

## APPENDIX 2 - OUTSOURCING

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

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

This table will be applicable as of 15 July 2023 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 30 September 2023.

	Description of the service	Type of shared data	Access to the data
<b>Services of access services for Third-Party Payment Service Providers under the Payment Services Directive (PSD2)</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 with the applicable regulations regarding payment services regulations.</p>	<p>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.</p>	<p>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 entity and/or (iii) to its subcontractors in the Netherlands, Germany, Spain, Belgium, Romania and Poland.</p>
<b>Know Your Customer (KYC) Services</b>	<p><b>CUSTOMER DUE DILIGENCE (CDD) PERFORMANCE AND REVIEW</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 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, CRS, MiFID, MAR etc.</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 ING Bank NV (Netherlands) and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, Poland, and Slovakia.</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><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 from other 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 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.</p> <p>Moreover, 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 “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, branches and/or subcontractors in the Netherlands, Romania, the Philippines and Slovakia.</p> <p>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.</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.</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 legislation and in particular 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 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 (the Netherlands) and/or to its subsidiaries, branches and/or subcontractors in the Netherlands, Poland, Slovakia and the Philippines.</p>

\* 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><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 legislation 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, and Slovakia.</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>To process and execute all processes related to Clients' incoming and outgoing payment transactions, and to store and archive such transactions.</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 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.</p>	<p>In this context, some information may be made available in a confidential manner to Swift ING Belgium and/or its subcontractors in the Netherlands, Poland or Slovakia.</p>
	<p><b>INSTANT PAYMENT</b></p> <p>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.</p> <p>To track and monitor payment transactions initiated or received centrally at ING Group level for all ING entities, including ING Luxembourg.</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.</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, the Netherlands, India and in the United Kingdom.</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 accessible in a confidential manner to a Financial Sector Professional (FSP) located in Luxembourg.</p>
<p><b>Technical infrastructure services</b></p>	<p>Provision of an infrastructure hosting the Bank's applications to a Financial Sector Professional</p>	<p>The data transferred concerns the email service, active directory service and mobile application management of ING Staff.</p>	<p>In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) located in</p>

\* 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>(FSP) in addition to a workstation infrastructure managed by ING Bank NV 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 of items and applications enabling a data store to be managed.</p>	<p>The Client's data that may be transferred include: the Client reference, name, email address, phone number, company name, email content and attachments.</p> <p>The data transferred in the private cloud computing infrastructure are the same as mentioned in the KYC and credit and market risks management services.</p>	<p>Luxembourg and to ING Bank NV (Netherlands) and/or to its partners in Poland, Portugal and Ireland.</p> <p>The infrastructure platform and data are hosted on a Microsoft Azure cloud platform* whose servers are located in the European Union, in Austria, Finland, Ireland and the Netherlands.</p> <p>In this context, some information may be stored on an IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands</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 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: 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 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.</p>	<p>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.</p>
<p><b>Credit Risk Management Service</b></p>	<p>Central orchestration and storage of credit applications and decisions (whether the time of application and during the life of the loan), determination of credit limits and credit exposures per Client.</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.</p>	<p>In this context, some information may be made available in a confidential manner to a third party in Luxembourg, ING Bank NV in the Netherlands, and its subcontractors in the Netherlands in Belgium,</p>

\* 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.

	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).	<p>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.</p> <p>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>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.</p>	<p>Poland, Slovakia and/or ING Bank NV's subsidiaries worldwide.</p> <p>The central platform and the data are hosted and stored on an IPC cloud infrastructure managed by ING Bank NV, whose servers are located in the European Union, in the Netherlands.</p> <p>The infrastructure platform and the data transmitted to the third party in Luxembourg are hosted and stored on an Amazon Web Services cloud platform* whose servers are located in the European Union in Ireland.</p>
<b>Market Risk Management Services</b>	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 subsidiary in Belgium.

\* 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><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 Business Banking Clients to manage their payments and access reporting related to payments, credit and financial markets.</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 across the world).</p>	<p>The data transferred include, <i>inter alia</i>, the Client's identity and the required data to manage daily bank activities including inter alia:</p> <ul style="list-style-type: none"> <li>• Authentication (LuxTrust Certificate...) and security and fraud prevention</li> <li>• Personal data 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>• Mobile payments with Payconiq</li> <li>• Account balances</li> <li>• Account movements</li> <li>• Alerts (email and push notifications)</li> <li>• Account Aggregation</li> <li>• Secure messaging</li> <li>• Electronic documents</li> <li>• Proposal and Subscription to products and/or services</li> </ul>	<p>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, or Poland.</p>
<p><b>Digital Communication Channels</b></p>	<p>Making available secure digital communication channels such as audio calling, chat messaging and messaging.</p> <p>These channels use Internet cloud services*.</p>	<p>The data transferred concerns 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> <li>• Technical identifier of the ING Contact Person</li> </ul> <p>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):</p> <ul style="list-style-type: none"> <li>• IP address</li> <li>• 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.</li> </ul>	<p>In this context, some information may be made available in a confidential manner to ING Bank NV (the Netherlands) and/or its subcontractors in the Netherlands, Belgium or 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>

