APPENDIX 2 - OUTSOURCING

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

(see Article A.9.Bis Outsourcing of the General Terms and Conditions Business Banking)

This table will be applicable as of 1st November 2024 to the Clients of Business Banking segment. However, for Business 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 1st January 2025.

	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/its country of residence, IBAN, associated means of authentication (including the LuxTrust certificate), the associated link between the Client and his/its payment accounts, his/its account balance, the availability of existing funds in the accounts at any given time, and the details of the payment operations performed.	In this context, certain information may be made available on a confidential basis to (i) 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 and Poland.
Know Your Customer (KYC) Services	**CUSTOMER DUE DILIGENCE (CDD) PERFORMANCE AND REVIEW** 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 on 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 (Netherlands) 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 may be regulated or unregulated entities that are either subject by law to an obligation of professional secrecy or contractually required by the Bank to comply with strict rules of confidentiality.*

* However, based on the US applicable laws and link of shareholding of the service provider with the US, it cannot be excluded that the data might be exceptionally accessed by the US competent authorities.

	COLLECT OF DATA Obtaining data from public and private sources in a centralized manner by ING Group.	The data transferred are: name of the entity, unique identifier (LEI), country of incorporation, address, which are used to collect data from public and paying sources via an automated system to facilitate KYC on the said entity. The following personal data of the legal representatives and beneficial owners are also collected: first name, last name, date of birth, country of residence and if available, nationality, residence address, ID card or passport number.	In this context, ING Luxembourg uses the BlackSwan Technologies platform located in Israel and United Kingdom. Some information may be made available in a confidential manner to ING Bank NV (Netherlands) and/or to its subsidiaries, branches and/or subcontractors in the Netherlands and in Slovakia. If the Client is also client in another ING entity, the data may be shared with any other ING entity in the world. The results will be stored on a cloud platform* managed by Amazon Web Services (AWS), whose servers are located in the European Union in Ireland.
	NAME SCREENING 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. Moreover, screening of the same persons in the media is also centralised within the ING Group.	In addition to what is 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. 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 (Netherlands) and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, Romania, the Philippines and Slovakia. 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. 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 the European Union in Germany and Ireland.
	PRE-TRANSACTION SCREENING 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 to ING Belgium, ING Bank NV (Netherlands) and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, Poland, Slovakia and the Philippines. This information may also 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 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 (Netherlands) and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, in Poland, and Slovakia. This information may also be stored on the IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands.
Data operations services	The purpose of this service is to check the mandatory reports transmitted to the CSSF pursuant to the rules on the central electronic data retrieval system in order to identify potential errors and remediate them.	Cf. "CDD Performance and Review" above. In particular, the following (personal) data of any legal representatives and beneficial owners of Clients are collected: first name, last name and any data contained in documentation serving to evidence the powers and legitimacy of the Clients' beneficial owners and proxies.	In this context, some information may be made available in a confidential manner to ING Bank NV's affiliate in Slovakia.
Market abuse and conflicts of interest related compliance services	The purpose of service is to allow the Bank to identify (potential) issues (e.g. conflicts of interest, insider trading, market manipulation) 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 and any type of information provided on recorded conversations and emails.	In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and to its affiliates, including in Romania and the Philippines. Some information may also be stored on the IPC 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** 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. 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, the Client's identity, his/its address, IBAN, 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 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. To track and monitor payment transactions initiated or received centrally at ING Group level for all ING entities, including ING Luxembourg. To perform tasks in the context of the Verification of Payee (VoP).		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, and the Philippines, and its subcontractors in India and the United Kingdom. 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 as well as to the service provider Fidelity National Information Services which stores this information on a Microsoft Azure cloud platform* with servers located in Germany and Ireland and with potential remote access to these servers from India on an occasional basis. In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and to the service providers EBA Clearing (based in France) and SurePay (based in the Netherlands) as well as to any of their subcontractors.
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 (including maintenance) of an infrastructure hosting the Bank's applications to a Financial Sector Professional (FSP) and its subcontractors in addition to 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. Making available, via a cloud computing infrastructure managed by ING Bank NV of items	The data transferred concerns the email service, active directory service and mobile application management of ING Staff. The Client's data that may be transferred include: the Client reference, name, email address, phone number, company name, email content and attachments. The data transferred in the private cloud computing infrastructure include those mentioned in the KYC (Know Your Customer) and credit and market risks management services.	In this context, some information may be made available in a confidential manner to service providers in Luxembourg, Belgium, Poland and Hungary and to ING Bank NV (Netherlands) and/or to its subcontractors in Poland, Portugal and Ireland. The infrastructure platform and data are hosted on a Microsoft Azure cloud platform* whose servers are located in the European Union, in Austria, Finland, Germany, Ireland and the Netherlands. In this context, information is stored on the IPC cloud infrastructure, managed by ING Bank NV, whose

