**APPENDIX 2 – OUTSOURCING**

**"SUMMARY TABLE - Third party and ING Group common infrastructure[1]"**

(see **Article A.9 bis** of the "General Terms and Conditions of the Bank (Retail & Private Banking)")

**This table will be applicable as of 1 December 2023 to the Clients of Retail & Private Banking segment. However, for Retail & Private Banking Clients who have established and maintained a banking relationship with ING Luxembourg prior to this date, this table will only come into force on 15 February 2024.**

| | Description of the service | Type of shared data | Access to the data |
|---|---|---|---|
| **Services of access to Third-Party Payment Service Providers in connection with the Revised Payment Services Directive (PSD2)** | To enable Third-Party Payment Service Providers (Third-Party PSPs) to collect information on accounts, to initiate payment operations and to confirm the availability of funds in accordance with the legal obligations of the Bank and with the applicable regulations regarding payment services. | The data transferred include, inter alia, the Client's identity, his country of residence, his IBAN, his associated means of authentication (including the LuxTrust certificate), the associated link between the Client and his payment accounts, his account balances, the availability of existing funds in the accounts at any given time, and the details of the payment operations performed. | In this context, some information may be made available in a confidential manner to (i) a Financial Sector Professional (FSP) located in Luxembourg currently LuxTrust (ii) to ING Bank NV (Netherlands) and/or (iii) to its subcontractors in the Netherlands, Germany, Spain, Belgium, Romania or Poland. |
| **Know Your Customer (KYC) Services** | **CUSTOMER DUE DILIGENCE (CDD) PERFORMANCE AND REVIEW**<br>In the frame of transactions monitoring and fight against money laundering and terrorism financing, perform in a centralised manner, the necessary steps to collect, control and check as required by applicable national and international legislation regarding, in particular, the identification of the Clients, their proxyholders or legal representatives and beneficial owners or any other documentation linked to the same or the Client's transactions with the Bank, both upon opening of accounts and throughout the lifetime of these accounts. This centralised management will also enable the Bank to classify its Clients on the basis of their specific situation as regards various applicable laws and regulations such as anti-money laundering and the financing of terrorism, FATCA regulation, CRS regulation, MiFID 2 regulation, MAR (market abuse regulation), etc. | The data transferred relate to all the identifying data of the Client, the Client reference and, where applicable, their proxyholders or (legal) representatives and beneficial owners including inter alia their identifying data, profession, date and place of birth, passport number, national and/or tax identification number, address, place of residence, telephone number, any public data about the same persons and in general all the data communicated when opening the account or thereafter with regard to "Know Your Customer" and source of funds and all the information communicated to the Bank during each transaction performed on the accounts opened with the Bank from time to time. | In this context, some information may be made available in a confidential manner to ING Bank NV and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, Poland and Slovakia. This information may be stored on the IPC (ING Private Cloud) infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands. |

[1] *The subcontractors thus designated by the Bank are regulated entities that by law are subject to an obligation of professional secrecy or contractually bound by the Bank to adhere to strict rules of confidentiality*

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| | **NAME SCREENING**<br><br>To perform in a centralised manner within ING Group, the necessary name screening relating to identity of the Clients, their proxyholders or (legal) representatives and beneficial owners as per applicable standard and/or national and international legislation regarding, in particular, identification of Clients and beneficial owners and anti-money laundering and counter-terrorist financing, both upon opening accounts and throughout the lifetime of these accounts.<br><br>Moreover, screening of the same persons in the media is also centralised within the ING Group. | In addition to what is it mentioned above in the "CDD Performance and Review" the data transferred to perform the screening are the first name, last name, date of birth and country of residence.<br><br>To perform the media screening by "Regulatory Data Corp Ltd" (or any other entity of the same group) the data transferred are the first name, last name, date of birth and country of residence. | In this context, some information may be made available in a confidential manner to ING Bank NV and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, Romania, Slovakia and in the Philippines. This information may be stored on the IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands.<br><br>Some data relating to the persons subject to the media screening may be made available to the service provider based in the United Kingdom. In this context, the name screening and its results are recorded in a database stored on a cloud platform* managed by Amazon Web Services (AWS), whose servers are located in Germany and in Ireland. |
