to the Client (account holder, mandate holder, legal representative or VISA card holder).**

**The extent of the Access may also be limited to Access for consultation rather than transactional in the case of a Client resident in a high-risk country or a country which prohibits Internet banking.**

**Any change in one of these factors may therefore give rise to a change in the type of access granted to the Client, or even withdrawal of Access. The Bank shall however only be bound to change the Access or to withdraw it on the fifth banking day following the date on which it was duly advised in writing of the changes affecting the Access. Those changes shall however not affect transactions in progress and any forward or term transactions not yet matured.**

## **B.3. Right to refuse Access**

The Bank is entitled to refuse Access in full or in part and/or to impose additional conditions on Access, without explanation of why.

The Bank may also limit Access geographically. Accordingly, Access may be limited or even prohibited from certain countries.

## **B.4. Withdrawal period**

**The Client has fourteen (14) calendar days (from the date he receives his Identification details, required to establish the connection to the Internet Service) to withdraw, without penalty and with no need to indicate the reasons, under the conditions set out in Article C.5. of the provisions regulating remote selling.**

**The Access granted to the Client in his capacity as mandate holder shall also be dependent on the consent of (one of) the account holder(s) on the client number(s) in question.**

## **B.5. Connection to the Access**

The Client has Access via the Internet address [www.ing.lu](http://www.ing.lu) on the worldwide web. Access is therefore available at all times, wherever the Client may be.

The Client is responsible for his connection with the Internet service provider of his choice.

The Client must change his initial Password when he first connects according to the procedure in force.

**The Client has sole responsibility for his choice of Password.**

**To be able to connect, the Client must subscribe to one of the authentication products provided by LuxTrust and accepted by the Bank for use as Identification details.**

**A Client who requests LuxTrust services has sole responsibility for all consequences of any kind that could arise from the use of LuxTrust's services according to the terms and conditions set out in the LuxTrust General Terms and Conditions.**

**The Customer undertakes not to connect in a country that does not allow remote connection.**

## **B.6. Recommendations**

Each time he connects to his Access, the Client must ensure that his installation (or his Mobile device, as the case may be) presents no technical anomaly or contains any virus or other programme which could jeopardise the security of the Access. The Client's installation must have the minimum required configuration in accordance with the procedures in force provided on the Website. Generally speaking, he shall take all appropriate measures to preserve the security of his access and in particular use a high-quality anti-virus and anti-spyware software, permanently keep it up to date, and regularly update the operating system's software of his installation.

The Client will always make sure that it is not possible for him to be watched without him knowing when entering his Identification details. In addition, the Customer may refer to Appendix 2 of these General Terms and Conditions - Internet and Remote Selling of the Bank, which

contains cautionary advice to be observed when using Internet and/or Mobile Access.

The Client acknowledges that he has been duly notified by the Bank that it recommends using the LuxTrust Mobile offered by LuxTrust,.

**The Client has sole responsibility for all consequences, direct or indirect, resulting from the choice of the LuxTrust product used in accordance with the technical features of each of these products and, in this respect, also has sole responsibility, at the entire discharge of the Bank, of any wrong, improper or fraudulent use of the means of authentication and signature linked to the chosen product, , except in the case of gross negligence on the part of the Bank.**

Since the Access is possible anywhere in the world, the Client must comply with the legislation of his place of residence and/or domicile and with the legislation of the place where he uses the Access and/or the destination country of the transactions.

In order to reduce the risks of unauthorised persons having access to the Identification details, the Client must connect to the Bank's Website directly and not indirectly, for example via a link. Any indirect Access by the Client to the Bank's Website will be at his own risk and peril.

The Client may at any time verify the authenticity of the Bank's Website to which he is connected by checking that the digital certificate of the Bank's Web server appears in his browser. The data exchange is protected by an encryption mechanism. Currently, a closed padlock appearing in the browser status bar shows that this device is activated.

If the Client imports bank details into management software, he must take every precaution to ensure that the confidentiality of the data is safeguarded and to prevent access by unauthorised third parties.

### **B.7. Safekeeping of Identification details**

**A Client's Identification details are strictly personal and non-transferable.**

The Identification details are the technical means that make it possible to identify the Client.

The Client Identification Elements consist of an Identifier (hereinafter User ID LuxTrust), an ING Contract Number, a Password, and a One Time Password (OTP) generated, as the case may be, using the LuxTrust product selected by the Customer.

**The Client is bound to take all the necessary steps to ensure the safety and confidentiality of all his Identification details and undertakes in particular:**

- not to write down his Password and to change it regularly;
- to keep his LuxTrust product and his User ID / Contract number in a safe place not accessible to third parties.