	and applications enabling a data store to be managed. Performing operational IT or maintenance tasks, including IT system relying on cloud computing. Using third party providers to support the technical infrastructure service, monitoring of production jobs, and incident management.	The data accessible relate to all data identifying the Client, and, where applicable, their proxyholders or (legal) representatives and beneficial owners as well as the data required and used to manage services and products.	servers are located in the European Union, in the Netherlands. Support on the technical infrastructure services and incident management is also provided by the service providers TATA Consultancy Services Netherlands B.V., HCL Technologies B.V. (based in the Netherlands) and Cognizant Worldwide Limited (based in the UK) and their affiliated companies in India which may occasionally have access to client data.
IT security	Provisions of maintenance and support services relating to the Bank's applications hosted in the infrastructure. Management of IT security system particularly the detection and management of security incidents.	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). 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.	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) and/or to its subcontractors in Poland.
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 purposes (see above) and enabling 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 outside Luxembourg once the search is completed.	The data transferred includes inter alia all data identifying the Client and the data required to take out and manage services and products: • Personal and consent data; in particular: 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 opening an account and during the entire Client relationship management period; • Services and Products signed up for (current accounts, savings accounts, Visa accounts, credit accounts…); • Payments (SEPA, standing orders, beneficiaries management, operations on accounts…); • Electronic documents signed or not; • Documents signed by the Client; • Proposal and subscription to products and/or services.	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.

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, and as well to ING Belgium for the formatting 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 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. 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 the time of application and during the life of the credit), determination of credit limits and credit exposures per Client. Monitoring and modelling of 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. 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 any 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 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. 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.	In this context, some information may be made available in a confidential manner to Nexvia (a service provider based in Luxembourg), ING Bank NV in the Netherlands, and its subcontractors in the Netherlands in Belgium, Poland, Slovakia and/or ING Bank NV's subsidiaries and branches worldwide. The central platform and the data are hosted on the IPC cloud infrastructure managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands. The infrastructure platform and the 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.

Market Risk Management Services	Monitoring and modelling of market risks in general, internal reportings and export of the Bank's interest rate tradings risks 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 to its subsidiaries in Belgium, in Poland or in the Philippines.
Web Banking	My ING, to offer a Web Banking platform on iOS/Android internet and mobile applications. Inside Business Portal and Payment, to provide a single internet and mobile access point for Business Banking Clients to manage their payments and access reporting related to payments, credit and financial markets. Inside Business Connect, to enable a connection between the Client's Enterprise Resource Planning systems and ING Bank NV (and/or its subsidiaries or branches across the world).	The data transferred include, *inter alia*, the Client's identity and the required data to manage daily bank activities including inter alia: • Authentication (LuxTrust Certificate…) and security and fraud prevention • Personal data and consents • Product Overview (Current accounts, Saving accounts, Visa accounts, Loan accounts,…) • Payments (SEPA Payments, Standing orders, Beneficiary Management,…) • Account balances • Account movements • Alerts (email and push notifications) • Account Aggregation • Secure messaging • Electronic documents • Proposal and Subscription to products and/or services	In this context, certain information may be made available in a confidential manner to a Financial Sector Professional (FSP) located in Luxembourg (currently LuxTrust), and to ING Bank NV and/or its subcontractors in the Netherlands, Belgium, Romania or Poland. 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.
Services related to audit letters (for businesses only)	Harmonising and automating the request, creation and delivery of the audit letters. Web-based platform enabling auditors to request audit letters directly from ING.	The data transferred include, *inter alia:* • Client data such as client reference, company name, ultimate beneficial owner, account names, email address • Client employee data such as first name and last name, email address, phone number and IP address (electronic signature data) • Client auditor data such as the email address, phone number and IP address (electronic signature data)	In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and/or its affiliates in Slovakia and to the authorised Client's auditor. Certain 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. In this context, some information may be made available to the service provider Thomson Reuters and the data may be hosted on the private cloud infrastructure of Equinix Hosting, located in the European Union in the Netherlands.
Digital Communication Channels	Making available secure digital communication channels such as audio calling, chat messaging and messaging. These channels use Internet cloud services*.	The data transferred concerns the information necessary to establish the communication and for speech recognition: • IP address • Phone number • Email address • Photo or video • Technical identifier of the ING contact person	In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and/or its subcontractors in the Netherlands, Belgium or Poland.