| | **PRE-TRANSACTION SCREENING**<br><br>To perform in a centralised manner within ING Group, the necessary pre-screening, controls and checks on transactions and operations on the Clients' accounts as per applicable national and international legislation and, in particular, regarding anti-money laundering and counter-terrorist financing. | Cf. "CDD Performance and Review" above. | In this context, some information may be made available in a confidential manner to Financial Sector Professional(s) (FSP) located in Luxembourg and their subsidiaries located in Europe (including in Poland and in Hungary) as well as ING Belgium, ING Bank NV and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, Romania, Poland, Slovakia and in the Philippines. This information may be stored on the IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands. |
| | **POST-TRANSACTION MONITORING**<br><br>To perform in a centralised manner within ING Group, the necessary post-monitoring of the transactions and operations on the clients' accounts and the necessary checks, controls and investigations to comply with applicable national and international legislation regarding anti-money laundering and counter-terrorist financing | Cf. "CDD Performance and Review" above. | In this context, some information may be made available in a confidential manner to ING Bank NV and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, in Poland, Slovakia. This information may be stored on the IPC (ING Private Cloud) infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands. |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| **My Compliance service** | The purpose of service is to allow the Bank to identify (potential) issues (e.g. conflicts of interests, insider trading) and assess, propose and take measures to ensure compliance with the Bank's policies against market abuse and conflicts of interest. | Name and contact details of Client which are legal entities. | In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and to its subsidiaries, including in Romania.<br><br>In this context, some information may be stored on the IPC (ING Private Cloud) infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands. |
| **Swift and Payment Services Platforms** | **IN GENERAL**<br><br>To process payment transactions via Swift and send messages via the same service, generally speaking, in addition to storing and archiving such messages and monitoring, filtering and verifying the said payment transactions or messages.<br><br>To process and execute all processes related to Clients' incoming and outgoing payment transactions, and to store and archive such transactions. | The data transferred relate to all the data included in the various fields in the messages or payment systems (Swift or otherwise), including but not limited to: the Client reference, Client's identity, his address, his IBAN, his account balance, the activity on the accounts, the identity of the instructing parties or beneficiaries of payment transactions and all the details of such transactions in general. | In this context, some information may be made available in a confidential manner to Swift, ING Bank NV (Netherlands) and/or its subcontractors in Belgium, Poland or Slovakia. |
| | **INSTANT PAYMENT**<br><br>In addition to the above, to process and execute all processes related to Clients' incoming and outgoing payment transactions, and to store and archive such transactions centrally.<br><br>To track and monitor payment transactions initiated or received centrally at ING Group level for all ING entities, including ING Luxembourg. | | In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and to its subsidiaries including in Romania, the Philippines, and its subcontractors in India and the United Kingdom.<br><br>In this context, certain information may be made available on a confidential basis to ING Bank NV (Netherlands) and ING Belgium and/or their subcontractors in Belgium and the Netherlands. |
| **Portal used to facilitate the management of the products and services offered to the clients of the Bank** | Use of a cloud infrastructure managed by ING Bank NV (Netherlands) relying on certain personal data stored centrally for KYC purpose, see above) and enabling an ING sales employees of the Bank to access centrally via this portal to the various secure applications of the Bank and allowing to facilitate the management of the client relationship without storing | The data transferred includes inter alia all data identifying the Client and the data required to take out and manage services and products:<br>• Personal and consent data; in particular: the Client reference, Client name, mail addresses, email addresses, phone numbers, single identifier (TIN, LEI), date and place of birth, and in general all the data communicated to the Bank when | In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and/or its subsidiaries / branches in the Netherlands and in Poland. |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| | the data outside Luxembourg once the search is completed. | opening an account and during the entire Client relationship management period;<br>• Services and Products signed up for (current accounts, savings accounts, Visa accounts, credit accounts...) ;<br>• Payments (SEPA, standing orders, beneficiaries management, operations on accounts...) ;<br>• Electronic documents signed or not;<br>• Documents signed by the Client;<br>• Proposal and subscription to products and/or services. | |
