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

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

	Description of the service	Type of shared data	Access to the data
Services of access services for Third-Party Payment Service Providers under the Payment Services Directive (PSD2)	To enable Third-Party Payment Service Providers (Third-Party PSPs) to collect information on accounts, to initiate payment operations and to confirm the availability of funds in accordance with the legal obligations of the Bank and with the applicable regulations regarding payment services regulations.	The data transferred include, inter alia, the Customer's identity, his country of residence, his IBAN, his associated means of authentication (including the LuxTrust certificate), the associated link between the Customer and his payment accounts, his account balances, the availability of existing funds in the accounts at any given time, and the details of the payment operations performed.	In this context, certain information may be made available on a confidential basis to the ING Bank NV entity and/or to its subcontractors in the Netherlands, Germany, Spain, Belgium, Romania or Poland.
Know Your Customer (KYC) Services	To perform in a centralised manner, the necessary controls and checks on the basis of applicable national and international legislation and regarding, in particular, identification of customers and beneficial owners, regular media screening relating to clients, their agents, representatives and UBOs, monitoring of transactions and anti-money laundering and counter-terrorist financing, both upon opening accounts and throughout the lifetime of these accounts. This centralised management will also enable the Bank to classify its customers on the basis of their specific situation as regards various applicable regulations such as applicable legislation on anti-money laundering and the financing of terrorism, FATCA, CRS, MiFID, etc.	The data transferred relate to all the identifying data of the Customer and, where applicable, of their officers and beneficial owners including their identifying data, date and place of birth, passport number, national and/or tax identification number, address, place of residence, telephone number, and in general all the data communicated when opening the account or thereafter with regard to KYC and source of funds and all the information communicated to the Bank during each transaction performed on the accounts opened with the Bank. The data transferred to the service provider appointed by ING for the media screening Regulatory DataCorp Ltd (or any other entity of its group) are the name, surname, date of birth and country of residence.	In this context, some information may be made available in a confidential manner to Financial Sector Professionals (FSP) located in Luxembourg and their subsidiaries located in Europe (including in Poland and in Hungary) as well as ING Bank NV and/or to its subsidiaries and branches and/or subcontractors in The Netherlands, Poland, the United Kingdom, Slovakia, Romania, and Philippines. Some data relating to the customer may be made available, in connection with the screening, to the provider based in the UK. The screening and its results will be recorded in a database stored on a cloud platform* managed by Amazon Web Services (AWS), whose servers are located in Ireland and Germany.
Swift and Payment Services Platforms	To process payment transactions via Swift and send messages via the same service, generally speaking, in addition to storing and archiving such messages and monitoring, filtering and verifying the said payment transactions or messages. To process and execute all processes related to customers' incoming and outgoing payment transactions and to store and archive such transactions.	The data transferred relate to all the data included in the various fields in the messages or payment systems (Swift or otherwise), including but not limited to: the Customer's identity, his address, his IBAN, his account balance, the activity on the accounts, the identity of the instructing parties or beneficiaries of payment transactions and all the details of such transactions in general.	In this context, some information may be made available in a confidential manner to Swift, ING Belgium and/or to its subcontractors including Equens Worldline in the Netherlands, Poland or Slovakia.

1 *The subcontractors thus designated by the Bank may be regulated or unregulated entities that are either subject by law to an obligation of professional secrecy or contractually required by the Bank to comply with strict rules of confidentiality.*