		• Natural Language Processing (NLP, Voice recognition). The communications are recorded and stored by ING and may be used as evidence in accordance with the applicable General Terms and Conditions. The operator of the cloud services* only has access to the technical data according to the channel (and not to the decrypted content of the communications): • IP address • The messages 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.	The infrastructure platform and the data are hosted on Amazon Web Services (AWS) and Google cloud platforms*, both located in the European Union, in Ireland and Germany.
Multiline (for businesses only)	Hosting and management of the Multiline multi-banking platform through which any company having subscribed to this service can, in particular, consult data linked to its bank accounts and initiate payment transactions.	The data transferred includes, among other things, the identity of the Client and the data necessary to manage their accounts on a daily basis, including inter alia: • Authentication (LuxTrust Certificate…) and security and fraud prevention • Data related to their accounts: consultation of balance and transaction list • Payments (SEPA, standing order, 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 and Germany, without prejudice to the Instant Payment section.
Central services for OTC (over-the-counter) financial instruments transactions	All OTC transactions between the Client entity and the Bank are centralised on ING Bank NV's platforms in the Netherlands, 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), MIFID 2 regulation (including MIFIR).	The data transferred includes data of the Client entities, including without limitation notably the Client reference, the legal entity name, Legal Entity Identifier, contact e-mails and transactions details.	In this context, some information may be made available in a confidential manner to ING Bank NV in the Netherlands and/or to its subsidiaries or branches in Belgium, Slovakia, the United Kingdom, Singapore, India and the Philippines.
Central services related to acquired positions in financial instruments in the European markets	In order to identify 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 related to SRD II (Shareholder Rights Directive EU 2017/828, as amended).	The data transferred includes, in particular: the Client reference, Client name, postal address, email address, unique identifier (TIN, LEI), position held of the security concerned in addition to the Client's choice in case of voting at the general meeting.	In addition to information transmitted to the relevant issuer as per SRD II (including for the proxy voting services), certain information may be made available on a confidential basis to a service provider, Broadbridge Financial Solutions Ltd, located in the United Kingdom 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 or Debit Card and transaction authentication via the Internet	Comprehensive management of credit or debit cards (including 3D Secure): - at the level of the transactions made with these cards, but also of the life cycle of the cards (ordering, blocking, contactless function, ...) - monitoring of suspicious or fraudulent transactions - managing complaints in the Visa network - managing ecommerce transaction through 3D secure authentication.	The data transferred include, inter alia, the Client reference, Client's or card holder's last name and first name, his address, IBAN number, availability of existing funds in the accounts linked to his cards at any given time. 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.	In this context, certain information may be made available on a confidential basis to ING Bank NV (Netherlands), its affiliated companies in Poland including its subcontractor IT Card S.A. and to Financial Sector Professionals (FSP) in Luxembourg, namely (i) LuxTrust and (ii) Worldline Financial Services and its affiliated companies in France, Belgium, the Netherlands and Germany.
Production of Credit or Debit Cards	Managing the production of credit and debit cards and their delivery to Clients/ card holders.	The data transferred includes the Client reference, Client's or cardholder's last name, Cardholder's IBAN, last name and first name, IBAN number, address and information linked to the credit or debit card.	In this context, some information may be made available in a confidential manner to ING's affiliated companies in Poland and/or to their partner Thales (or its subsidiaries) in France and/or Germany. 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 for legal documentation between the Bank and its Clients.	The data transferred include, among others, the documents to be signed, the first and last name of each signatory, his position, his link with the legal entity for which he is acting, his phone number (in order to send SMS messages), his date of birth 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 are located in the European Union, in Ireland and Germany.
Marketing Event Management service	Use of an external platform to collect electronic registrations of guests, Clients and prospects at marketing events organised by ING Luxembourg	The data transmitted concerns the following identification data (directly encoded) by the person registering for such an internet marketing event in response to his/her invitation: • Last name • First name • Company name for legal entities • Email address • Telephone number (optional)	In this context, certain information may be made available on a confidential basis to ING Bank NV in the Netherlands or its subsidiary in Belgium and to its partner Via Futura Bvba established in Belgium. The data will be recorded in a database on an Amazon Web Services (AWS) cloud* platform with servers located in the European Union, in Belgium and the Netherlands and in 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, Belgium and/or its worldwide subsidiaries participating in the subscribed cash management product.
Client Relationship Management Services	To register, view and share on centralised platforms within ING Bank NV and its subsidiaries information supplied by the Client and any other information relating to the Client (including its related individuals) which enables the Bank to better serve the Client.	The data transferred includes, in particular: • Client data including identity and the identity of any related individuals (e.g. ID documents and ID-related data), client reference, address, ownership structure, city and country of incorporation; • data of the Client's contact persons including name, address, position, date of birth and contact data such as telephone number, email address, LinkedIn profile; • data from Client interactions, such as minutes of meetings, participation in campaigns or events; • product characteristics and financial data, such as credit or market risk limits, outstanding balances, account numbers, account references, IBAN, transactions, incoming and outgoing funds.	In this context, certain information may be made available on a confidential basis to ING Bank NV (Netherlands) and/or to its subsidiaries or branches worldwide. ING uses the SFDC Ireland Ltd (Salesforce) platform hosted in an Amazon Web Services (AWS) cloud* platform whose data remains in databases located in the European Union, including France, Ireland and Germany.
Lending Administration Services	Business processes related to Front Office and Back Office lending activities such as capturing Clients credit data in related tools for financial analysis, check of the powers of the signatories of credit documentation and other related contractual documents, the creation of risk rating proposals, the monitoring of creditor and guarantor commitments and periodic credit reviews.	The data transferred include all information related to credit applications and supporting documents. It includes notably, the identity of the Client (or guarantors), the object being financed, the Client's ownership structure, the identity of investors, know your Client due diligence information, signatories data, financial data of the Client (or guarantors) (such as balance sheet, turnover, number of employees, performance) and any other financial information held by the Bank in relation to the Client (or guarantors) (such as credit or debit balance, existing credit facilities or other loans granted by the Bank or other ING entities and their outstanding amounts).	In this context, some information may be made available in a confidential manner to ING Bank NV in the Netherlands, and/or to its subsidiaries or branches in Belgium, Poland, Romania, Slovakia, the Philippines, Sri Lanka and Ireland. Some data may also be accessed by Acuity Knowledge Partners in Sri Lanka as subcontractor of the branch of ING Bank NV located in Sri Lanka.