| **Tech Service** | First-level IT assistance to the users of the Bank in Luxembourg. | Under this contract the service provider may have access, occasionally and within the framework of the IT assistance, to any data hosted on the Bank's IT infrastructure. | In this context, some information may be made accessible in a confidential manner to a Financial Sector Professional (FSP) located in Luxembourg. |
| **Technical infrastructure services** | Provision and management of an infrastructure hosting the Bank's applications to a Financial Sector Professional (FSP) and its subcontractors and a workstation infrastructure managed by ING Bank NV (Netherlands) allowing a secure workplace environment including email service, active directory service and mobile application management service as well as physical desktops, File Servers and Shared Service Desk.<br><br>Making available, via a cloud computing infrastructure managed by ING Bank NV tech infrastructure items and applications enabling a data store to be managed.<br><br>Performing operational IT or maintenance tasks, including IT system relying on cloud computing. | The data transferred concern the email service, active directory service and mobile application management of ING Staff.<br><br>The Client's data that may be transferred include (without limitation): Client reference, name, email address, phone number, company name, email content and attachments.<br><br>The data transferred in the private cloud computing infrastructure are the same as those mentioned in the KYC (Know Your Customer) services and credit and market risk management services. | In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) based in Luxembourg (including its subcontractors) and whose data centers are located in the European Union in Belgium and in Luxembourg and to ING Bank NV (Netherlands) and/or to its subcontractors in Poland, Portugal, and Ireland. The infrastructure platform and data are hosted and stored on a Microsoft Azure cloud platform* whose servers are located in the European Union, in Austria, Finland, Ireland and the Netherlands.<br><br>In this context, some information may be made stored on the IPC cloud infrastructure managed by ING Bank NV, whose servers are located in the European Union in the Netherlands. |
| **IT security** | Provisions of maintenance and support services relating to the Bank's applications hosted in the infrastructure. | The data transferred concern the email service, active directory service and mobile application management of ING Staff. The data transferred may thus potentially contain all types of (personal) data and information, documents and contracts collected and/or processed by the Bank with its Clients in the course of its activities (e.g. Client reference, name, email address, phone number, company name, email content and attachments). | In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) based in Luxembourg (including its subcontractors) and whose data centers are located in the European Union in Luxembourg, and to ING Bank NV (Netherlands) |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| | Management of IT security system particularly the detection and management of security incidents. | For the management of IT security system, the concerned data also includes the technical data contained in the system logs and flows (containing users' IP addresses) as well as the data contained in ingoing and outgoing internet flows. | and/or to its subcontractors in Poland. |
| **Services related to printing and Client document management** | Client documents formatting, printing and scanning service. | The data transferred concern all the Client data contained in the Client documents, including inter alia the Client reference, last name and first name, address, account number, account movements, account balance, products and services subscribed. | In this context, some information may be made accessible in a confidential manner to a Financial Sector Professional (FSP) located in Luxembourg in the context of the digitalisation of documents and their printing, as well as to ING Belgium for the formatting of various types of Client documents. |
| **Physical archives management** | Storage of archives, collection of archives for secure transport to the storage warehouse, return of archives for consultation purposes and destruction of the archives with provision of a certificate of destruction. | The Client's data that may be transferred include (without limitation): Client's reference, name, email address, correspondence, phone number, company name, and any other data and documents processed during the Client's relationship with the Bank and contained in the physical archives.<br><br>Data used for the tracking of the archives (for consultation purposes) and for their destruction. | In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) based in Luxembourg and with a warehouse located in Luxembourg. The FSP only handles the container and not the content. |