**In the event of loss, theft, fraudulent use or if the Client suspects that a third party has had access to his Identification details, he must voluntarily and immediately block his Access or his authentication method, as the case may be, by entering an incorrect password or One Time Password (OTP) several times in succession (currently five times) in the transactional part of the Bank's Website until a message confirms that his Access or authentication method, as the case may be, has been blocked.**

**Otherwise, the Client must ask for his Access to be blocked by telephoning the Bank's Contact Centre on 44.99.1. and/or block the registration of his Mobile device via the transactional part of the Website.**

**Furthermore, in the same circumstances, the Client is bound to immediately notify the Bank and to revoke any Certificate with LuxTrust by following the procedure established by LuxTrust and/or by contacting LuxTrust's help desk on 24 550-550. For further information, the Client must refer to the information provided on the Website [www.luxtrust.lu](http://www.luxtrust.lu), part "My LuxTrust".**

**The Client shall bear all losses related to any unauthorised payment transaction following the loss, theft, or misappropriation of his**

**Identification details until the moment his Access and Certificate are blocked, except where he has acted fraudulently.**

**Accordingly, the Client has sole responsibility for keeping his Identification details.**

**If he is a consumer, however, the Client shall be liable for these losses after his Access and/or Certificate has been blocked only up to the limits established by applicable law unless these losses are the result of fraudulent conduct on his part or of a failure to comply with the duty to use the Access or the Identification details in accordance with the conditions governing their issue and use either intentionally or following gross negligence.**

**In this respect, it is expressly agreed that the fact that a third party uses the Access, notably after correctly entering the Client's Identification details, shall be conclusive evidence that they were accessible to a third party and that the Client has seriously failed in his obligation to safeguard their security and confidentiality. The Client shall however be entitled to submit evidence to the contrary.**

### **B.8. Description of the services provided**

**B.8.1.** The Access shall enable the Client to connect via the Internet to the Bank at any time, to perform banking transactions (transfers, standing orders) and stock market transactions (sale/purchase of securities and SICAV units) on accounts held with the Bank. The Client can also, depending on the options offered by the Bank, take out or apply, subject to acceptance by the Bank and mutual agreement, to take out contracts relating to banking, financial or insurance products or services with the Bank.

The Client may consult accounts, securities deposits and statements of account relating to the client number(s) indicated in the Request or in any other subsequent request.

For consumer clients, mail (account statements, Visa card statements) in PDF format, may be downloaded and printed at any time. It is stored for five years in a secure data storage dedicated to the Client. On expiry of that period, of the account's mail can no longer be consulted, printed, or downloaded. Clients who wish to conserve their mail beyond that storage period are therefore requested to print them and/or to download them before expiry of that period.

**B.8.2.** The Client also has access to various types of financial information and a secure messaging service to and from the Bank.

**B.8.3.** The Bank reserves the right to amend the services, in particular by withdrawing, amending, or adding any additional service at any time. The Client will be informed by a message on the Bank's Website.

**B.8.4.** When this service is activated for the Client, the Bank enables users of the Internet and Mobile Access to send messages by 'Chat' within a time frame that depends on the technical and human capacities, defined by the Bank.

The Bank can use artificial intelligence ('Chatbot') in order to automatically reply to the queries sent by 'Chat'. The user should never indicate secret codes (codes required to perform banking operations online or the debit card PIN number) in a 'Chat' conversation. The Bank will never request this information. The 'Chat' feature can be used to provide support on the Bank's products or on-line channels.

The user is responsible and shall bear all the consequences:

- No instructions will be accepted by 'Chatbot';
- Of his use of the 'Chat' feature through the questions asked or the queries sent;
- Concerning the protection and incorrect usage of the device on which he uses the chat function.

The Bank can terminate the 'Chat' session at any time:

- If the messages sent are considered to be inappropriate or disrespectful;
- For security reasons.

The user shall not hold the Bank responsible for the harmful consequences and prejudice suffered by the user for having used the

'Chat' feature, or for the data obtained by this function. 'Chat' conversations are recorded and may be used for training courses, to improve the quality of the feature and in case of legal proceedings.

### **B.9. Information on the Website**

Information published on the Website, whether financial, political, economic, socio-cultural, or otherwise, is provided for information purposes only. It is gathered by the Bank from various sources and reproduced unchanged with no warranty that it is reliable, up-to-date, or exhaustive or as to the quality and accuracy of its content. In no case shall such information constitute an offer or solicitation to buy or sell or a call for savings. It has no value in terms of legal, accounting or tax advice and is valid only at such time as it is provided. It is not intended to replace the Client's knowledge and skills and must therefore be used only by or in conjunction with the assistance of an informed qualified professional. This information may be withdrawn or changed at any time without prior notice.