Consolidated regulatory reporting of the Bank	Consolidation of COREP (Common Reporting Framework) and EBA (European Banking Authority) regulatory reports.	The data transferred includes in particular the Client reference, Client name, their LEI, national identification number only 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. 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, certain 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.
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 (Netherlands). This infrastructure has an archive managed by ING Bank NV (Netherlands), of all emails sent to and from ING mailboxes. Exchange O365 is a cloud computing infrastructure managed by ING Bank NV (Netherlands).	The data transferred concerns all data related to the processing of all emails sent to and from ING mailboxes (to employees or not) (internal and external) as well as their attachments. This also includes the employee calendar, contacts, and all email-related features.	In this context, certain information may be made in a confidential manner accessible 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. Certain information may also be stored on the IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union in the Netherlands. Archiving of these emails will also be accessible confidentially 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. SharePoint is a cloud computing infrastructure managed by ING Bank NV (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, certain information may be made in a confidential manner accessible to ING Bank NV in the Netherlands or to its subsidiaries and branches worldwide 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 or its subcontractors (including B-Connected, N-Allo and CXL) via the use of the called telephony platform. Provision of technological and application infrastructure elements through a cloud infrastructure managed by ING Bank NV to manage a data warehouse.	The data transferred are those contained in the call transferred, the telephone number, the customer's first and last name. Communications transferred 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, certain information may be made available in a confidential manner to ING Belgium and to its subcontractors (including B-Connected, N-Allo and CXL) located in the European Union in Belgium. Moreover, certain 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.
Reporting service in accordance with the **Central Electronic Payment Information System (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: • The BIC or other business identification code that identifies the payment service provider responsible for reporting, • The name or business name of the beneficiary, • The VAT identification number or any other national tax number of the beneficiary, • The IBAN number or any other identifier that identifies the beneficiary and his/her location, • The address of the beneficiary, • Whether it is a payment or refund, • The date and time of payment or refund of refund, • The amount and currency of the payment or refund of payment, • The country code of the Member State of origin of the payment, • The country code of the Member State of destination of the refund, • The information used to determine the origin or destination of the payment or refund of payment, • Any reference that identifies the payment, and • Where applicable, all information indicating that the payment is initiated at the merchant's premises. The information transmitted varies depending on the payment method used. The reports generated are sent to the Direct Contributions Administration for centralization and aggregation in a European database, the central electronic system for payment information (CESOP).	In this context, certain information may be made available in a confidential manner to ING Bank NV (Netherlands). 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.

