Annexe 2 - Externalisation

Business Banking

Edition juillet 2026

Sous la surveillance de la Commission de Surveillance du Secteur Financier (CSSF), 283 route d'Arlon, L-2991 Luxembourg, tél. +352.262511

ING Luxembourg, Société Anonyme
26, Place de la Gare L-2965 Luxembourg
R.C.S. Luxembourg B. 6041, TVA LU 11082217

Téléphone : + 352 44 99 1
Fax : +352 44 99 2310
BIC : CELLLULL, www.ing.lu

ANNEXE 2 - EXTERNALISATION

"DOCUMENT RECAPITULATIF - Infrastructures communes de tiers et/ou du groupe ING[1] "
(voir l'**article A.9 bis** Externalisation des "Conditions Générales Business Banking")

Les présentes informations sont applicables à compter du 1er juillet 2026 aux clients du segment Business Banking. Néanmoins pour les Clients Business Banking ayant noué et maintenu une relation bancaire avec ING Luxembourg préalablement à cette date, ces présentes informations n'entreront en vigueur qu'au 1er septembre 2026.

Services d'accès aux Prestataires de Services de Paiement Tiers dans le cadre de la Directive révisée sur les Services de Paiement (PSD2)

- **Description des services :**
  Permettre aux Prestataires de Services de Paiement Tiers (PSP Tiers) de collecter les informations sur les comptes, initier des opérations de paiement et confirmer la disponibilité de fonds conformément aux obligations légales de la Banque et à la réglementation applicable en matière de services de paiement.

- **Type de données partagées :**
  Les données transférées incluent notamment l'identité du Client, son pays de résidence, son numéro IBAN, ses moyens d'authentification associés (dont le certificat LuxTrust), le lien associé entre le Client et ses comptes de paiement, le solde de ses comptes, la disponibilité de fonds existants sur les comptes à un moment donné, ainsi que le détail des opérations de paiement effectuées.

- **Accès aux données :**
  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à (i) un Professionnel du Secteur Financier (PSF) situé au Luxembourg, à savoir LuxTrust, (ii) à ING Bank NV (Pays-Bas) et/ou (iii) à ses sous- traitants aux Pays-Bas, en Allemagne, Espagne, Belgique, Roumanie et en Pologne.

---

1 Les sous-traitants ainsi désignés par la Banque sont des entités régulées qui sont soumises par la loi à une obligation de secret professionnel ou contractuellement tenues par la Banque à se conformer à des règles strictes de confidentialité.

** Cependant, au regard des lois américaines applicables en la matière et des liens du fournisseur de la plateforme en nuage (cloud*) avec les Etats-Unis, il ne peut être exclu que certaines données puissent exceptionnellement être accessibles par les autorités américaines.*

Services de connaissance du Client (KYC – Know Your Customer)

- **Description des services :**
  - **Performance et examen du devoir de vigilance à l'égard de la clientèle** :
    Dans le cadre de la surveillance des transactions et de la lutte contre le blanchiment d'argent et du financement du terrorisme, effectuer de manière centralisée la collecte, les contrôles et vérifications nécessaires sur base des lois nationales et internationales applicables et notamment en matière d'identification des Clients, de leurs mandataires ou représentants légaux et des bénéficiaires économiques effectifs, de ou toute autre documentation liée à ceux-ci ou aux transactions du Client avec la Banque, tant lors de l'ouverture des comptes que durant toute la durée de vie de ceux-ci. Cette gestion centralisée permettra aussi à la Banque de classifier ses Clients sur base de leur situation propre au regard des diverses lois et réglementations applicables comme les lois celles applicables en matière de lutte contre le blanchiment et le financement du terrorisme, de réglementation FATCA, de réglementation CRS, de réglementation MiFID 2, de réglementation sur les abus de marché, etc.

  - **Collecte de données** :
    Obtention de données de sources publiques et privées de manière centralisée par le Groupe ING.

  - **Vérification par nom (screening)** :
    Effectuer de manière centralisée au sein du Groupe ING le screening par nom nécessaire pour identifier les Clients, leurs mandataires ou représentants (légaux) et bénéficiaires effectifs sur base des normes et/ou lois nationales et internationales applicables et notamment en matière d'identification des Clients et bénéficiaires effectifs, de blanchiment et de financement du terrorisme, tant lors de l'ouverture des comptes que durant toute la durée de vie de ceux-ci.

    Par ailleurs, un screening dans les médias des personnes mentionnées ci-dessus est également centralisé au sein du Groupe ING, à noter que la veille médiatique négative (ou *adverse media screening*) est inclue dans cette catégorie dite de « vérification par nom ».

  - **Vérification préalable des transactions (pré-transaction screening)** :
    Effectuer de manière centralisée au sein du Groupe ING le screening préalable, les contrôles et vérifications nécessaires sur les transactions et opérations des comptes du Client sur base des lois nationales et internationales applicables et notamment en matière de blanchiment et de financement du terrorisme.

  - **Surveillance postérieure des transactions (post-transaction monitoring)** :
    Effectuer de manière centralisée au sein du Groupe ING la surveillance postérieure des transactions et opérations des comptes du Client et les contrôles, vérifications et investigations nécessaires sur base des lois nationales et internationales applicables en matière de blanchiment et de financement du terrorisme.

- **Type de données partagées :**
  - **Performance et examen du devoir de vigilance à l'égard de la clientèle, vérification préalable des transactions (pré-transaction screening)** et **surveillance postérieure des transactions (post-transaction monitoring) :**

    Les données transférées concernent toutes les données d'identification du Client, la référence Client, et, le cas échéant, de ses mandataires ou représentants (légaux) et bénéficiaires effectifs, dont leurs éléments d'identité, profession, date et lieu de naissance, numéro de passeport, numéro d'identification national et ou fiscal, adresse, lieu de résidence, numéro de téléphone, toute donnée publique concernant les mêmes personnes et, de manière plus générale, toutes les données communiquées lors de l'ouverture du compte ou par la suite en matière de connaissance du Client et d'origine des fonds et tous les éléments communiqués à la Banque lors de chaque transaction effectuée sur les comptes ouverts auprès de la Banque.