The Client also acknowledges that any reference to past performance referred to in such information shall under no circumstances be a guarantee of future performance by the relevant product.

The Bank shall under no circumstances be held liable for the direct or indirect consequences of use of such information, unless there is fraud or gross negligence on its part.

There may be links to other websites; the Bank takes no responsibility whatsoever for the content, services, products, or materials offered by those sites.

The Client may download the information on the site for personal use for a period limited to his needs. Furthermore, the Client is authorised to print the downloaded information onto paper provided that any copies thus produced are limited to the Client's personal use. The Client undertakes not to sell or republish in any way whatsoever any kind of information published on the service.

### **B.10. Blocking and unblocking Access**

The Bank reserves the right to, at any time, permanently or provisionally, block the Client's Access for any reason, in particular relating to:

- the security of the Access including maintenance and improvement of the Access;
- presumed unauthorised or fraudulent use of the Access, in particular in the event of modification in the characteristics defining the extent of Access or of withdrawal of the authorisation for access to the Internet Service given to a mandate holder, or;
- an appreciably increased risk of the holder of a client number(s) being unable to meet any of his payment obligations.

If a card is blocked, the Bank shall inform the Client that it has been blocked and the reason for this by a notice placed on the Bank's Website and/or by mail (paper or electronic), if possible before the Access is blocked, or immediately thereafter unless providing this information is unacceptable for reasons of security or prohibited under any European or national legislation.

The Bank may refuse to execute any transaction and/or block all accounts or transactions in all cases where it considers there is a risk that it could contravene the law or any obligation or regulation that the Bank is bound to or has undertaken to comply with. The same applies to the cases provided for in the articles of the General Terms and Conditions of the Bank applicable to the Client. The Client cannot claim any damages as a result of the account being blocked or such operations being suspended under the terms of this article.

The Bank will be allowed to refuse any request for unblocking made by the Client, as long as in its sole discretion it considers that the reasons for the blocking are still valid.

**In any case, its responsibility will be limited in accordance with the terms of the articles of the General Terms and Conditions of the Bank applicable to the Client.**

So far as possible, the Bank shall keep the Client informed of the foreseeable length of interruptions. It shall unblock Access or shall, as the case may be, replace the Identification details when the grounds for the blockage do no longer exist.

The Client is informed that incorrectly introducing a password and/or a One Time Password (OTP) after a limited number of attempts (currently five) also automatically blocks Access.

The Client may request the unblocking of the Access by contacting his branch or by calling the Contact Centre at +(352).44.99.44.1.

The Bank will be allowed to refuse the unblocking if, in its sole discretion, it considers that the reasons for the blocking are still present.

Questions raised by the Client relating to LuxTrust hardware and/or software will be dealt with directly by LuxTrust's helpdesk. For further information on this issue, the Client must refer to the information provided on the Website [www.luxtrust.lu](http://www.luxtrust.lu) or by calling LuxTrust's helpdesk at +(352) 24.550.550.

Questions related to the Access must be directed directly to the Bank. In case of maintenance operations, the Bank will make every effort to complete its maintenance tasks within a reasonable time. In performing these maintenance tasks, it is however only bound by a best efforts obligation.

The Bank is not bound to carry out upgrade maintenance and accordingly does not guarantee that its Internet and Mobile Access Services are suited to the Client or user's own needs and desires. The Client and user are bound to check themselves whether the Internet and Mobile Access services are suited to their needs

**Generally speaking, the Client may not claim any damages as a result of his Access being blocked for any reason whatsoever.**

### **B.11. Execution of transactions**

#### **B.11.1. General provisions**

The Client authorises the Bank to execute any transaction confirmed by the validation procedure indicated whilst the transaction is in progress (hereinafter "validation procedure").

Any transaction not validated in accordance with that procedure shall be deemed not to be authorised by the Client.

The Bank also reserves the right to delay or to refuse to execute any transaction in accordance with its general terms and conditions in force at the time.

Without prejudice to the Bank's general terms and conditions in force at the time defining the time at which a payment order is received, any transaction shall be deemed received by the Bank at the time and on the date indicated in the transaction summary notice or at the time the message is received.

The Client is informed that the secure messaging service is not intended to be used to transmit payment orders or stock market orders, in particular when the said operations require a direct contact with one of the Bank's account managers.