| **Credit risk management services** | Central orchestration and storage of credit applications and decisions (whether at the time the application is made or during the life of the credit), determination of credit limits and credit exposures per Client.<br><br>Monitoring and modelling of the credit and market risks, Internal and external reporting of the Bank's credit risks linked to Clients in different market conditions (scenarios). | The data transferred concern all the Client's data relating to the initial loan application, a change or any other event linked to the life cycle of the product as well as any supporting document.<br><br>This information includes: the Client reference, account number, account balance, repayment schedules, type and characteristics of the products subscribed to, remuneration conditions, guarantees, securities, names of any guarantors, assets, defaults, if relevant detailed information of the real estate property used to secure the loan application (including its address) and any other financial information held by the Bank in relation to the Client (such as credit or debit balance, existing credit facilities or other loans granted by the Bank and their outstanding amounts). For legal entities only, the data transferred also include the Client's financial data, including balance sheet, revenue and number of employees. | In this context, some information may be made available in a confidential manner to Nexvia (a service provider based in Luxembourg), ING Bank NV (Netherlands), and its subcontractors in the Netherlands, Belgium, Poland, and/or in Slovakia.<br><br>The central platform and the data are hosted and stored on the IPC cloud infrastructure managed by ING Bank NV, whose servers are located in the European Union in the Netherlands.<br><br>The infrastructure platform and data transmitted to Nexvia in Luxembourg are hosted and stored on an Amazon Web Services cloud platform* whose servers are located in the European Union in Ireland. |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| | | In addition, for Legal entities only, the data transferred also include the beneficial owners and legal representatives' personal data, including its identity, address, ownership structure, sector of activity, town and country of incorporation.<br><br>For individuals, the data transferred also include the Client's personal data, including its identify, profession, marital status, matrimonial agreement and number of dependent children. | |
| **Market risk management service** | Monitoring and modelling of market risks in general, internal reporting and export of the Bank's interest trading rate and liquidity risks. | The data transferred are of a financial nature: Client reference, account number, account balance, repayment schedules, type and characteristics of the products subscribed to, remuneration conditions, etc. | In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) or its subsidiaries in Belgium, in Poland or in the Philippines. |
| **My ING – Web Banking** | My ING, to offer a Web-Banking platform on iOS/Android mobile and web applications. | The data transferred include the Client's identity and required data to manage daily activities, including inter alia:<br>• Authentication (LuxTrust Certificate…), security and fraud prevention<br>• Personal data and consents<br>• Product Overview (Current accounts, Saving accounts, Visa accounts, Loan accounts, etc.)<br>• Payments (SEPA Payments, Standing orders, management of payees, etc.)<br>• Mobile Payments with Payconiq<br>• Alerts (email and push notifications)<br>• Account aggregation<br>• Secured messaging<br>• Electronic documents<br>• Proposal and subscription to products and/or services | In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) based in Luxembourg (currently LuxTrust) and to ING Bank NV and/or its subcontractors in the Netherlands, Belgium or Poland. |
| **Digital communi-cation channels** | Making available secure digital communication channels such as audio calling, chat and messaging.<br><br>These channels use Internet cloud services*. | The data transferred concern the information needed to establish the communication and for speech recognition:<br><br>• IP address<br>• Phone number<br>• Email address<br>• Photo or video<br>• Natural Language Processing (NLP, Voice recognition)<br>• Technical identifier of the ING Contact Person. | In this context, some information may be made available in a confidential manner to ING Bank NV and/or its subcontractors in the Netherlands, Belgium or Poland.<br><br>The infrastructure platform and the data are hosted and stored on Amazon Web Services (AWS) and Google cloud platforms*, both located in the European Union, in Ireland and Germany. |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| | | The communications are recorded and stored by the Bank and may be used as means of proof in accordance with the applicable General Terms and Conditions.<br><br>The operator of the Cloud services* only has access to technical data depending on the channel (and not to the communications' decrypted content):<br>• IP address<br>• The message's encrypted content (for which only ING has the decryption keys) for the duration of the communication; before being deleted at the end of the call. | |