  - **Collecte de données** :

    Les données transférées sont : nom de l'entité, identifiant unique (LEI), pays d'incorporation, l'adresse. Elles sont utilisées pour collecter des données auprès de sources publiques et payantes via un système automatisé pour faciliter le KYC sur ladite entité.

    Les données personnelles suivantes des représentants légaux et bénéficiaires effectifs sont également collectés : nom, prénom, date de naissance, pays de résidence et si disponible, nationalité, adresse de résidence, numéro carte d'identité ou passeport.

  - **Vérification par nom (screening)** :

    Outre ce qui est mentionné ci-dessus à la rubrique « Performance et examen du devoir de vigilance à l'égard de la clientèle », les données transférées pour réaliser le screening sont le prénom, le nom, la date de naissance et le pays de résidence.

    Pour réaliser le screening, les données transférées sont le prénom, le nom, la date de naissance et le pays de résidence.

- **Accès aux données :**
  - **Performance et examen du devoir de vigilance à l'égard de la clientèle** :

    Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses filiales, succursales et/ou sous-traitants aux Pays-Bas, en Pologne, aux Philippines et en Slovaquie.

    Ces informations peuvent être stockées sur l'infrastructure informatique en nuage privé IPC (ING Private Cloud*), gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

  - **Collecte de données** :

    Dans ce contexte, ING fait appel au prestataire de services Encompass Corporation qui traite les données au Royaume-Uni et aux Pays-Bas. Certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses filiales, succursales et/ou sous-traitants aux Pays-Bas et en Slovaquie.

    Si le Client est aussi Client d'une autre entité ING, les données peuvent être partagées avec tout autre entité du Groupe ING à travers le monde.

Les résultats sont enregistrés dans une base de données logée sur une plateforme en nuage (cloud)* d'Amazon Web Services (AWS), dont les serveurs sont localisés dans l'Union européenne en Irlande.

- **Vérification par nom (screening)** :
  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses filiales, succursales et/ou sous-traitants aux Pays-Bas, en Pologne, en Roumanie, aux Philippines et en Slovaquie. Ces informations peuvent être stockées sur l'infrastructure en nuage (cloud*) privé IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

  Certaines données relatives aux personnes soumises au screening dans les médias peuvent être rendues accessibles au fournisseur Regulatory Data Corp Ltd basé au Royaume-Uni, ainsi qu'à toute autre entité de son groupe. Dans ce contexte, le screening par nom et ses résultats sont enregistrés dans une base de données logée sur une plateforme informatique en nuage (cloud*) d'Amazon Web Services (AWS)*, dont les serveurs se trouvent dans l'Union européenne en Allemagne et en Irlande.

- **Vérification préalable des transactions (pré-screening)** :
  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) situé au Luxembourg et à ses filiales localisées en Europe (y compris en Pologne et en Hongrie) ainsi qu'à ING Belgique, ING Bank NV (Pays-Bas) et/ou leurs sous-traitants aux Pays Bas, en Roumanie, en Pologne, en Slovaquie, et aux Philippines.

  Ces informations peuvent être stockées sur l'infrastructure en nuage (cloud*) privé IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

- **Surveillance postérieure des transactions (post-transaction monitoring)** :
  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas), ses filiales, succursales et/ou ses sous-traitants aux Pays-Bas et en Pologne.

  Ces informations peuvent être stockées sur l'infrastructure en nuage (cloud*) privé IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

Services de remédiation de données

- **Description des services :**
  L'objectif de ce service est de créer, maintenir et modifier les données dans les systèmes d'ING afin de garantir l'exactitude des entrées et sorties de données pour les systèmes et processus internes, conformément aux exigences métier (par exemple, en mettant à jour les données suite à différents rapports d'exception sur la qualité des données).

- **Type de données partagées :**

  Cf. « Performance et examen du devoir de vigilance à l'égard de la Clientèle » ci-dessus.

  En particulier, les données (à caractère personnel) suivantes des représentants légaux et des bénéficiaires effectifs des Clients sont collectées : le prénom, le nom de famille et toute donnée figurant dans la documentation servant à prouver les pouvoirs et la légitimité des bénéficiaires effectifs et des mandataires des Clients. De plus, afin d'améliorer la qualité des données dans nos reportings globaux/réglementaires, les données clients potentiellement contenues dans des données de marché, des données financières, des données de risque, des données de référence produits ainsi que des données de services et de transactions seront également partagées.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV et à ses sociétés affiliées en Slovaquie et en Roumanie.

Services de support à la conformité en matière d'abus de marché, de conflits d'intérêts et de lutte contre la corruption et la subornation

- **Description des services :**

  L'objectif de ces services est notamment de permettre à la Banque d'identifier les problèmes (potentiels) (tels que les conflits d'intérêts, les délits d'initiés et les manipulations de marché) et d'évaluer, de proposer et de prendre des mesures pour assurer la conformité avec les politiques de la Banque en matière de lutte contre les abus de marché et les conflits d'intérêts.

  En outre, ces services permettent à la Banque d'enregistrer, d'évaluer et de contrôler les intérêts externes des employés d'ING, afin de gérer de manière adéquate le risque de conflits d'intérêts personnels avec les clients.

  Enfin, ces services permettent à la Banque d'enregistrer et de contrôler les cadeaux et les divertissements offerts ou reçus par les employés d'ING de la part des clients ou à leur intention, afin de gérer de manière adéquate le risque de subornation et de corruption.

- **Type de données partagées :**

  Le nom et les coordonnées du Client et tout type d'informations fournies dans les conversations enregistrées et les emails.

  Nom du Client, de son/ses représentant(s) / bénéficiaire(s) effectif(s) et détails de leur relation avec le(s) employé(s) d'ING concerné(s).

  Nom du Client, de son/ses représentant(s) / bénéficiaire(s) effectif(s) et cadeaux ou divertissements reçus ou offerts par le(s) employé(s) d'ING concerné(s).

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) est ses sociétés affiliées, y compris en

Roumanie, en Pologne et aux Philippines, ainsi qu'aux prestataires de services Workday Ltd et Kainos qui traitent les données en Irlande.