The Bank reserves the right to not take account of such instructions forwarded through the secure messaging service.

The Bank shall not be held responsible in such a situation, in particular due to failure to execute or delays in executing such orders.

#### **B.11.2. Securities transactions**

He Access enables stock market orders to be transmitted 24 hours a day, seven days a week.

In order to place orders for the purchase and sale of securities, including SICAV units, the Client must hold a securities account with the Bank.

The Bank shall transmit those orders to the market(s) in question as soon as possible subject to the rules and current practices and the periods when the market(s) and the various parties which must be involved in the transaction are closed.

The Bank reserves an indisputable right to refuse orders which appear to it to be incompatible with market conditions or which in its opinion do not comply with its requirements or relate to securities traded on markets other than those permitted by the Access.

The fact that an order has been validated and transmitted by a Client shall not imply in any way its successful execution taking into account in particular parameters beyond the Bank's control such as market liquidity and/or the volatility of the security.

The order shall be executed only where market conditions so allow and where it satisfies all applicable statutory, regulatory, or contractual conditions.

If it has not been possible to transmit an order for any reason, the Bank shall inform the Client of that fact as soon as possible. Where it has not been possible to transmit an order, the said order will be deemed to have expired. It shall be the Client's responsibility to issue new instructions as appropriate.

The Bank particularly draws the Client's attention to the fact that:

- if a securities purchase order is placed and no price limit is indicated, the existence of sufficient cover shall be confirmed at such time as the order is transmitted to the Bank, irrespective of any subsequent change in the price of the security in question and the time required for execution of the order, and
- any stock market order not executed may be classified as 'in progress' until the working day following its expiry date.

For remaining matters, the Client is asked to refer to the section dedicated to Operations on financial instruments in the Bank's General Terms and Conditions applicable to him as well as to its best execution/selection and processing of orders policy.

### **B.12. Revocation of a transaction**

Unless stipulated otherwise in this article, a payment or stock market order may not be revoked by the Client once the latter has confirmed the transaction in accordance with the validation procedure in force.

An invoice payment or standing order may be revoked no later than the cut-of-time indicated in the Bank's tariffs in force at the time on the banking day preceding the debit of funds.

In principle, a stock exchange order cannot be revoked by the Client, as the execution of the order is, as a rule, almost instantaneous following the automation of the transmission of such orders in the market.

However, in exceptional cases, the Bank may accept such a revocation request, without assuming any liability, provided that it is received by post in sufficient time to enable the Bank to cancel the order before it is executed.

### **B.13. Posting of transactions**

The balances and available funds on accounts are communicated subject to any transactions in progress not yet posted in real time.

A payment order will appear in the movements and statements of account available using the Access the day following its execution.

### **B.14. Delay applied to indexes and quotes**

The Client's attention is drawn in particular to the fact that for certain technical reasons or in order to meet the requirements of certain stock exchanges, stock exchange indexes and prices are transmitted with a time delay of approximately 15 to 30 minutes.

The Bank may under no circumstances be held liable for any errors or delays applied to quotes and indexes or for their direct or indirect consequences.

### **B.15. Regularisation, securities transaction, and other notices**

**The Client declares that he has been informed that the Bank may send him notices at times other than at the frequency at which account statements are sent to him as agreed with the Client, in**

**order to inform the Client of an event requiring his rapid response. The Client is therefore strongly advised to consult his notices and statements of account very regularly. The Client shall be solely liable for the direct or indirect consequences of failing to do so.**

### **B.16. Proof of transactions**

The Client is identified by keying in his Identification details on connecting to the Access. Any consultation, transaction or subscription for a product or service carried out during a connection, if any, confirmed by the Client's Identification details is deemed to come from the Client alone.

The Client's consent to the operation or subscription of the product or service is validly reported by the Bank by proving that the validation procedure provided for by the Bank was complied with.

The Client accepts that the Bank's electronic records, in any medium, shall be formal and sufficient evidence that the Client himself has consented to the transactions, products and/or services.

**The Client acknowledges that the validation procedure has the same legal validity as a handwritten signature.**

Provided that the authentication and signature procedures or electronic validation, if any, have been complied with, the Client acknowledges that they are equivalent to his signature or that of his mandate holder by which he confirms that he is the originator of the orders recorded and their content. Accordingly, the Client, when applicable, waives the right to avail himself of the provisions of article 1341 of the Luxembourg Civil Code and acknowledges that he accepts the electronic records held by the Bank (or by LuxTrust), in particular all transactions made via the Access, as the form of proof.