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: • Name and surname of individuals • Company name • Postal address • Customer number • Date of birth • Company number • Bank account • Account balance • Financial details • Products and services used • Tax identification number(s) • Tax residence(ies) • Role between physical and legal persons (Ultimate Beneficial Owner) • FATCA and CRS statutes	In this context, certain information may be made available on a confidential basis to ING Bank NV (Netherlands). 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.
Trading and contract management services for International Swaps and Derivatives Association "ISDA" and related collateral	Assistance in the negotiation of ISDA contracts and related collateral management agreements, and management of the life cycle of the contract until its expiry (including modifications and terminations).	The transferred data concerns all data of the client and guarantors in the context of the negotiation and management of the contract. The data also includes transactions made under the ISDA contract and collateral provided over time.	In this context, certain information may be made available confidentially to ING Bank NV (Netherlands) and its branch in Belgium.
Internal Control Process	Control identification, monitoring and evaluation to ensure ING Luxembourg is acting in line with ING's internal policies, procedures, controls, and minimum standards and applicable laws.	The data transferred relate to all data identifying the Client, and, where applicable, their proxyholders or (legal) representatives and beneficial owners as well as the data required, used to manage services and products and, more generally, any client data which is processed in relation to the tested process (e.g. KYC, Payment, Fraud, Market Abuse).	In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and/or its affiliates in Slovakia, the Philippines, and Romania.
Services of complementary research in case of dormant or inactive account and inactive safe deposit boxes	Using a third party provider to perform complementary research to obtain and use information on dormant/inactive Clients, to initiate research operations with the aim of re-establishing contact and obtaining instructions on the will of the Client (continue or end the relationship with the Bank). This is in line with the legal obligations of the Bank and with the applicable regulations regarding inactive or dormant accounts and inactive safe deposit boxes.	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	In this context, some information may be made available in a confidential manner to Dynaslux, a third party provider licensed as PSA (*Professionnel du Secteur des Assurances*) located in Luxembourg and to its subcontractors (including Finaca, ARCA CONSEIL, DETECNET, ARGENE) located in the European Union, in France.

		each transaction performed on the accounts opened with the Bank from time to time.	
Whistleblowing process	To comply with regulatory requirements on the protection of persons who report breaches of European Union law, the Bank encourages employees or other individuals (e.g. consultants) to report in good faith suspected or actual criminal conduct, unethical conduct or other misconduct by or within the Bank through the internal whistleblowing process. An external platform serves as one of the whistleblowing reporting channels, as well as a case management system and storage database of all reports received via other channels (e.g. e-mail).	Any (personal) data regarding the Client might be included in whistleblower reports.	In this context, some information may be made available in a confidential manner to ING Belgium SA (Belgium), ING Bank NV (Netherlands) and to the service provider Vault Platform Ltd (based in the United Kingdom) and its subcontractors, including Amazon Web Services (AWS), which are located in the UK, Ireland, Germany, Sweden, and the USA. Some information may be stored on the AWS cloud infrastructure* whose servers are located in the United Kingdom.