Certaines informations peuvent être stockées sur des plateformes en nuage gérées par: (1) par Amazon Web Services (AWS), avec des serveurs situés en Irlande; (2) Microsoft, avec des serveurs situés en Allemagne et en Irlande et (3) ING Bank NV, avec des serveurs situés aux Pays-Bas.

SWIFT et les plateformes de services de paiement

- **Description des services :**

  Traiter des opérations de paiement via Swift et l'envoi des messages via le même service en général ainsi que le stockage et l'archivage de tels messages ainsi que la surveillance, le filtrage et la vérification des dites opérations de paiements ou messages (y inclus les investigations liées aux paiements).

  Traiter et exécuter l'ensemble des processus liés aux opérations de paiement entrantes ou sortantes des clients ainsi que leur stockage et leur archivage.

  Effectuer des tâches dans le cadre de la vérification du bénéficiaire, le cas échéant.

- **Type de données partagées :**

  Les données transférées concernent toutes les données reprises dans les différents champs figurant dans les messages ou systèmes de paiement (Swift ou non), ou dans le cadre du processus de vérification du bénéficiaire, en ce compris, de manière non limitative : la référence Client, l'identité du Client (notamment, nom, prénom, dénomination sociale ou nom commercial), l'identifiant d'entité juridique (LEI), le numéro fiscal ou un autre identifiant unique européen, son adresse, son numéro IBAN, le solde des comptes, les mouvements sur les comptes, l'identité des donneurs d'ordre ou des bénéficiaires d'opérations de paiement ainsi que tous les détails de telles opérations en général.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à Swift, ING Bank N.V. (Pays-Bas) et/ou à ses sous-traitants en Belgique, en Roumanie, en Pologne et en Slovaquie, aux Philippines, en Inde et au Royaume-Uni.

  En ce qui concerne la vérification du bénéficiaire en particulier, certaines informations peuvent également être mises à disposition de manière confidentielle à ING Bank N.V. (Pays-Bas), sa société affiliée en Roumanie, ainsi qu'aux prestataires de services Luxhub (basé au Luxembourg), EBA Clearing (basé en France), et SurePay (basé aux Pays-Bas) qui peuvent stocker ces informations sur les plateformes cloud* AWS ou Oracle dont les serveurs situés en Allemagne et en Irlande.

Services de support technique

- **Description des services :**

  Assistance informatique aux utilisateurs (principalement les employés) de la Banque Luxembourg, incluant la gestion des incidents.

- **Type de données partagées :**

  Le prestataire peut avoir accès, de manière occasionnelle et dans le cadre de l'assistance informatique, à toute donnée hébergée sur les infrastructures informatiques de la Banque.

- **Accès aux données :**

  Dans ce contexte, certaines informations limitées peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) localisé à Luxembourg, à ING Bank NV (Pays-Bas) et au fournisseur de services, Fujitsu, établi en Belgique et qui pourra être amené à traiter les informations au Portugal.

Services d'infrastructure technique

- **Description des services :**

  (1) Mise à disposition et gestion (y compris la maintenance) d'une infrastructure hébergeant les applications de la Banque à un Professionnel du Secteur Financier (PSF) et à ses sous-traitants ainsi qu'une infrastructure de stations de travail gérée par ING Bank NV (Pays-Bas) permettant un environnement de travail sécurisé incluant les mails, l'annuaire de services d'exploitation, la gestion des ordinateurs et téléphone portable, les serveurs de fichier et helpdesk centralisé de seconde ligne.

  (2) Mise à disposition d'une infrastructure en nuage* (cloud computing) et d'une famille de produits numériques allant des réseaux, de la gestion de pare-feu, de machines virtuelles, de plateforme d'hébergement de conteneurs et de bases de données. Exécution de tâches informatiques opérationnelles ou de maintenance, y compris sur des systèmes informatiques reposant sur l'informatique en nuage.

  (3) Utilisation de prestataires de services pour soutenir les services d'infrastructure technique, le suivi des travaux de production et la gestion des incidents.

- **Type de données partagées :**

  (1) (2) (3) Les données transférées pouvant être partagées dans ce cadre incluent : la référence Client, le nom, adresse mail, contenu de l'email, numéro de téléphone, nom de sociétés et pièces jointes, les informations mentionnées dans les parties « services de connaissance du Client (KYC – Know Your Customer) » (plus haut), « service de gestions des risques de crédit » et « service de gestion des risques de marché » (plus bas), ainsi que, de manière générale, toutes les données identifiant le Client et, le cas échéant, ses mandataires, représentants (légaux) et bénéficiaires effectifs, ainsi que les données requises ou utilisées pour gérer les services et produits.

- **Accès aux données :**

  (1) Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle aux prestataires de services situés au Luxembourg, en Belgique, en Pologne et en Hongrie, ainsi qu'à ING Bank NV (Pays-Bas) et/ou à ses sous-traitants en Pologne, au Portugal et en Irlande. La plateforme d'infrastructure et les données sont hébergées et stockées sur une plateforme en nuage (cloud)* de Microsoft Azure dont les serveurs sont situés dans l'Union européenne en Autriche, en Finlande, en Allemagne, en Irlande et aux Pays-Bas.

(2) Les informations sont stockées sur l'infrastructure en nuage (cloud*) IPC, gérée par ING Bank NV, dont les serveurs sont situés dans l'Union européenne aux Pays-Bas. Un soutien opérationnel est assuré par des sociétés affiliées depuis la Roumanie et la Turquie.

(3) Le support sur les services d'infrastructure technique et sur la gestion d'incident est fourni par les sociétés affiliées d'ING Bank NV en Pologne, les prestataires de services TATA Consultancy Services Netherlands B.V., HCL Technologies B.V. (basé aux Pays-Bas), Cognizant Worldwide Limited (basé au Royaume-Uni), Infosys Ltd., Acuity Knowledge Partners, ainsi que leurs sociétés affiliées aux Pays-Bas, en Inde, aux Philippines et au Canada qui peuvent occasionnellement avoir accès à des données.

Sécurité Informatique (IT)

- **Description des services :**

  Mise à disposition de service de maintenance et de support des applications de la Banque hébergés dans les infrastructures.

  Gestion du système de sécurité informatique, en particulier la détection et la gestion des incidents de sécurité.