\* 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><b>Multiline (for companies only)</b></p>	<p>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.</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• Authentication (LuxTrust Certificate...) and security and fraud prevention</li> <li>• Data related to their accounts: consultation of balance and transaction list</li> <li>• Payments (SEPA, standing order, management of payees),</li> </ul>	<p>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.</p>
<p><b>Central services for OTC financial instruments transactions</b></p>	<p>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 EMIR, MIFID, or MIFIR regulations.</p>	<p>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.</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, Slovakia, the United Kingdom, Singapore, India and the Philippines.</p>
<p><b>Central services related to acquired positions in financial instruments in the European markets.</b></p>	<p>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).</p>	<p>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.</p>	<p>In addition to information transmitted to the relevant issuer as per SRDII (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.</p>
<p><b>Management of Credit or Debit Card and transaction authentication via the Internet</b></p>	<p>Comprehensive management of credit or debit cards (including 3D Secure):</p> <ul style="list-style-type: none"> <li>- at the level of the transactions made with these cards, but also of the life cycle of the cards (ordering, blocking, contactless function, ...)</li> <li>- monitoring of suspicious or fraudulent transactions</li> <li>- managing complaints in the Visa network</li> <li>- managing ecommerce transaction through 3D secure authentication</li> </ul>	<p>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.</p> <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>	<p>In this context, certain information may be made available on a confidential basis to ING Bank NV (Netherlands), its subsidiaries in Poland and to Financial Sector Professionals (FSP) in Luxembourg, namely (i) LuxTrust and (ii) Worldline Financial Services and its affiliated companies in France, Belgium, and Germany.</p>

\* 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.

<b>Production of Credit or Debit Cards</b>	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, first name, 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 Bank NV in the Netherlands or its subsidiaries in Poland and/or to their partner Thales (or its subsidiaries) in France and/or Germany.
<b>Signature Sharing Platform Service</b>	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 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.
<b>Marketing Event Management service</b>	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: <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>• Telephone number (optional)</li> </ul>	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.
<b>Client Relationship Management Services</b>	To record, view and share information provided by the Client or any other Client-related information on centralised platforms with ING Bank NV and its subsidiaries, for the purpose of improving Client service.	The data transferred includes, in particular: <ul style="list-style-type: none"> <li>• The Client's data including identity, address, ownership structure, city and country of incorporation.</li> <li>• The 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.</li> <li>• Data on exchanges with the Client such as minutes of meetings, participation in campaigns or events.</li> <li>• Product characteristics such as credit or market risk limits, outstanding balances, account numbers.</li> </ul>	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.

\* 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><b>Consolidated regulatory reporting of the Bank</b></p>	<p>Consolidation of COREP and EBA regulatory reports.</p>	<p>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.</p>	<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. 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, contracts, procedures, reports, product and support information, websites, etc.</p>	<p>In this context, certain information may be stored on an 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, of all emails sent to and from ING mailboxes</p> <p>Exchange O365 is a cloud computing infrastructure managed by ING Bank NV (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 the employee calendar, contacts, and all email-related features.</p>	<p>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.</p> <p>Archiving of these emails will also be accessible confidentially by ING Bank NV.</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 during high traffic 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 to ING Belgium, the telephone number, the customer's first and last name.</p> <p>Communications transferred to ING Belgium are recorded and stored by ING Belgium and may be used as evidence in accordance with the applicable General Terms and Conditions.</p>	<p>In this context, certain information may be made available in a confidential manner to ING Belgium.</p> <p>In this context, certain information may be stored on an IPC cloud infrastructure, managed by ING Bank NV, whose servers are located in the European Union in the Netherlands.</p>

\* 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><b>Reporting service in accordance with the Central Electronic Payment Information System ("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 (EU) No 904/2010, as may be amended.</p>	<p>The data transferred relates to, but is not 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> <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 refund,</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>In this context, certain information may be made available in a confidential manner to ING Bank N.V. (Netherlands).</p> <p>The information is stored on an IPC cloud platform 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>

\* 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.