

**“SUMMARY TABLE” - Third party and/or ING Group common infrastructure<sup>1</sup>**

(see Article 7 and 8 of the Schedule “Country Specifics Luxembourg” of the Wholesale Banking Conditions)

This table will be applicable as of 1<sup>st</sup> November 2024 to the Clients of Wholesale Banking segment. However, for Wholesale 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 1<sup>st</sup> January 2025.

	Description of the service	Type of shared data	Access to the data
<b>Services of access to Third-Party Payment Service Providers in connection with the Revised Payment Services Directive (PSD2) and other financial services subscribed by the Client</b>	<p>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 the applicable regulations regarding payment services.</p> <p>To enable and support national and/or international products or services subscribed by the Client, including payments or reporting tools (statements of accounts, transactions and fees reports, ...), cash management tools, cash pooling services, documentary credit, lending product and services, spot and forward exchange product, as well as channels and/or tools and/or portals and/or platforms offering access to the above listed products and services by the Client.</p>	<p>The data transferred include, inter alia, the Client's identity, his/its country of residence, his/its IBAN, his/its associated means of authentication (including the LuxTrust certificate), the associated link between the Client and his/its payment accounts, his/its account balances, the availability of existing funds in the accounts at any given time, and the details of the payment operations performed.</p>	<p>In this context, some information may be made available in a confidential basis to (i) Financial Sector Professional (FSP) located in Luxembourg currently LuxTrust, (ii) to the ING Bank NV entity and/or (iii) to its subcontractors in the Netherlands, Belgium, Germany, Spain, Slovakia, Romania, Poland and the Philippines.</p>
<b>Know Your Customer (KYC) Services</b>	<p><b>CUSTOMER DUE DILIGENCE (CDD) PERFORMANCE, REVIEW, CONTROLS AND CHECKS</b></p> <p>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 legislations 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.</p>	<p>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</p>	<p>In this context, some information may be made available in a confidential manner by ING Luxembourg or by ING Bank NV (Netherlands) to: (i) Luxembourg-based subcontractors (including PWC) and their affiliates located in the European Union (including in Belgium, Cyprus, France, Germany, Poland, and Spain) as well as in Mauritius, and (ii) to ING Bank NV and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, Poland, the United Kingdom (in particular to the service provider Encompass Corporation), Slovakia, Romania, the Philippines (in particular to the service provider PWC), and India . If the Client is also</p>

<sup>1</sup> 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.

	<p>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, CRS, MiFID, MAR, etc.</p>	<p>accounts opened with the Bank from time to time.</p>	<p>client from other ING entity, the data may be shared with any other ING entity in the world.</p> <p>This information may be stored on the ING Private Cloud (IPC) infrastructure, managed by ING Bank NV, and on Microsoft Azure* whose servers are located in the European Union, in the Netherlands.</p>
	<p><b>COLLECT OF DATA</b></p> <p>Obtaining data from public and private sources in a centralized manner by ING Group.</p>	<p>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.</p> <p>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.</p>	<p>In this context, ING Luxembourg uses the BlackSwan Technologies platform located in Israel and United Kingdom.</p> <p>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.</p> <p>If the Client is also client in another ING entity, the data may be shared with any other ING entity in the world.</p> <p>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.</p>
	<p><b>NAME SCREENING</b></p> <p>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 legislations regarding, in particular, identification of Clients and beneficial owners and anti-money laundering and counter-terrorist financing, both upon opening of accounts and throughout the lifetime of these accounts.</p> <p>Moreover, the screening of the same persons in the media is also centralised within the ING Group.</p>	<p>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.</p> <p>To perform the media screening by the "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.</p>	<p>In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and/or to its subsidiaries and branches as well as to its subcontractors in the Netherlands, Romania, the Philippines and Slovakia. This information may be stored the IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands.</p> <p>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) located in the European Union, whose servers are located in Germany and in Ireland.</p>