- **Type de données partagées :**

  Les données transférées peuvent contenir potentiellement tous types de données et informations (personnelles), documents et contrats collectés et/ou traitées par la Banque avec ses Clients dans le cadre de ses activités (par exemple, la référence Client, le nom, adresse mail, contenu de l'email, numéro de téléphone, nom de sociétés et pièces jointes).

  Pour la gestion du système de sécurité informatique, les données concernées Les données concernées dans le cadre de la gestion du système de sécurité comprennent également les données techniques contenues dans les logs et flux du système (contenant les adresses IP des utilisateurs) ainsi que les données contenues dans les flux internet entrants et sortants.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) localisé à Luxembourg (en ce compris ses sous-traitants) et à ING Bank NV (Pays-Bas) et/ou ses sous-traitants en Pologne.

Portail utilisé pour faciliter la gestion des produits et services offerts aux Clients par la Banque

- **Description des services :**

  Utilisation d'une infrastructure en nuage (cloud*) gérée par ING Bank NV (Pays-Bas) reposant sur certaines données personnelles stockées centralement à des fins de KYC (voir ci-dessus) et permettant aux commerciaux de la banque de la Banque d'accéder centralement via ce portail aux différentes applications sécurisées de la Banque et de faciliter la gestion de la relation Client sans avoir à stocker les données hors du Luxembourg une fois la recherche terminée.

- **Type de données partagées :**

  Les données transférées incluent, entre autres, toutes les données d'identification du Client et les données requises pour extraire et gérer des services et produits :

  - Données personnelles et consentements ; en particulier : la référence Client, nom du Client, adresses postales, adresses électroniques, numéros de téléphone, identifiant unique (TIN, LEI), date et lieu de naissance et, en général, toutes les données communiquées à la Banque lors de l'ouverture d'un compte et durant toute la période de gestion de la relation Client ;
  - Services et produits souscrits (comptes courants, comptes épargne, comptes Visa, comptes de crédit…) ;
  - Paiements (paiements SEPA, paiements instantanés, ordres permanents, gestion des bénéficiaires, opérations sur comptes…) ;
  - Documents électroniques signés ou non ;
  - Documents signés par le Client ;
  - Proposition et souscription aux produits et/ou services.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses sous-traitants / succursales aux Pays-Bas et en Pologne.

Services relatifs à l'impression et à la gestion de documents Clients

- **Description des services :**

  Service de mise en page et d'impression et de numérisation des documents Clients.

- **Type de données partagées :**

  Les données transférées concernent toutes les données Clients présentes dans les documents Clients, notamment la référence Client, le nom et le prénom, l'adresse, le numéro de compte, les mouvements, le solde des comptes ainsi que les produits et les services souscrits.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) localisé à Luxembourg dans le cadre de la dématérialisation des documents et l'impression, ainsi qu'à ING Belgique pour la mise en page de différents types de documents Clients.

Gestion des archives physiques

- **Description des services :**

  Stockage des archives, collecte des archives en vue de leur transport sécurisé vers l'entrepôt de stockage, retour des archives à des fins de consultation et destruction des archives avec remise d'un certificat de destruction.

- **Type de données partagées :**

  Les données transférées concernent toutes les données Clients, notamment la référence Client, le nom et le prénom, l'adresse email, les correspondances, le numéro de téléphone et toutes les autres données et documents traités lors de la relation client et contenus dans les archives physiques.

Les données utilisées pour le suivi des archives (à des fins de consultation) et pour leur destruction.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) localisé à Luxembourg et stockant les archives dans le pays. Le PSF ne gère que le contenant et non le contenu.

Services de gestion du risque crédit

- **Description des services :**

  Orchestration et stockage de manière centrale des demandes et des décisions de crédits (que ce soit lors de la demande de crédit ou pendant leur durée de vie), détermination des limites de crédit et des expositions de crédit par Client.

  Suivi et modélisation des risques de crédit et de marché, reporting interne et externe des risques de crédit de la Banque liés aux Clients dans différentes conditions de marchés (scénarios).

- **Type de données partagées :**

  Toutes les données du Client relatives à la demande initiale de prêt, aux biens (pris en sûreté ou financés), à une modification ou à tout autre événement lié au cycle de vie du produit, ainsi que tout document justificatif.

  Ces informations incluent notamment : la référence Client, le numéro de compte, le solde du compte, les échéanciers, la typologie et les caractéristiques des produits souscrits, les conditions de rémunérations, les garanties, les sûretés, les noms des éventuels garants, les actifs, les défauts, la notation du risque, adresse du bien (financé ou pris en sûreté) ; le cas échéant les informations détaillées sur le bien immobilier utilisé pour garantir la demande de crédit et toute autre information financières détenue par la Banque relative au Client (telle que le solde créditeur ou débiteur, les facilités de crédit en place ou autres prêts octroyés par la Banque et leurs montants).

  Pour les Clients personnes morales uniquement, les données transférées comprennent les données financières du Client telles que le bilan, chiffre d'affaires et nombre d'employés ainsi que les données des bénéficiaires effectifs et représentants légaux, notamment leur identité, leur adresse, leur structure propriétaire, leur secteur d'activité, leur ville et leur pays de constitution.

  Pour les Clients personnes physiques, les données transférées incluent également les données personnelles du Client, notamment son identité, sa profession, son statut matrimonial, son contrat de mariage et le nombre de ses enfants à charge.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle, le cas échéant à Nexvia (un fournisseur de services basé au Luxembourg), à ING Bank NV et ses sous-traitants aux Pays-Bas, en Belgique, en Pologne, en Slovaquie et aux Philippines.

La plateforme centrale et les données sont hébergées et stockées sur l'infrastructure en nuage (cloud*) IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

La plateforme d'infrastructure et les données transmises à Nexvia au Luxembourg sont hébergées et stockées sur une plateforme en nuage (cloud)* Amazon Web Services, dont les serveurs sont situés dans l'Union européenne en Irlande.

Service de gestion des risques de marché

- **Description des services :**

  Suivi et modélisation des risques de marché en général, reporting internes et exportation des risques de taux et de liquidité de la Banque.