The confirmation of the use of the Identification details and/or the authenticity and the completeness of the orders and instructions provided by LuxTrust is also considered as a valid and sufficient form of proof between parties.

Accordingly, subject to the signature or validation procedure being complied with, the Client shall refrain from disputing that he consented to the transaction, product, or service.

Although it is possible for the Client to raise in defence against the Bank the printout of any transaction from his computer equipment, the fact remains that said printout alone does not constitute conclusive evidence of the financial transaction but must be compared with the Bank's record of the transaction.

### **B.17. Restrictions on use**

**The Bank reserves the right to set daily and/or weekly limits on payment transactions to an account other than an account linked to the same Client number.**

The Bank may also authorise the Client, in certain situations, to set himself other user limits for certain transactions.

### **B.18. Exclusion of liability**

The Internet is an open international network, and the Client declares that he is aware of its structure, properties, and risks.

**The Client declares that he is aware of and understands the operational characteristics of the means of telecommunication (Internet, telephone and wireless networks), and the technical limitations, risk of interruption, response times for consultation, enquiries or data transfer, the risk of all kinds inherent to any connection and any data transfer in particular over the open Internet network.**

The Bank has taken the necessary measures to ensure the confidentiality of the Client's financial information and secure processing of transactions via the Access, without however being in a position to give any warranty of result. **The Bank shall have only an obligation of means in that regard.**

**Accordingly, unless there is gross negligence by the Bank, the Client uses the Access with full knowledge of the facts and under his sole liability.**

Further, the Bank shall not be liable for any direct or indirect loss or damage which may be caused in relation to:

- a) any error or negligence by the Client, the Internet service provider or a third party, in particular in installing and using the Access;
- b) interruption, stoppage, or malfunction of the Access in particular in the event of maintenance or repair of the computer service, technical breakdown in the computer system or overload of the Internet network or disconnection of a telephone line;
- c) a virus or a spyware originating on the Internet which neither the Client's anti-virus system nor the reasonable measures taken by the Bank could have detected;
- d) unlawful access by a third party to the Bank's or the Client's computer system as a result of error or negligence by the Client;
- e) the protection and the confidentiality of the communications via devices, networks, terminals, or equipment resources not approved by the Bank.
- f) any malfunctioning and/or interruption caused by the use of one or several of LuxTrust's services (including in particular in the event of unavailability of its servers, a revocation or suspension of a Certificate causing an interruption of the Access or a failure in the security rules of LuxTrust's products or services, etc.),
- g) an event not directly attributable to the Bank, and beyond its reasonable control.

All information sent by the Bank to the Client at the request of the latter (such as financial position, balances, account history, securities statements, general information etc.) shall be sent under the Client's responsibility at his own risk and peril in accordance with his knowledge of the risks involved in the Internet network. In no circumstances shall the Bank be held liable for poor reception or non-receipt of any information sent by the Bank to the Client or vice versa.

The Bank shall not be held liable either for the expediency of a stock market order given or its direct and indirect consequences for the Client, nor for whether that order conforms to the profile of the Client or account holder in question.

The Client has sole responsibility for all consequences, direct or indirect, resulting from the choice and the use of any LuxTrust product, including in the event of any wrong, improper or fraudulent use of the means of authentication and signature linked to a LuxTrust product or in the event of a blocking of the services provided by LuxTrust for any reason whatsoever.

## **B.19. Mobile Access to the Internet service**

### **B.19.1. General provisions**

B.19.1.1. The Mobile Access to the Internet service is provided by the Bank by making available an ING Mobile Application.

The Client shall make sure that the ING Mobile Application meets the specifications laid down in the procedures in force provided on the www.ing.lu Website, and their regular update.

The Client is responsible for taking all necessary measures (in particular in terms of IT security) to ensure that the technical characteristics of his Mobile Device and his subscription to the telecommunication network allow him to check the information and to have access to the functionalities offered by the ING Mobile Application. In order to ensure full accessibility to the services, the Client must have a Wi-Fi connection or a subscription to the telecommunication network allowing him access to the ING Mobile Application.

In particular, the Client must have high-quality, up-to-date anti-virus and anti-spyware software and make sure not to jailbreak his Mobile Device and/or computer applications installed on it and each time that he connects to the Access via his Mobile Device to enter as appropriate his Password and his Contract Number and/or his Mobile PIN away from prying eyes. The Bank reserves the right to take the technical measures that it deems appropriate to detect when a Mobile device has been jailbroken.

B.19.1.2. The ING Mobile Application includes, inter alia, a security module and also a security file that contains certain encrypted Client information and which ensures the security of the access and its use.