	<p><b>PRE-TRANSACTION SCREENING</b></p> <p>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 legislations regarding anti-money laundering and counter-terrorist financing.</p>	<p>Cf. "CDD Performance and Review" above.</p>	<p>In this context, some information may be made available in a confidential to ING Belgium, ING Bank NV (Netherlands) and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, Romania, Poland, Slovakia, and the Philippines.</p> <p>This information may be stored the IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands.</p>
	<p><b>POST-TRANSACTION MONITORING</b></p> <p>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 legislations regarding anti-money laundering and counter-terrorist financing.</p>	<p>Cf. "CDD Performance and Review" above</p>	<p>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, Slovakia, and the Philippines. This information may be stored the IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands.</p>
<p><b>Data operations services</b></p>	<p>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.</p>	<p>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.</p>	<p>In this context, some information may be made available in a confidential manner to ING Bank NV's affiliate in Slovakia.</p>
<p><b>Market abuse and conflicts of interest related compliance services</b></p>	<p>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.</p>	<p>Name and contact details of Client and any type of information provided on recorded conversations and emails.</p>	<p>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.</p> <p>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.</p>
<p><b>Swift and Payment Services Platforms</b></p>	<p><b>IN GENERAL</b></p> <p>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.</p>	<p>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's identity, Client reference, his/its address, IBAN, account balance, the activity on the accounts, the identity of the instructing parties or beneficiaries of</p>	<p>In this context, some information may be made available in a confidential manner to Swift, ING Bank N.V. (Netherlands) and/or its subcontractors in Belgium, Romania, Poland and Slovakia.</p>

	<p>To process and execute all processes related to Clients' incoming and outgoing payment transactions, and to store and archive such transactions.</p>	<p>payment transactions and all the details of such transactions in general.</p>	<p>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.</p> <p>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.</p> <p>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.</p>
<p><b>Tech Service</b></p>	<p>First-level IT assistance to the users of the Bank in Luxembourg.</p>	<p>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.</p>	<p>In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) located in Luxembourg.</p>
<p><b>Technical infrastructure services</b></p>	<p>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.</p> <p>Making available, via a cloud computing-type infrastructure managed by ING Bank NV items and applications enabling a data store to be managed.</p>	<p>The data transferred concern the email service, active directory service and mobile application management of ING Staff.</p> <p>The Client's data that may be transferred are: Client reference, the name, email address, phone number, company name, email content and attachments.</p> <p>The data transferred in the private cloud computing infrastructure include those mentioned in the KYC (Know Your Customer) services and credit and market risks management services.</p>	<p>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 its subcontractors in Poland, Portugal, Romania and Ireland.</p> <p>The infrastructure platform and data is hosted and stored on a Microsoft Azure cloud platform* with servers located in the European Union in Austria, Finland, Germany, Ireland and the Netherlands.</p> <p>In this context, information is stored on the IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union in the Netherlands.</p>

	<p>Performing operational IT or maintenance tasks, including IT system relying on cloud computing.</p> <p>Using third party providers to support the technical infrastructure service, monitoring of production jobs, and incident management.</p>	<p>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 or used to manage services and products.</p>	<p>Support on the technical infrastructure services and on incident management is also provided by ING Bank NV's affiliate in Poland, 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.</p>
<p><b>IT security</b></p>	<p>Provisions of maintenance and support services relating to the Bank's applications hosted in the infrastructure.</p> <p>Management of IT security system particularly the detection and management of security incidents.</p>	<p>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).</p> <p>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.</p>	<p>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.</p>
<p><b>Portal used to facilitate the management of the products and services offered to the clients of the Bank</b></p>	<p>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.</p>	<p>The data transferred includes inter alia all data identifying the Client and the data required to take out and manage services and products:</p> <ul style="list-style-type: none"> <li>• 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 opening an account and during the entire Client relationship management period;</li> <li>• Services and Products signed up for (current accounts, savings accounts, Visa accounts, credit accounts...);</li> <li>• Payments (SEPA, standing orders, beneficiaries management, operations on accounts...);</li> <li>• Electronic documents signed or not;</li> <li>• Documents signed by the Client;</li> <li>• Proposal and subscription to products and/or services.</li> </ul>	<p>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.</p>