- **Type de données partagées :**

  Les données transférées sont principalement des données financières : la référence Client, numéro de compte, solde de compte, échéanciers, typologie et caractéristiques des produits souscrits, conditions de rémunérations, etc.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) ou auprès de ses sociétés affiliées en Belgique, en Pologne et aux Philippines.

Web Banking

- **Descriptions des services :**

  My ING, afin d'offrir une plateforme de Web Banking sur les applications internet et mobiles iOS/Android.

  Inside Business Portal and Payment, afin d'offrir un point d'accès internet et mobile unique aux clients Business Banking en vue de gérer leurs paiements et avoir accès au reporting lié aux paiements, crédits bancaires et marchés financiers.

  Inside Business Connect, afin de permettre une connexion entre le(s) Progiciel (s) de Gestion Intégré du Client et ING Bank NV (et/ou ses filiales ou succursales de par le monde).

- **Type de données partagées :**

  Les données transférées incluent entre autres, l'identité du Client et les données nécessaires pour gérer son activité journalière notamment :

  - Authentification (certificat LuxTrust) et sécurité et prévention contre la fraude ;
  - Données personnelles et consentements ;
  - Présentation des produits (comptes courant, comptes épargne, comptes visa, comptes crédit…) ;
  - Paiements (paiements SEPA, paiements instantanés ordre permanent, gestion des bénéficiaires) ;
  - Solde des comptes ;
  - Mouvements sur les comptes ;
  - Système d'alertes (email et notifications) ;

- Agrégation des comptes ;
- Messagerie sécurisée ;
- Documents électroniques ;
- Proposition et souscription à des produits et ou services.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) localisé à Luxembourg (à savoir LuxTrust), à ING Bank NV et/ou à ses sous-traitants aux Pays-Bas, en Belgique, Roumanie, ou en Pologne.

  Ces informations peuvent être stockées sur l'infrastructure en nuage (cloud*) privé IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

Services liés aux lettres d'audit (pour les entreprises uniquement)

- **Description des services :**

  Harmoniser et automatiser la demande, la création et l'envoi des lettres d'audit. Plateforme basée sur le Web permettant aux auditeurs de demander des lettres d'audit directement à ING.

- **Type de données partagées :**

  Les données transférées comprennent entre autres :

  - Les données relatives au Client, telles que la référence du client, le nom de la société, le bénéficiaire effectif final, le nom des comptes, l'adresse email ;
  - Les données relatives aux employés du Client, telles que le prénom et le nom de famille, l'adresse email, le numéro de téléphone et l'adresse IP (données de signature électronique)
  - Les données relatives à l'auditeur du Client, telles que l'adresse email, le numéro de téléphone et l'adresse IP (données de signature électronique).

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses sociétés affiliées en Slovaquie et à l'auditeur autorisé du Client. Certaines informations peuvent être stockées sur l'infrastructure en nuage (cloud*) IPC, gérée par ING Bank NV, dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à Thomson Reuters et les données peuvent être hébergées sur l'infrastructure en nuage (cloud*) privée d'Equinix Hosting, située dans l'Union européenne aux Pays-Bas.

Canaux de communication digitaux

- **Description des services :**

  Mise à disposition de canaux de communication digitaux sécurisés tels que (appel audio, chat, et messagerie).

Ces canaux utilisent des services dans le cloud* Internet.

- **Type de données partagées :**

  Les données transférées concernent les informations nécessaires à l'établissement de la communication et à la reconnaissance vocale :

  - Adresse IP ;
  - Numéro de téléphone ;
  - Adresse email ;
  - Photo ou vidéo ;
  - Traitement automatique du langage naturel (NLP, reconnaissance vocale).

  Les communications sont enregistrées et conservées par ING et peuvent servir en tant que moyen de preuve conformément aux Conditions Générales applicables.

  L'exploitant des services cloud* n'a accès qu'aux données techniques selon le canal (et non au contenu décrypté des communications) :

  - Adresse IP
  - Le contenu encrypté du message (dont seul ING possède les clés de décryptage) pendant la durée de la communication, avant d'être supprimé à la fin de l'appel.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses sous-traitants aux Pays-Bas, en Belgique ou en Pologne.

  La plateforme d'infrastructure et les données sont hébergées dans une plateforme de nuage (cloud)* d'Amazon Web Services (AWS) et une plateforme de nuage (cloud)* Google situées dans l'Union européenne en Irlande et en Allemagne.

MultiLine (pour les entreprises uniquement)

- **Description des services :**

  Hébergement et gestion de la plateforme multi-bancaire MultiLine par laquelle toute société ayant souscrit à ce service peut notamment consulter ses données liées à ses comptes bancaires et initier des opérations de paiements.

- **Type de données partagées :**

  Les données transférées incluent entre autres, l'identité du Client et les données nécessaires pour gérer ses comptes de manière journalière et notamment :

  - Authentification (certificat LuxTrust…), sécurité et prévention contre la fraude ;
  - Données liées à ses comptes : consultation de solde et de liste des transactions ;
  - Paiements (paiements SEPA, paiements instantanés, ordres permanents, gestion des bénéficiaires).

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) localisé à Luxembourg, à savoir Worldline Financial Services et ses sociétés affiliées en France, Belgique et Allemagne, sans préjudice de la rubrique « Swift et Plateformes de services de paiement » ci-dessus.

Services centraux liés aux transactions sur instruments financiers conclues de gré-à-gré

- **Description des services :**

  Toutes les transactions conclues de gré-à-gré entre l'entité cliente et la Banque sont centralisées sur les plateformes d'ING Bank NV aux Pays-Bas, afin d'améliorer le service Client et de permettre d'effectuer la surveillance et les contrôles légaux de manière centrale, y compris sans limites pour la réglementation EMIR (European Market Infrastructure Regulation), pour la réglementation MIFID 2 (y inclus MIFIR).

- **Type de données partagées :**

  Les données transférées incluent les données du Client, à savoir notamment la référence Client, le nom de l'entité légale, l'Identifiant d'entité juridique, l'adresse email et les détails de la transaction.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être accessibles de manière confidentielle à ING Bank NV (Pays- Bas) et/ou à ses filiales ou succursales localisée en Belgique, Slovaquie, Royaume-Uni, Singapour, Inde et aux Philippines.