| **Multiline (for businesses only)** | Hosting and management of the Multiline multi-banking platform, through which any company having subscribed to this service may, in particular, consult data linked to its bank accounts and initiate payment transactions. | The data transferred include, among other things, the Client's identity and the data needed to manage its accounts on a daily basis, including inter alia:<br>• Authentication (LuxTrust Certificate…), security and fraud prevention<br>• Data linked to its accounts: consultation of balance and list of transactions<br>• Payments (SEPA, standing orders, management of payees) | In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) based in Luxembourg currently Worldline Financial Services and its affiliated companies in France, Belgium, Germany, without prejudice to the Instant Payment section. |
| **Central services for OTC (over-the-counter) financial instruments transactions** | All OTC (over-the-counter) transactions between the Client and the Bank are centralised on ING Bank NV's platforms, in order to improve Client service and to allow for central monitoring and legal controls, including without limitation for the European Market Infrastructure Regulation (EMIR), the MIFID 2 Regulation (including MIFIR). | The data transferred include Client data, including without limitation the Client reference, name of the legal entity, the Legal Entity Identifier (if any), the email address and the transaction details. | In this context, some information may be made available in a confidential manner to ING Bank NV in the Netherlands and/or its subsidiaries or branches in Belgium, Slovakia, the United Kingdom, Singapore, India and the Philippines. |
| **Central services linked to positions acquired in financial instruments on the European markets** | In order to identify the shareholders, at the request of the relevant issuer, transmit information relating to general meetings, facilitate the exercise of shareholders' rights and meet the Bank's regulatory obligations regarding SRD II (Shareholder Rights Directive II EU 2017/828, as amended). | The data transferred include in particular: the Client reference, Client's name, postal address, email address, unique identifier (TIN, LEI), position held of the relevant security as well as Client's choice in case of voting at the general meeting. | In addition to information transmitted to the relevant issuer as per SRDII (including for the proxy voting services), some information may be made available in a confidential manner to a Broadbridge Financial Solutions Ltd service provider based in the UK, and to a cloud infrastructure solution (IBM-Managed Private cloud)* whose servers are located in the European Union, in France and Germany. |
| **Management of credit and debit cards and transaction** | Comprehensive management of credit or debit card processing (including 3D Secure): | The data transferred include inter alia the Client reference, the Client's or card holders last name and first name, his address, IBAN number, availability of | In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands), its affiliated companies in Poland and to |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| **authentication via the Internet** | - at the level of transactions effected through such cards, as well as operations during the card's lifetime (ordering the card, blocking the card, contactless function, etc.);<br>- monitoring of suspicious or fraudulent transactions;<br>- managing complaints at the level of the Visa network;<br>- managing ecommerce transaction through 3D secure authentication. | existing funds in the accounts linked to his cards at any given time.<br>The data managed by the providers include card information, associated means of authentication (including the LuxTrust certificate) and details of transactions effected with the card. | Financial Sector Professionals (FSP) in Luxembourg, namely (i) LuxTrust and (ii) Worldline Financial Services and its affiliated companies in France, Belgium, and Germany. |
| **Marketing event management service** | Use of an external platform to collect the electronic registrations of guests, Clients and prospects to marketing events organised by ING Luxembourg. | The data transmitted concern the following identification data (encoded directly) by the person registering online for such a marketing event in response to an invitation:<br>• Last name<br>• First name<br>• Company name for legal entities<br>• Email address<br>• Phone number (optional) | In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) or to its subsidiary in Belgium, and to its partner Via FUTURA bvba, based in Belgium.<br>The data is recorded in a database stored on an Amazon Web Services (AWS) cloud platform* whose servers are located in the European Union, Belgium, the Netherlands and the United States as regards the email address. |