<p><b>Services related to printing and Client document management</b></p>	<p>Client documents formatting, printing and scanning service.</p>	<p>The data transferred concern all the Client data contained in Client documents, including the Client reference, last name and first name, address, account number, account movements, account balance, products and services subscribed.</p>	<p>In this context, some information may be made available 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 types of Client documents.</p>
<p><b>Physical archives management</b></p>	<p>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.</p>	<p>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.</p>	<p>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.</p>
<p><b>Credit Risk Management Services</b></p>	<p>Central orchestration and storage of credit applications and of Loan decisions (whether at the time of the credit application or during the life of the credit), determination of credit limits and credit exposures per Client.  Monitoring and modelling of credit and market risks and internal and external reporting of the Bank's credit risks linked to Clients in different market conditions (scenarios).</p>	<p>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: Client name, the Client reference, account number, account balance, repayment schedules, unique identifier (TIN, LEI), 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 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.</p>	<p>In this context, some information may be made available in a confidential manner, as the case may be, to Nexvia (a service provider based in Luxembourg), to ING Bank NV in the Netherlands, and its subcontractors in the Netherlands in Belgium, Poland, Slovakia and/or ING Bank NV's subsidiaries worldwide.  Some information may also be made available in a confidential manner on Google's cloud platform* whose servers are located in the European Union: in Belgium and the Netherlands.  For the risk modelling, the central platform and data are hosted and stored on a cloud infrastructure managed by ING Bank NV, whose servers are located in the European Union in the Netherlands.</p>
<p><b>Credit Risk management on capital call</b></p>	<p>Centralised platform for monitoring the use of so-called "capital call" / private equity credit lines for the purposes of managing the</p>	<p>The data transferred is of a financial nature: Client reference, account number, account balance, Type and characteristics of the products</p>	<p>In this context, some information may be made available in a confidential manner, to ING Bank NV in the Netherlands, and its</p>

<p><b>product / private equity</b></p>	<p>underlying risks (credit, operational, contractual, etc.) as well as the resulting monitoring.</p>	<p>subscribed, conditions of remuneration.</p>	<p>subcontractors in the Netherlands in Belgium, Poland, Slovakia and/or ING Bank NV's subsidiaries worldwide.</p> <p>Some information may also be made available to the service provider Genesis Global located in the United Kingdom.</p> <p>For the risk modelling, the central platform and data are hosted and stored on a cloud infrastructure managed by AWS*, whose servers are located in the United Kingdom.</p>
<p><b>Market Risk Management Services</b></p>	<p>Monitoring and modelling of market risks in general, internal reportings and export of the Bank's interest rate tradings risks and liquidity risks.</p>	<p>The data transferred are of a financial nature: the Client reference, account number, account balance, repayment schedules, type and characteristics of the products subscribed to, remuneration conditions, etc.</p>	<p>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.</p>
<p><b>Web Banking</b></p>	<p>My ING, to offer a web banking platform on iOS/Android internet and mobile applications.</p> <p>Inside Business Portal and Payment, to provide a single internet and mobile access point for Wholesale Banking Clients allowing them, amongst other, to manage their payments, to speed up account opening and onboard new legal entities, to make and/or manage FX trades and FM products, to access reporting related notably to payments and trades, bank credit and financial markets as well as to manage which individuals use Inside Business Portal and Payment on behalf of the Client.</p> <p>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 worldwide).</p>	<p>The data transferred include, <i>inter alia</i>, the Client's identity (e.g. client reference, company name, ultimate beneficial owner) and the required data to manage daily bank activities amongst others:</p> <ul style="list-style-type: none"> <li>• Authentication (LuxTrust Certificate...) and security and fraud prevention</li> <li>• Personal data (including personal data of Client employees such as first name, last name, date of birth, nationality) and consents</li> <li>• Product Overview (Current accounts, Saving accounts, Visa accounts, Loan accounts,...)</li> <li>• Payments (SEPA Payments, Standing orders, Beneficiary Management,...)</li> <li>• Alerts (email and push notifications)</li> <li>• Account balances</li> <li>• Account movements</li> <li>• Account Aggregation</li> <li>• Secure messaging</li> <li>• Electronic documents</li> <li>• Proposal and Subscription to products and/or services</li> <li>• all data related to transactions of financial instruments and other financial data held by the Client.</li> </ul>	<p>In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) located in Luxembourg currently LuxTrust, to ING Bank NV and/or its subcontractors in the Netherlands, Belgium, Romania or Poland, or even the subsidiaries or branches in which the Client also has accounts.</p> <p>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.</p>