B.19.1.3. To access the Mobile Access, the Client has to previously activate the Internet service in accordance with the procedures in force provided on the Website. For this purpose, he must download the ING Mobile Application and install it on the Mobile Device which he has. The Mobile Access is subject to the prior registration of the Mobile Device which will be used by the Client in order to access it. This mechanism thus allows the level of authentication required to access the Mobile.

On his first connection, the Client must create a "profile" based on the means of access made available to him by the Bank (such as the Contract Number/User ID, the Password, the Luxtrust Mobile and/or the One Time Password (OTP); subsequently, he will only need to enter his Contract Number and Password on each connection or his Mobile PIN or use the Fingerprint or Facial ID if available on their Mobile Device.

B.19.1.4. The Customer may cancel the registration of his Mobile Devices at any time by following the procedure in place, in particular that described in Article B.7. above.

### **B.19.2. Nature of the electronic services**

B.19.2.1. The Client is referred to article B.8. of these General Terms and Conditions - Internet and Remote Selling of the Bank for the description of the services proposed through Mobile Access.

Subject to the options offered by the Bank, the Client accepts that, unless specifically requested at his bank branch, all accounts of which he is the holder or joint holder at the Bank are accessible via the Mobile Access to carry out all transactions authorised via said Mobile Access. As things currently stand, the Mobile Access allows the Client to do the following, inter alia, via his Mobile Device.

The Bank reserves the right to amend the services, in particular by withdrawing, amending, or adding functionalities

B.19.2.2. As far as the Mobile Access is concerned, notwithstanding the provisions of this article B.19.2 and of article B.18. of these General Terms and Conditions - Internet and Remote Selling, the Client accepts that confirmation by the Client of a transaction initiated by a Mobile Device is deemed to come from the Client and him alone, provided that these means of access are validated by the relevant ING Mobile Application.

### **B.19.3. Protection of privacy**

B.19.3.1. Without prejudice to the Bank's general terms and conditions in force, the following data, called "environment variables" is sent to the Bank and recorded by it via the ING Mobile Application used by the Client when he uses the Mobile Access:

- his TCP/IP address (identification number for the computer system which the Client is using on the Internet network)
- the brands and versions of the Mobile Device used and also its operating system.

The above data is processed by the Bank in order to be able to take account of the information specific to the configuration of the computer system which the Client is using. It is also processed to draw up Mobile Access statistics and to ensure that the content of this service is improved.

By authorising the Bank to order authentication hardware from Luxtrust on behalf of the Client, he authorises the Bank to communicate his personal data to LuxTrust, which will process it in accordance with the LuxTrust General Terms and Conditions.

B.19.3.2 The Client must make sure that the connection terminal which he uses to connect to the Mobile Access on the Internet service does not have any problem or infection by a virus or malware and that he takes all reasonable precautions to guarantee the security and the



confidentiality of the access via the connection points used by the Client to connect to the Mobile Access.

**B.19.4. Licence for using the ING Mobile Application and the Mobile Access Database**

Without prejudice to making the Mobile Access available to the Client as provided for in these General Terms and Conditions, the Bank or the person who has granted the rights of use to the Bank retains ownership of all property rights and all intellectual property rights (including the rights of use) on the ING Mobile Application and also on the elements that make them up, in particular and without limitation on the texts, illustrations and other elements appearing in the ING Mobile Application.

**B.20. Intellectual property**

The Client shall acquire no right of ownership over the software, programs, applications, or instructions for use provided to him by the Bank. The Client is merely granted a right of use in this respect. The Client undertakes to comply with the rules of use set by the Bank and will refrain from making any copies, alterations, adaptations or making them available to third parties.

In general, the Client undertakes to respect the property rights of the Bank and its suppliers.

**B.21. Tariffs**

The Client shall bear all costs and expenses of equipment, communications, telecommunications, and other expenses necessary for connection to the Access, and any associated authorisation.

The Bank reserves the right, in respect of certain specific services to take a fee, the amount and frequency of which it shall set, in accordance with the general terms and conditions in force.

The Bank reserves the right to invoice the Client in accordance with the Bank's current tariffs if a lost or stolen Token is replaced.

The Client must refer to LuxTrust's tariffs for the use of the LuxTrust products he uses.

Further, all transactions performed via the Access shall be invoiced in accordance with the Bank's current tariffs.

**B.22. Termination or suspension**

The Internet Service Access is granted for an indefinite period.