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

Tech Service	First-level IT assistance to the users of the Bank in Luxembourg..	Under this contract the service provider may have access, occasionally and within the framework of the IT assistance, to any data hosted on the Bank's IT infrastructure.	In this context, some information may be made accessible in a confidential manner to a Financial Sector Professional (FSP) located in Luxembourg.
Technical infrastructure services	Provision of an infrastructure hosting the Bank's applications to a Financial Sector Professional (FSP) in addition to a workstation infrastructure managed by ING Bank NV (Netherlands) allowing a secure workplace environment including email service, active directory service and mobile application management service as well as physical desktops, File Servers and Shared Service Desk. Making available, via a cloud computing-type infrastructure managed by ING Bank NV (in the Netherlands) items and applications enabling a data store to be managed.	The data transferred concerns the email service, active directory service and mobile application management of ING Staff. The, Customer's data that may be transferred include (without limitation): name, email address, phone number, company name, email content and attachments. The data transferred in the private cloud computing infrastructure are the same as mentioned in the KYC and credit and market risks management services.	In this context, some information may be made available in a confidential manner to a Financial Sector Professional (FSP) located in Luxembourg and to ING Bank NV (Netherlands) and/or to its partners in Poland, Portugal and Ireland. The infrastructure platform and data will be hosted on a Microsoft Azure cloud platform* whose servers are located in the European Union, Austria, Finland, Ireland and the Netherlands. Regarding the ING private cloud managed by ING Bank NV, only Luxembourg ING's employees have access to the data stored on it.
Services related to the printing and management of customer documents	Customer documents formatting, printing and scanning service.	The data transferred includes all customer data contained in customer documents, such as first and last name, address, account number, transactions and account balance.	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 of various types of costumer documents.
Credit Risk Management Service	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 customer. Monitoring and modelling of credit and market risks, internal and external reporting of the Bank's credit risks indifferent market conditions (scenarios).	The data transferred includes all customer data relating to a credit application, a modification or any other event related to the life cycle of the product as well as any supporting documents. It includes notably, the identity of the Customer (or the guarantor), the object being financed, the Customer's ownership structure, the identity of investors (or the guarantor), know your customer due diligence information, financial data of the Customer (such as balance sheet, turnover, number of employees, performance), sureties and guarantees, and any other financial information held by the Bank in relation to the Customer (such as	In this context, certain information may be made available on a confidential basis to ING Bank NV in the Netherlands, Belgium, Slovakia, Poland and/or to its subsidiaries worldwide.

* 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.

		credit or debit balance, existing credit facilities or other loans granted by the Bank and their outstanding amounts).	
Market Risk Management Services	Monitoring and modelling of market risks in general, internal reportings and export of the Bank's interest rate tradings risks and liquidity risks.	The data transferred are of a financial nature: customer 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 in the Netherlands or to its subsidiary in Belgium.
Web Banking	MyING, to offer a Web Banking platform on iOS/Android internet and mobile applications. Inside Business Portal and Payment, to provide a single internet and mobile access point for Business Banking customers to manage their payments and access reporting related to payments, credit and financial markets.	The data transferred include, *inter alia*, the Customer's identity and the required data to manage daily bank activities amongst others: • Authentication and security and fraud prevention • Personal data and consents • Product Overview (Current accounts, Saving accounts, Visa accounts, Loan accounts…) • Payments (SEPA Payments, Standing orders, Beneficiary management…) • Mobile payments with Payconiq • Account balances • Account movements • Alerts (email and push notifications) • Account Aggregation • Secure messaging • Electronic documents • Proposal and Subscription to products and/or services	In this context, certain information may be made available on a confidential basis to a Financial Sector Professional (FSP) located in Luxembourg, to ING Bank NV and/or its subcontractors in the Netherlands, Belgium or Poland.
Digital Communication Channels	Making available secure digital communication channels (video conferencing, audio calling, chat and messaging). These channels use Internet cloud services.	The data transferred concerns the information necessary to establish the communication: • IP address • Phone number • Email address • Photo or video • Technical identifier of the ING contact person The communications are recorded and stored by ING and may be used as evidence in accordance with the applicable General Terms and Conditions. The operator of the Cloud services only has access to the technical data according to the channel (and not to the decrypted content of the communications): • IP address	In this context, some information may be made available in a confidential manner to ING Bank NV and/or its subcontractors in the Netherlands, Belgium or Poland. The infrastructure platform and the data will be hosted on an Amazon Web Services (AWS) cloud* platform located in the European Union in Ireland and Germany. As regards the private cloud operated by ING Bank NV (Netherlands), only ING Luxembourg employees have access to the data stored there.