<p><b>Services related to audit letters</b></p>	<p>Harmonising and automating the request, creation and delivery of the audit letters.</p> <p>Web-based platform enabling auditors to request audit letters directly from ING.</p>	<p>The data transferred include, <i>inter alia</i>:</p> <ul style="list-style-type: none"> <li>• Client data such as client reference, company name, ultimate beneficial owner, account names, email address</li> <li>• Client employee data such as first name and last name, email address, phone number and IP address (electronic signature data)</li> <li>• Client auditor data such as the email address, phone number and IP address (electronic signature data)</li> </ul>	<p>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.</p> <p>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.</p>
<p><b>Deal &amp; Price manager service</b></p>	<p>Pricing software tool used by the sales organisation within the ING Group in order to offer business services to Clients.</p>	<p>Client name and contact details of individuals related to the Client (e.g. employees).</p>	<p>In this context, some information may be made available in a confidential manner to ING Bank NV in the Netherlands, its worldwide subsidiaries or branches in which the Client also has accounts as well as to SunTec Business Solutions, a service provider located in India.</p> <p>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.</p>
<p><b>Digital Communication Channels</b></p>	<p>Making available secure digital communication channels such as audio calling, chat and messaging.</p> <p>These channels use Internet cloud services*.</p>	<p>The data transferred concern the information necessary to establish the communication and for speech recognition:</p> <ul style="list-style-type: none"> <li>• IP address</li> <li>• Phone number</li> <li>• Email address</li> <li>• Photo or video</li> <li>• Technical identifier of the ING Contact Person</li> <li>• Natural Language Processing (NLP, Voice recognition).</li> </ul> <p>The communications are recorded and stored by ING and may be used as means of proof in accordance with the applicable General Terms and Conditions.</p> <p>The operator of the cloud services* only has access to technical data depending on the channel (and not to the communications' decrypted content):</p> <ul style="list-style-type: none"> <li>• IP address</li> </ul> <p>The message's encrypted content (for which only ING has the decryption keys) for the duration of the</p>	<p>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 and Poland.</p> <p>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.</p>



		communication; before being deleted at the end of the call.	
<b>Multiline</b>	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 data 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: <ul style="list-style-type: none"> <li>• Authentication (LuxTrust Certificate...) and security and fraud prevention</li> <li>• Data linked to its accounts: consultation of balance and list of transactions</li> <li>• Payments (SEPA, standing order, management of payees).</li> </ul>	In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) located in Luxembourg currently Worldline Financial Services and its affiliated companies in France, Belgium and Germany without prejudice to the Instant Payment section.
<b>Central services for OTC (over-the-counter) financial instrument transactions</b>	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), the MIFID 2 regulation (including MIFIR).	The data transferred include Client entities data, including without limitation namely the Client reference, the name of the legal entity, the LEI (Legal Entity Identifier), 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 located in Belgium, Slovakia, the United Kingdom, Singapore, India and the Philippines.
<b>Central services related to acquired positions in financial instruments in the European markets</b>	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 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 SRD II (including for the proxy voting services), some information may be made available in a confidential manner to a service provider, Broadbridge Financial Solutions Ltd based 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.
<b>Management of credit or debit card management and transaction authentication via the Internet</b>	Comprehensive management of credit or debit card processing (including 3D Secure): <ul style="list-style-type: none"> <li>- 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.)</li> <li>- monitoring suspicious or fraudulent transactions</li> <li>- managing complaints at the level of the Visa network.</li> <li>- managing ecommerce transaction through 3D secure authentication.</li> </ul>	The data transferred include, inter alia, the Client reference, the 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. <p>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.</p>	In this context, some information may be made available in a confidential manner 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. <p>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.</p>
<b>Production of Credit or Debit Cards</b>	Management of the production of credit or debit cards and their delivery to Clients/cardholders.	The data transferred include in particular the Client reference, Client's or cardholder's last name, IBAN number, first name, address, and	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