The Client shall be entitled to terminate the contract at any time subject to one month's notice to the Bank by registered letter or presented to the Bank against a written receipt.

The Bank may also terminate the contract at any time, unless the Client is a consumer in which case the Bank has to give two months' notice to the Client by post or e-mail.

The Internet Service Access contract shall also terminate automatically in any of the following situations:

- closure of all the client numbers included in the Request and/or the Client's life insurance products;
- termination of the relationship between the Bank and the Client giving rise to closure of all the Client's client numbers;
- death of the Client.
- revocation of the last Certificate by LuxTrust used as an identification Element for the Client relating to the Mobile Access concerned.

Where the Internet Access is terminated in respect of some or all of the client numbers, statements of account, after termination and unless advised otherwise by the Client, shall be communicated monthly to the Client's postal address, provided the client number(s) in question is/are not covered by the Internet Access of a different holder of the client number(s) in question.

**C. REMOTE SELLING**

**C.1. Request to open an account online**

Opening an account on-line is done by inputting on a screen page the data and the Client's choice from the products and/or services offered online. After any necessary corrections are made to the data input by the Client and the data has been validated, the Bank will send the Client an acknowledgement that the Client's request has been received. The Client will then have to print off the request to open an on-line account, date it, sign it, and return it to the Bank with the supporting documents specified during the on-line account opening process.

By clicking on the "Confirm your application" icon, the Client confirms his request to open an on-line account with the Bank. Any request to open an on-line account signifies complete acceptance of these General Terms and Conditions - Internet and Remote Selling, as well as the general conditions and tariffs applicable to the products and services included in the Client's request to open an on-line account.

The Client shall receive those general conditions and tariffs in PDF format, printable and downloadable, during the on-line account opening process and before any commitment is made by the Client. They are also available to be consulted at any time and in the same format on the Bank's Website at the address [www.ing.lu](http://www.ing.lu).

The Bank shall inform the Client by e-mail of its decision to grant or refuse the Client's request to open an on-line account.

The banking relationship (or the opening of the account) shall only take effect after the Bank has sent the Client his client number.

The Bank reserves the right to refuse a request to open an on-line account, and is not required to give reasons for its decision.

Once the procedure is concluded, the documents used to open the banking relationship or account shall be retained by the Bank. A copy shall be made available to the Client upon written request.

**C.2. Object of the sale**

This contract is entered into for an indeterminate period, as part of a remote-selling programme between the Client and the Bank.

The purpose of the contract is to open an account and, where appropriate, to subscribe to an on-line financial product and/or service.

**C.3. Essential features of products and services offered online**

The essential features of products and services offered online are set at [www.ing.lu](http://www.ing.lu), as well as in the general conditions that are applicable to products and services and that are available at and downloadable from [www.ing.lu](http://www.ing.lu).

**C.4. Tariff**

Products and services offered online shall be opened/issued, where appropriate and unless otherwise stipulated, against payment deducted automatically from the ING Luxembourg current account, in accordance with the Bank scale of tariffs in force, which is available on the Website in PDF format, being freely downloadable and printable.

**C.5. Right of withdrawal**

The Client has a period of fourteen (14) calendar days, from the date on which the Bank notifies the Client of the latter's client number (date of entry into force of the distance contract) or the mail informing the Client that his card has been sent by the Bank, in which to withdraw without penalty and without being required to give reasons, and in accordance with the conditions set out below.

In order to exercise the right of withdrawal, the Client must notify the Bank of his withdrawal by registered letter, or – where appropriate – by any other means accepted by the Bank for example by using the model in Annex 1 below. The period is deemed to have been respected



## General Terms and Conditions – Internet and Remote Selling of the Bank

Edition November 2022

Page 10/12

if the notification is sent before the expiry of the period, using the attached withdrawal form, to the following address:

ING Luxembourg S.A.  
Att. Client Services - Individuals  
L-2965 Luxembourg

The withdrawal of the online request to open a banking relationship (or online request to open a current account) leads to the termination as of right of other products subscribed to online by the Client.

The withdrawal procedure may lead to the blocking of all or part of the functions of the bank card that the Client applies for. In such circumstances, the Bank shall not be liable in any way.

Where the right of withdrawal is exercised, the Bank shall reimburse the withdrawing party for any sums paid by the Client as part of the online opening of a banking relationship, and/or any other amount received by the Bank, within a maximum period of thirty (30) days. All refunds shall be performed by bank transfer to the previously debited account.

After the withdrawal period, the Client may cancel the account(s) and/or products subscribed to online, in accordance with the general terms and conditions in force and applicable to the products and/or services.