* 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.

		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.	
Multiline (for companies only)	Hosting and management of the Multiline multi-banking platform through which any company having subscribed to this service can, in particular, consult data linked to its bank accounts and initiate payment transactions.	The data transferred includes, among other things, the identity of the customer and the data necessary to manage their accounts on a daily basis, including: • Authentication and security and fraud prevention • Data related to their accounts: consultation of balance and transaction list • Payments (SEPA, standing order, management of payees),	In this context, certain information may be made available on a confidential basis to a Financial Sector Professional (FSP) located in Luxembourg.
Central services for OT financial instruments transactions	All OTC transactions between the customer entity and the Bank are centralised on ING Bank NV's platforms in the Netherlands, in order to improve customer service and to allow for central monitoring and legal controls, including without limitation for EMIR, MIFID, or MIFIR regulations.	The data transferred includes data of the Customer entities, notably the legal entity name, Legal Entity Identifier, contact e-mails and transactions details.	In this context, some information may be made available in a confidential manner to ING Bank NV in the Netherlands and/or to its subsidiaries or branches in Belgium, Slovakia, the United Kingdom, Singapore, India and the Philippines.
Central services related to acquired positions in financial instruments in the European markets.	In order to identify shareholders, 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).	The data transferred includes, in particular: Customer name, postal address, email address, unique identifier (TIN, LEI), position held of the security concerned in addition to the Customer's choice in case of voting at the general meeting.	In this context, certain information may be made available on a confidential basis to a service provider, Broadbridge Financial Solutions Ltd, located in the United Kingdom and to a cloud infrastructure solution (IBM-Managed Private Cloud)* whose servers are located in the European Union, in France and Germany.
Management of credit or debit card	Comprehensive management of credit or debit cards: - at the level of the transactions made with these cards, but also of the life cycle of the cards (ordering, blocking, contactless function, ...) - monitoring of suspicious or fraudulent transactions - managing complaints in the Visa network	The data transferred includes the Customer's first and last name, address, IBAN number and the availability of funds in the accounts linked to the Customer's cards at any given time. The data managed by the service providers includes card information and details of card transactions.	In this context, certain information may be made available on a confidential basis to ING Bank NV (Netherlands), its subsidiaries in Poland and a Financial Sector Professional (FSP) in Luxembourg, namely Worldline Financial Services.

* 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.

Production of credit or debit cards	Managing the production of credit and debit cards and their delivery to customers/ card holders.	The data transferred includes the Customer'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.
Signature Sharing Platform Service	Use of a platform in order to collect electronic signatures for legal documentation between the Bank and its Customers.	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.
Marketing event management service	Use of an external platform to collect electronic registrations of guests, customers and prospects at marketing events organised by ING Luxembourg	The data transmitted concerns the following identification data (directly encoded) by the person registering for such an internet marketing event in response to his/her invitation: • Last name • First name • Company name for legal entities • Email address • Telephone number (optional)	In this context, certain information may be made available on a confidential basis to ING Bank NV in the Netherlands or its subsidiary in Belgium and to its partner Via Futura Bvba established in Belgium. The data will be recorded in a database on an Amazon Web Services (AWS) cloud* platform with servers located in the European Union, in Belgium and the Netherlands and in the United States ~~for~~ as regards the email address.

* 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.

Customer Relationship Management Services	To record, view and share information provided by the Customer or any other customer-related information on centralised platforms with ING Bank NV and its subsidiaries, for the purpose of improving customer service.	The data transferred includes, in particular: • The Customer's data including identity, address, ownership structure, city and country of incorporation. • The data of the Customer's contact persons including name, address, position, date of birth and contact data such as telephone number, email address, LinkedIn profile. • Data on exchanges with the Customer such as minutes of meetings, participation in campaigns or events. • Product characteristics such as credit or market risk limits, outstanding balances, account numbers.	In this context, certain information may be made available on a confidential basis to ING Bank NV in the 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* where the servers are located. The 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.