		information linked to the debit or credit card.	subsidiaries) in France and/or in 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.
<b>Signature sharing platform services</b>	Use of a platform 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), 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, Ireland and Germany.
<b>Marketing Event Management Service</b>	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: <ul style="list-style-type: none"> <li>• Last name</li> <li>• First name</li> <li>• Company name for legal entities</li> <li>• Email address</li> <li>• Phone number (optional)</li> </ul>	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.  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.
<b>Cash Management</b>	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.
<b>Global Client support</b>	To provide support in subscribing to and setting up the international financial products and services offered by ING Group, particularly in the area of payments and/or cash management.	The data transferred concerning the Client include in particular: <ul style="list-style-type: none"> <li>• Name</li> <li>• Address</li> <li>• Telephone number</li> <li>• Email address,</li> <li>• Account number</li> <li>• Nationality</li> <li>• TIN</li> </ul> And the financial data include: <ul style="list-style-type: none"> <li>• Proof of payments</li> <li>• Account statements</li> <li>• Account balances</li> <li>• Bank confirmations</li> <li>• Requests for direct debits and standing orders</li> </ul>	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 worldwide in connection with the products and/or services purchased.  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.
<b>Client Relationship Management Services</b>	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	The data transferred include among others: <ul style="list-style-type: none"> <li>• Client data, notably the Client's identity and the identity of its</li> </ul>	In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands), its affiliates in Poland, in Slovakia, in the Philippines and/or

	to the Client (including its related individuals) which enables the Bank to better serve the Client.	<p>related individuals (e.g. ID documents and ID-related data), client reference, address, ownership structure, industry, town and country of incorporation;</p> <ul style="list-style-type: none"> <li>• data of Client's contact persons including name, address, job title, date of birth and contact details such as telephone number, email address, LinkedIn profile.</li> <li>• data from Client interactions, such as meeting minutes, participation to campaigns and events product characteristics and financial data, such as credit and market risk limits, outstanding balances, account references, IBAN, transactions, incoming and outgoing funds.</li> </ul>	<p>to its other subsidiaries or branches worldwide. 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.</p> <p>ING also uses a service platform from SFDC Ireland Ltd (Salesforce) hosted in a cloud* platform of Amazon Web Services (AWS), whose data remains in the European Union databases located in Ireland, France and Germany.</p> <p>Moreover, ING uses a client software tool to better understand and serve clients. In relation to this tool, the Bank uses both the cloud platform of Microsoft 365* and the IPC cloud infrastructure managed by ING Bank NV, whose data remains in the European Union in the Netherlands.</p>
<b>Lending Administration Services</b>	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.	<p>The data transferred include all information related to credit applications and supporting documents.</p> <p>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).</p>	<p>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.</p> <p>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.</p>
<b>Consolidated regulatory Reporting of the Bank</b>	Consolidation of COREP (Common Reporting Framework) and EBA (European Banking Authority) regulatory reports.	The data transferred are 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.	<p>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.</p> <p>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.</p> <p>The data will remain in the European Union, in Solvinity's databases in the Netherlands.</p>

<p><b>Automated translation system</b></p>	<p>Translation tool using artificial intelligence.</p>	<p>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, procedures, reports, product and support information, websites, etc.</p>	<p>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.</p>
<p><b>Infrastructure of ING Luxembourg employees' emails and archiving</b></p>	<p>Provision of the exchange Online O365 messaging infrastructure for the Luxembourg entity managed by ING Bank NV.</p> <p>This infrastructure has an archive managed by ING Bank NV (Netherlands), all emails sent to and from ING mailboxes.</p> <p>Exchange O365 is a cloud computing infrastructure managed by ING Bank NV (the Netherlands).</p>	<p>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 employee calendar, contacts, and all email-related features.</p>	<p>In this context, certain information may be made 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.</p> <p>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.</p> <p>Archiving of these emails will also be accessible confidentially by ING Bank NV (Netherlands).</p>
<p><b>SharePoint data storage infrastructure</b></p>	<p>Provision of a Microsoft SharePoint type data sharing infrastructure for ING Luxembourg managed by ING Bank NV.</p> <p>SharePoint is a cloud computing infrastructure managed by ING Bank NV (Netherlands).</p>	<p>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.</p>	<p>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.</p>
<p><b>Contact Center</b></p>	<p>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.</p> <p>Provision of technological and application infrastructure elements through a cloud infrastructure managed by ING Bank NV to manage a data warehouse.</p>	<p>The data transferred are those contained in the call transferred, the telephone number, the customer's first and last name.</p> <p>Communications transferred are recorded and stored by ING Belgium and may be used as evidence in accordance with the applicable General Terms and Conditions.</p>	<p>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.</p> <p>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.</p>
<p><b>Reporting service in accordance with the Central Electronic System for Payment Information (CESOP) regulations</b></p>	<p>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</p>	<p>The data transferred relates to, but is limited to:</p> <ul style="list-style-type: none"> <li>• The BIC or other business identification code that identifies the payment service provider responsible for reporting,</li> <li>• The name or business name of the beneficiary,</li> <li>• The VAT identification number or any other national tax number of the beneficiary,</li> </ul>	<p>In this context, certain information may be made available in a confidential manner to ING Bank NV (Netherlands).</p> <p>The information is stored on the IPC cloud infrastructure, managed by ING Bank NV in the Netherlands, whose servers are located in the European Union in the Netherlands.</p>