Services centraux liés aux positions acquises en instruments financiers sur les marchés européens

- **Description des services :**

  Afin d'identifier les actionnaires, à la demande de l'émetteur concerné et répondre aux obligations réglementaires de la Banque liées à SRD II (Shareholder Rights Directive UE 2017/828, telle que modifiée).

- **Type de données partagées :**

  Les données transférées incluent notamment : la référence Client, le nom du Client, l'adresse postale, l'adresse email, l'identifiant unique (TIN, LEI) et la position détenue de la valeur concernée.

- **Accès aux données :**

  Outre les informations transmises à l'émetteur concerné conformément à SRDII, certaines informations peuvent être accessibles de manière confidentielle à un fournisseur de service Broadbridge Financial Solutions Ltd localisé au Royaume-Uni ainsi qu'à une solution d'infrastructure cloud (IBM-Managed Private cloud)* dont les serveurs sont situés dans l'Union européenne en France et en Allemagne.

Gestion des cartes de crédit ou de débit, de l'authentification des transactions par internet, et des activités de lutte contre la fraude

- **Description des services :**

  Gestion globale du traitement des cartes de crédit ou de débit (y compris 3D Secure) :
  - à la fois au niveau des transactions opérées au moyen desdites cartes, mais aussi du cycle de vie des cartes (commande, blocage, fonction sans contact, etc.) ;
  - la surveillance des transactions suspectes ou frauduleuses ;
  - la gestion des réclamations au niveau du réseau Visa ;
  - la gestion des transactions de commerce électronique par authentification 3D Secure.

  Gestion complète des activités anti-fraude :
  - la surveillance (et, le cas échéant, blocage) des transactions suspectes ou frauduleuses effectuées via VISA ChannelsCard, les virements de la Banque en ligne (paiements SEPA) et/ou via les applications mobiles My ING de My ING Web Banking;
  - la surveillance de l'accès aux comptes ;
  - le suivi des processus d'authentification (tels que LuxTrust) ;
  - les activités de gestion des dossiers pour suivre, gérer et évaluer les réclamations et les enquêtes liées à la fraude.

- **Type de données partagées :**

  Les données transférées incluent, entre autres, la référence Client, le nom et prénom du Client ou du porteur de la carte, son adresse, son numéro IBAN, la disponibilité de fonds existants sur les comptes liés à ses cartes à un moment donné ainsi que des données démographiques (telles que le lieu, l'adresse, l'âge du Client ou du titulaire de la carte), les informations de connexion et les actions effectuées dans le cadre de l'application mobile My ING ou de la session Web Banking l'emplacement de l'appareil et les données de paiement.

  Les données gérées par les prestataires incluent les informations cartes, les moyens d'authentification associés (dont le certificat LuxTrust) et le détail des opérations.

  En ce qui concerne les activités anti-fraude, en plus de ce qui précède, les données transférées peuvent également inclure le numéro PAN de la carte, les informations de connexion à My ING, y compris le type d'appareil, le système d'exploitation utilisé, la localisation de l'appareil, l'adresse IP, les actions effectuées dans l'application mobile My ING ou la session Web Banking ainsi que les informations sur les transactions, y compris les montants, les détails du bénéficiaire, l'heure et la date, le type d'authentification (LuxTrust). Enfin, les données peuvent inclure des rapports de police et des notes relatives à des plaintes pour fraude ou à des enquêtes sur des fraudes (y compris les résultats).

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays- Bas), à ses sociétés affiliées en Pologne et à des Professionnels du Secteur Financier (PSF) au Luxembourg, à savoir (i) LuxTrust et (ii) Worldline Financial Services et ses sociétés affiliées en France, Belgique et Allemagne.

Production des cartes de crédit ou de débit

- **Description des services :**

  Gestion de la production des cartes de crédit ou de débit et de leur livraison aux Clients/porteurs de cartes.

- **Type de données partagées :**

  Les données transférées comprennent notamment la référence Client, le nom et prénom du Client, ou du porteur de carte, l'IBAN, l'adresse et les informations liées à la carte de crédit ou de débit.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV aux Pays-Bas ou ses sociétés affiliées en Pologne et/ou ou à leur partenaire Thales (ou ses filiales) en France et/ou en Allemagne.

  La plateforme centrale et les données sont hébergées et stockées sur l'infrastructure en nuage (cloud*) IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

Service de signatures électroniques

- **Description des services :**

  Utilisation d'une plateforme afin de collecter des signatures électroniques relatives à la documentation légale entre la Banque et ses Clients.

- **Type de données partagées :**

  Les données transférées sont, entre autres, les documents à signer, le nom et prénom de chaque signataire, sa fonction, son lien avec l'entité juridique pour qui il agit le cas échéant, son numéro de téléphone (afin de permettre l'envoi de sms), sa date de naissance et son adresse email.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas), à sa filiale en Belgique et au fournisseur de services Adobe qui utilise Amazon Web Services (AWS) dont les serveurs sont situés dans l'Union européenne en Irlande et en Allemagne.

Service de gestion d'événements marketing

- **Description des services :**

  Utilisation d'une plateforme externe afin de collecter l'enregistrement électronique des invités, Clients et prospects aux évènements marketing organisés par ING Luxembourg.

- **Type de données partagées :**

  Les données transmises concernent les données d'identification suivantes (encodées directement) par la personne s'enregistrant à un tel événement marketing par internet en réponse à son invitation :

  - Nom ;
  - Prénom ;
  - Nom de la société pour les personnes morales ;
  - Adresse email ;
  - Numéro de téléphone (optionnel).

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays- Bas) ou à sa filiale en Belgique ainsi qu'à son partenaire Via Futura Bvba établi en Belgique.

  Les données sont enregistrées dans une base de données logée sur une plateforme en nuage (cloud)* d'Amazon Web Services (AWS) dont les serveurs sont localisés dans l'Union européenne en Belgique et aux Pays-Bas et aux Etats-Unis concernant l'adresse email.

Gestion de la trésorerie

- **Description des services :**

  Lors de la souscription par le Client à tout produit permettant la gestion de trésorerie par bascule automatique de liquidité entre les comptes principaux, sous comptes et comptes participants.