| **Cash Management** | When the Client subscribes to any product allowing cash management by automatic switching of liquidity between the main accounts, sub-accounts and participating accounts. | The data transferred concern the Client's employee data (company name, Client number, etc.) and financial data (account balances, account movements, etc.) within the group. | In this context, some information may be made available in a confidential manner to ING Bank NV in the Netherlands, ING Belgium and/or its other worldwide subsidiaries participating in the subscribed cash management product. |
| **Production of debit and credit cards** | Management of the production of credit and debit cards, and their delivery to Clients/card holders. | The data transferred include in particular the Client reference, Client's or cardholder's last name and first name, IBAN number, address, and information linked to the debit or credit card. | In this context, some information may be made available in a confidential manner to ING's affiliated companies in Poland and/or their partner Thales (or its subsidiaries) in France and/or Germany<br>The central platform and the data are hosted and stored on the IPC cloud infrastructure managed by ING Bank NV, whose servers are located in the European Union in the Netherlands. |
| **Signature sharing platform service** | Use of a platform in order to collect electronic signatures relating to the legal documentation between the Bank and its Clients. | The data transferred include, among others, the documents to be signed, the last name and first name of each signatory, his position, his link with the legal entity for which he acts, his phone number (in order to send SMS messages) and his email address. | In this context, some information may be made available in a confidential manner to a cloud* infrastructure provider provided by Adobe and hosted by Amazon Web Services (AWS) whose servers |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| | | | are located in the European Union, Ireland and Germany. |
| **Consolidated regulatory reporting of the Bank** | Consolidation of COREP (Common Reporting Framework) and EBA (European Banking Authority) regulatory reports. | The data transferred include in particular the Client reference, Client name, their LEI, national identification number for companies accounting for the 20 biggest credit risk exposures of the Bank. | In this context, some information may be made available in a confidential manner to ING Bank NV and to its subcontractors in the Netherlands including PwC.<br><br>In this context, some information may be made available in a confidential manner to a supplier of a cloud* infrastructure provided by Solvinity and hosted by Solvinity. The data will remain in the European Union, in Solvinity's databases in the Netherlands. |
| **Automated translation system** | Translation tool using artificial intelligence. | All types of texts and documents, including those collected by the Bank or communicated by the Client in the course of the business relationship, such as manuals, contracts, procedures, reports, product and support information, websites, etc. | In this context some information may be stored on the IPC cloud infrastructure managed by ING Bank NV, whose servers are situated in the European Union in the Netherlands. |
| **Infrastructure of ING Luxembourg employees' emails and archiving** | Provision of the exchange Online O365 messaging infrastructure for the Luxembourg entity managed by ING Bank NV.<br><br>This infrastructure has an archive managed by ING Bank NV, of all emails sent to and from ING mailboxes. Exchange O365 is a cloud computing infrastructure managed by ING Bank NV (the Netherlands). | The data transferred concerns all data related to the processing of all emails sent to and from ING mailboxes (of employees or not) (internal and external) as well as their attachments. This also includes employee calendar, contacts, and all email-related features. | In this context some information may be made accessible in a confidential manner to ING Bank NV in the Netherlands on a Microsoft Azure cloud platform* whose servers are located in the European Union in the Netherlands, Poland and Ireland.<br><br>Archiving of these emails shall also be accessible in a confidential manner by ING Bank NV (Netherlands). |
| **SharePoint data storage infrastructure** | Provision of a Microsoft SharePoint type data sharing infrastructure for ING Luxembourg managed by ING Bank NV.<br><br>SharePoint is a cloud computing infrastructure managed by ING Bank NV (the Netherlands). | The data transferred may potentially contain all types of (personal) data and information, documents and contracts collected and/or processed by the Bank with its Clients in the course of its activities. | In this context some information may be made accessible in a confidential manner to ING Bank NV in the Netherlands and is stored on a Microsoft Azure Cloud platform* whose servers are located in the European Union in the Netherlands, Poland and Ireland. |