	<p>(EU) No 904/2010, as may be amended.</p>	<ul style="list-style-type: none"> <li>• The IBAN number or any other identifier that identifies the beneficiary and his/her location,</li> <li>• The address of the beneficiary,</li> <li>• Whether it is a payment or refund,</li> <li>• The date and time of payment or refund of payment,</li> <li>• The amount and currency of the payment or refund of payment,</li> <li>• The country code of the Member State of origin of the payment,</li> <li>• The country code of the Member State of destination of the refund,</li> <li>• The information used to determine the origin or destination of the payment or refund of payment,</li> <li>• Any reference that identifies the payment, and</li> <li>• Where applicable, all information indicating that the payment is initiated at the merchant's premises.</li> </ul> <p>The information transmitted varies depending on the payment method used.</p> <p>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).</p>	
<p><b>Reporting service in accordance with the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standard (CRS) regulations</b></p>	<p>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.</p>	<p>The data transferred includes the following:</p> <ul style="list-style-type: none"> <li>• Name and surname of individuals</li> <li>• Company name</li> <li>• Postal address</li> <li>• Customer number</li> <li>• Date of birth</li> <li>• Company number</li> <li>• Bank account</li> <li>• Account balance</li> <li>• Financial details</li> <li>• Products and services used</li> <li>• Tax identification number(s)</li> <li>• Tax residence(ies)</li> <li>• Role between physical and legal persons (Ultimate Beneficial Owner)</li> <li>• FATCA and CRS statutes</li> </ul>	<p>In this context, certain information may be made available on a confidential basis to ING Bank NV (Netherlands).</p> <p>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.</p>
<p><b>Trading and contract management services for International Swaps and Derivatives Association "ISDA" and related collateral</b></p>	<p>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).</p>	<p>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.</p>	<p>In this context, certain information may be made available confidentially to ING Bank NV (Netherlands) and its branch in Belgium.</p>

<p><b>Internal Control Process</b></p>	<p>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.</p>	<p>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. Know Your Customer, Payment, Fraud, Market Abuse).</p>	<p>In this context, some information may be made available in a confidential manner to ING Bank NV (Netherlands) and/or its affiliates in Slovakia, Romania, and in the Philippines.</p>
<p><b>Client survey</b></p>	<p>Service to request and analyse Client feedback to better understand Clients' needs and expectations on the banking services, products or relationship.</p>	<p>The following data are transferred:</p> <ul style="list-style-type: none"> <li>• Name and surname of individuals</li> <li>• Professional email</li> <li>• Company name</li> <li>• Customer number; and</li> <li>• the answers collected during the survey(s).</li> </ul>	<p>In this context, certain information may be made available on a confidential basis to ING Bank NV (Netherlands) and to a service provider, Medallia Inc based in the USA, and its subcontractors. These providers store the information in the European Economic Area (with back-up in Germany) and in the United Kingdom and may also remotely access these data from India and the USA on an occasional basis.</p>
<p><b>Services of complementary research in case of dormant or inactive account and inactive safe deposit boxes</b></p>	<p>Using a third party provider to perform complementary research to obtain and use information on dormant/inactive accounts, 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.</p>	<p>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.</p>	<p>In this context, some information may be made available in a confidential manner to Dynaslux, a third party provider licensed as PSA (<i>Professionnel du Secteur des Assurances</i>) located in Luxembourg and to its subcontractors (including Finaca, ARCA CONSEIL, DETECNET, ARGENE) located in the European Union, in France.</p>
<p><b>Whistleblowing process</b></p>	<p>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.</p> <p>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).</p>	<p>Any (personal) data regarding the Client might be included in whistleblower reports.</p>	<p>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.</p> <p>Some information may be stored on the AWS cloud infrastructure* whose servers are located in the United Kingdom.</p>