- **Type de données partagées :**

  Les données transférées concernent les données relatives du Client (nom de l'entreprise, numéro de client, etc.) et les données financières (soldes de comptes, mouvements de comptes, etc.).

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas), ING Belgique ou à d'autres sociétés affiliées dans le monde qui participent au produit de gestion de trésorerie souscrit.

Services de gestion de la relation Client

- **Description des services :**

  Pour enregistrer, voir et partager des informations fournies par le Client ou toute autre information en lien avec le Client sur des plateformes centralisées auprès d'ING Bank NV (Pays-Bas) et de ses filiales, dans le but d'améliorer le service client.

- **Type de données partagées :**

  Les données transférées incluent notamment :

  - Les données du Client, notamment son identité, sa référence client, son adresse, sa structure propriétaire, sa ville et son pays de constitution.
  - Les données des personnes de contact du Client incluant le nom, l'adresse, la fonction, la date de naissance et les données de contact à savoir numéro de téléphone, l'adresse email, le profil LinkedIn.
  - Les données d'échanges avec le Client telles que les procès-verbaux de réunion, les participations à des campagnes ou des évènements.
  - Les caractéristiques produits et données financières telles que les limites de risque crédit ou de marché, les soldes impayés, les numéros de comptes, IBAN, transactions, les fonds entrants et sortants.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses filiales ou succursales dans le monde.

  ING utilise la plateforme SFDC Ireland Ltd (Salesforce) hébergée dans une plateforme nuage (cloud*) d'Amazon Web Services (AWS) dont les données demeurent dans des bases de données situées dans l'Union européenne, et notamment en France, en Irlande et en Allemagne.

Service d'administration des prêts

- **Description des services :**

  Processus opérationnels liés aux activités de crédit du Front Office et du Back Office comme la saisie des données de crédit des clients pour des outils liés à l'analyse financière, le contrôle des pouvoirs des signataires de la documentation crédit et des autres documents contractuels annexes, la création de propositions de notation des risques, le suivi des engagements des crédités et des garants et des revues périodiques des crédits ainsi que la création de contrats de prêt.

- **Type de données partagées :**

  Les données transmises comprennent toutes les informations liées aux demandes de crédit et tous les documents justificatifs à l'appui.

  Cela comprend notamment, l'identité du Client (ou des garants), l'objet financé, la structure de propriété du Client, l'identité des investisseurs, les informations concernant les diligences raisonnables KYC, les données des signataires, les données financières du Client (ou des garants), bilan, chiffre d'affaires, nombre d'employés, performance et toute autre information financière conservée par la Banque en relation avec le Client (ou des garants) (bilan débit-crédit, facilités de crédit existantes ou autres prêts accordés par la Banque ou d'autres entités d'ING et leurs encours).

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas), et/ou à ses filiales à travers le monde et

notamment en Belgique, en Pologne, en Roumanie, en Slovaquie, aux Philippines et en Irlande.

Rapports règlementaires consolidés

- **Description des services :**
  Création, consolidation et autres tâches liées aux rapports règlementaires (comme les reportings statistiques, COREP et AnaCredit, ainsi que les autres reportings requis par la BCE, l'ABE, la BCL et la CSSF).

- **Type de données partagées :**
  Les données transférées sont, en particulier, la référence Client, le nom du Client, ses données financières, ses données de crédits/transactions, le cas échéant son LEI, son pays d'établissement/résidence, et son numéro d'identification national pour les sociétés figurant parmi les expositions de risque de crédit les plus importantes de la Banque.

- **Accès aux données :**
  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle: (i) à ING Bank NV et à ses sous-traitants au Pays-Bas, dont PwC; (ii) au prestataire de services Solvinity BV qui héberge les données aux Pays-Bas; et (iii) au prestataire de services Regnology, basé en Allemagne et qui utilise une infrastructure Google Coud* avec des serveurs situés en Belgique.

Services de traitement et d'enregistrement des transactions liées aux coûts et aux recettes

- **Description des services :**
  Outils informatiques offrant des fonctionnalités de grand livre des comptes et permettant à la Banque de traiter et d'enregistrer des opérations liées aux coûts et aux recettes non couvertes par les systèmes de produits (y compris le traitement des factures émises à l'intention des clients).

- **Type de données partagées :**
  Les données transférées comprennent le nom du Client, son adresse, les données de facturation et les données financières (par exemple, le numéro de compte bancaire).

- **Accès aux données :**
  Dans ce contexte, certaines informations peuvent être mises à disposition de manière confidentielle à ING Bank NV aux Pays-Bas et à ses sous-traitants.

  Dans ce contexte, certaines informations peuvent être stockées sur la plateforme Oracle cloud* dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

Système de traduction automatisé

- **Description des services :**
  Outil d'aide à la traduction via de l'intelligence artificielle.

- **Type de données partagées :**
  Tous types de textes et de documents, en ce compris ceux collectés par la Banque ou communiqués par le Client au cours de la relation d'affaires, tels que les manuels, les contrats, les procédures, les rapports, les informations sur les produits et le support, les sites Web, etc.

- **Accès aux données :**
  Dans ce contexte, certaines informations peuvent être stockées sur l'infrastructure en nuage (cloud*) IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

Outils de communication et de productivité pour les employés d'ING Luxembourg

- **Description des services :**
  Utilisation d'outils de communication et de productivité, principalement une messagerie (courriels et messages instantanés), y compris l'archivage de cette messagerie. Ces outils permettent la collaboration, la communication et l'assistance intelligente (y compris des outils d'intelligence artificielle générative) dans les tâches quotidiennes des employés.

- **Type de données partagées :**
  Toutes les données relatives au Client pouvant se trouver dans les messages envoyés et reçus, les enregistrements effectués, le calendrier et le répertoire des employés et dans les autres outils et fonctionnalités.

- **Accès aux données :**
  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV aux Pays-Bas sur une plateforme en nuage (cloud*) Microsoft Azure dont les serveurs sont situés dans l'Union européenne aux Pays-Bas, en Pologne et en Irlande. Certaines informations peuvent aussi être stockées sur une l'infrastructure en nuage (cloud*) IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

  L'archivage de cette messagerie sera aussi accessible de manière confidentielle à ING Bank NV (Pays-Bas) et au prestataire de services Arctera Enterprise Vault, basé en Irlande et qui traitera les données aux Pays-Bas.