**Annex 1: Cancellation form**

Please send by registered letter to:

ING Luxembourg S.A.  
Att: Client Services - Individuals  
26, Place de la Gare  
L-2965 Luxembourg

The undersigned,

**Name:** \_\_\_\_\_ **First name:** \_\_\_\_\_

**Address:** \_\_\_\_\_

**Name:** \_\_\_\_\_ **First name:** \_\_\_\_\_

**Address:** \_\_\_\_\_

hereby declare wanting to withdraw:

- and request the closure of the banking relationship ING Orange Account with the Bank ING Luxembourg, established via online subscription on \_\_\_\_\_ (please indicate the date the Bank notified the undersigned of his/their client number)
- and request the closure of the ING Orange Savings account / Compte Vert opened with the Bank ING Luxembourg, established via online subscription on \_\_\_\_\_ (please indicate the date the Bank notified the undersigned of his/their account number)
- and request the closure of Current Account no. \_\_\_\_\_ with the Bank ING Luxembourg, on \_\_\_\_\_ (please indicate the date the Bank notified the undersigned of his/their client number)
- and request the closure of Custody Account no. \_\_\_\_\_ with the Bank ING Luxembourg, on \_\_\_\_\_ (please indicate the date the Bank notified the undersigned of his/their client number)
- from the following product(s) subscribed to online on \_\_\_\_\_ (please indicate the date when the Bank notified the undersigned that his/her card was sent). The undersigned undertakes (i) to inform the Bank by registered letter, or any other form of support accepted by the Bank, to have the card blocked and (ii) to return it to the Bank.
  - Visa Classic Card**
  - Visa Classic & Assistance Card**
  - Visa CyberCard**
  - Visa Gold Card**
  - Visa Platinum Card**
  - V PAY Card**

Date and signature(s)

**Annex 2: Cautionary advice on accessing and using Internet and/or Mobile Access**

**General safety advice for Internet and/or Mobile Access:**

- Print or request a printout or, if available, electronic communication of confirmations of your transactions made via Internet and/or Mobile Access and keep them. Also keep electronic or written confirmations of the execution or non-execution of your transactions.
- Always check your bank statements and account statements on receipt. Report any discrepancies to the Bank immediately.
- Only use the Internet Access and/or mobile application from the official stores: Apple Store and Google Play Store.
- Do not jailbreak your mobile computer system (Google Android or Apple iPad, iPhone, iPod Touch).

**Specific advice on the secret code for Internet and/or Mobile Access:**

- Memorise your password as soon as it is created, without keeping any record of it.
- When choosing your password, avoid combinations that are too obvious (e.g. part of your date of birth, the postcode of your municipality, the first four digits of your telephone number, your name or that of a family member, etc.).
- Choosing a single password for all your cards and/or all your means of access and signature carries obvious risks.
- Your secret code must remain secret: without prejudice to your right to use the services of a payment initiation or account information service provider duly authorised to carry out its activity, do not communicate it to anyone, not even to a member of your family or a friend, and certainly not to a supposedly well-meaning third party.
- No one has the right to ask you for your password: not ING (apart from encoding requests via ING e-Services), nor the police or insurance services, in any form whatsoever.
- Therefore, never communicate your secret code, password and/or PIN via e-mail, via an Internet site (if applicable, following an invitation by e-mail) or via telephone without being sure to transmit them to the Bank via ING Electronic Services. However, this does not affect your right to use the services of a duly authorised payment initiation or account information service provider.
- Beware of impostors and if you notice any unusual circumstances, inform the Bank immediately.
- Do not enter your password anywhere, even in encrypted form, for example by hiding it in a false telephone number.
- Use Internet and/or Mobile Access in places where discretion is ensured and out of sight. Also, always create and/or enter your password where it cannot be seen by prying eyes.
- Always ensure that you cannot be observed without your knowledge, for example by covering the keypad of your phone, iPad, iPhone, iPod, card reader or computer with your hand. Do not let anyone distract you and, if you do, never enter your password.
- If you notice any unusual circumstances, inform the Bank immediately.
- If you have good reason to believe that your password is no longer confidential, change it immediately. If you are unable to change your password, notify the Bank immediately.

**Specific advice regarding fingerprint recognition (e.g. Apple iOS Touch ID or Android Fingerprint) or facial recognition (e.g. Apple iOS Face ID) for Internet and/or Mobile Access:**

- Only enable the fingerprint or facial recognition function for Internet and/or mobile Access on a Mobile electronic system for which you are the only User and only enrol your fingerprints or face on that same Mobile electronic system.