| **Contact Center** | Transfer of calls to the ING Belgium Contact Center during high traffic via the use of the called telephony platform. | The data transferred are those contained in the call transferred to ING Belgium, the telephone number, the customer's first and last name. | In this context some information may be made accessible in a confidential manner to ING Belgium. |
| | Provision of technological and application infrastructure elements through a cloud infrastructure managed by ING Bank NV to manage a data warehouse. | Communications transferred to ING Belgium are recorded and stored by ING Belgium and may be used as evidence in accordance with the applicable General Terms and Conditions. | In this context some information may be stored on the IPC cloud infrastructure managed by ING Bank NV whose servers are located in the European Union in the Netherlands. |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| **Offboarding** | Software tools and technologies facilitating the process through which the Clients' relationship with the Bank is terminated (so-called "offboarding"). | The data transferred include the Client reference, Client name, mail addresses, email addresses, phone numbers, single identifier (TIN, LEI), date and place of birth, account balance, account number, and in general all the data communicated to the Bank when opening an account and during the entire Client relationship management period. | In this context, some information may be made accessible in a confidential manner by ING Bank NV in the Netherlands, by the service provider Xlinq BV in the Netherlands and by the service provider ABBYY Europe GmbH in Germany. The information is also stored on a Microsoft Azure Cloud platform* whose servers are located in the European Union in the Netherlands and Ireland. |
| **Reporting service in accordance with the Central Electronic System for Payment Information (CESOP) regulations** | Tool set up by ING Bank N.V. for its subsidiaries, including ING Luxembourg, to generate reports on information on cross-border payments from Member States and on the beneficiaries of such cross-border payments, in order to meet the requirements of the CESOP regulations, namely Directive (EU) 2020/284 amending Directive 2006/112/EC, as transposed into Luxembourg law, and Regulation (EU) 2020/283 amending Regulation (EU) No 904/2010, as may be amended. | The data transferred relates to, but is not limited to:<br>• The BIC or other business identification code that identifies the payment service provider responsible for reporting,<br>• The name or business name of the beneficiary,<br>• The VAT identification number or any other national tax number of the beneficiary,<br>• The IBAN number or any other identifier that identifies the beneficiary and his/her location,<br>• The address of the beneficiary,<br>• Whether it is a payment or refund,<br>• The date and time of payment or payment refund,<br>• The amount and currency of the payment or refund of payment,<br>• The country code of the Member State of origin of the payment,<br>• The country code of the Member State of destination of the refund,<br>• The information used to determine the origin or destination of the payment or refund of payment,<br>• Any reference that identifies the payment, and<br>• Where applicable, all information indicating that the payment is initiated at the merchant's premises.<br>The information transmitted varies depending on the payment method used. The reports generated are sent to the Direct Contributions Administration for centralisation and aggregation in a European database, the central electronic system for payment information (CESOP). | In this context some information may be made accessible in a confidential manner to ING Bank NV (Netherlands) and to its subcontractors, the service providers Cognizant, TCS and HCL in India.<br><br>The information is stored on the IPC cloud infrastructure managed by ING Bank NV whose servers are located in the European Union in the Netherlands. |
| | | | |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.

| | | | |
|---|---|---|---|
| **Reporting service in accordance with the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standard (CRS) regulations** | Service set up to generate reports relating to FATCA/ CRS obligations and information letter in order to meet the requirements of the Luxembourg "FATCA" Law and "CRS" Law. | The data transferred includes the following:<br>• Name and surname of individuals<br>• Postal address<br>• Client number<br>• Date of birth<br>• Bank account<br>• Account balance<br>• Financial details<br>• Products and services used<br>• Tax identification number(s)<br>• Tax residence(ies)<br>• FATCA and CRS statutes | In this context, certain information may be made available on a confidential basis to ING Bank NV (Netherlands) and to its subcontractors, the service providers Cognizant, TCS and HCL in India.<br><br>The information is stored on the IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union in the Netherlands. |

* However, in the eyes of applicable US laws and regarding the cloud platform provider's links with the United States, it cannot be excluded that some data may exceptionally be accessible by the US authorities.