Infrastructure de stockage et gestion de données et documents

- **Description des services :**
  Mise à disposition d'une infrastructure de stockage et gestion de données et documents utilisée par les employés de la Banque.

- **Type de données partagées :**
  Les données transférées peuvent contenir potentiellement tous types de données et informations, documents et contrats collectés et/ou traitées par la Banque avec ses Clients dans le cadre de ses activités.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV aux Pays-Bas ou à ses sociétés affiliées à travers le monde et sont stockées sur une plateforme nuage (cloud*) Microsoft Azure dont les serveurs sont logés dans l'Union européenne aux Pays-Bas, en Pologne et en Irlande.

Contact Center (Centre d'appels)

- **Description des services :**

  Transfert d'appels vers le Contact Center d'ING Belgique ou ses sous-traitants (y compris B-Connected, N-Allo et CXL) via l'utilisation de la plateforme de téléphonie appelée.

  Mise à disposition à travers une infrastructure en nuage (cloud)* gérée par ING Bank NV d'éléments d'infrastructures technologiques et applicatifs permettant de gérer un entrepôt de données.

- **Type de données partagées :**

  Les données transférées sont celles qui sont contenues dans l'appel transféré vers ING Belgique, le numéro de téléphone, le nom et le prénom du Client.

  Les communications transférées vers ING Belgique sont enregistrées et conservées par ING Belgique et peuvent servir en tant que moyen de preuve conformément aux Conditions Générales applicables.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Belgique et à ses sous-traitants (y compris B-Connected, N-Allo et CXL) situés dans l'Union européenne en Belgique.

  Dans ce contexte, certaines informations peuvent être stockées sur l'infrastructure en nuage (cloud*) IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

Service de création de rapports conformément à la réglementation relative au système électronique central concernant les informations sur les paiements (CESOP)

- **Description des services :**

  Outil informatique permettant de générer les rapports relatifs aux informations sur les paiements transfrontaliers provenant des Etats Membres et sur les bénéficiaires de ces paiements transfrontaliers, afin de répondre aux exigences de la réglementation CESOP, à savoir la Directive (UE) 2020/284 modifiant la directive 2006/112/CE, telle que transposée en droit luxembourgeois, et le Règlement (UE) 2020/283 modifiant le règlement (UE) no 904/2010, tels que le cas échéant modifié. Les rapports générés sont communiqués à l'Administration des Contributions Directes, aux fins de leur centralisation et agrégation dans une banque de données européenne, le système électronique central concernant les informations sur les paiements (CESOP).

- **Type de données partagées :**

  Les données transférées concernent de manière non limitative :

  - le code BIC ou tout autre code d'identification d'entreprise qui identifie le prestataire de service de paiement en charge du reporting ;
  - le nom ou la raison sociale du bénéficiaire ;
  - le numéro d'identification TVA ou tout autre numéro fiscal national du bénéficiaire ;
  - le numéro IBAN ou tout autre identifiant qui identifie le bénéficiaire et le lieu où il se trouve ;
  - l'adresse du bénéficiaire ;
  - s'il agit d'un paiement ou d'un remboursement ;
  - la date et heure du paiement ou remboursement de paiement ;
  - le montant et monnaie du paiement ou du remboursement de paiement ;
  - le code pays de l'Etat Membre d'origine du paiement ;
  - le code pays de l'Etat Membre de destination du remboursement ;
  - les informations utilisées pour déterminer l'origine ou la destination du paiement ou du remboursement de paiement ;
  - toute référence qui identifie le paiement ;
  - le cas échéant, toutes les informations indiquant que le paiement est initié dans les locaux du commerçant.

  Les informations transmises varient en fonction de la méthode de paiement utilisée.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank N.V. (Pays-Bas) et à ses sous-traitants.

  Les informations sont logées sur l'infrastructure en nuage (cloud*), IPC, gérée par ING Bank NV aux Pays-Bas et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

Service de création de rapports conformément à la réglementation FATCA et CRS

- **Description des services :**

  Outil mis en place aux fins de générer les rapports relatifs aux obligations FATCA/CRS et lettres d'information pour se conformer aux réglementations afférentes.

- **Type de données partagées :**

  Les données transférées concernent :

  - Nom et prénom des personnes ;
  - Le nom de l'entreprise ;
  - L'adresse postale ;
  - Adresse légale ;
  - Numéro de client ;
  - Date de naissance ;
  - Numéro d'entreprise ;
  - Compte bancaire ;
  - Solde du compte ;
  - Données financières ;
  - Produits et services utilisés ;
  - Numéro(s) d'identification fiscale ;
  - Résidence(s) fiscale(s) ;
  - Rôle des personnes physiques et morales (Bénéficiaire effectif final) ;
  - Statuts FATCA, Intermédiaire Qualifié et CRS.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank N.V. (Pays-Bas)

  Les informations sont logées sur l'infrastructure en nuage (cloud*), IPC, gérée par ING Bank NV aux Pays-Bas et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas.

Services de négociation et de gestion des contrats Internationaux Swaps and Dérivatives Association « ISDA » et du collatéral y liés

- **Description des services :**

  Assistance à la négociation des contrats ISDA et des conventions réglant la gestion du collatéral y liés, et gestion du cycle de vie du contrat jusqu'à son échéance (incluant les modifications et résiliations).

- **Type de données partagées :**

  Les données transférées concernent toutes les données du Client et des garants dans le contexte de la négociation et de la gestion du contrat. Les données concernent également les transactions effectuées sous couvert du contrat ISDA et du collatéral fourni au cours du temps.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et à sa succursale en Belgique.

Processus de contrôle interne

- **Description des services :**

  Identifier, suivre et évaluer les contrôles afin de s'assurer qu'ING Luxembourg agit en conformité avec les politiques, procédures, contrôles et normes minimales internes d'ING, et aux lois applicables.

- **Type de données partagées :**

  Les données transférées concernent toutes les données identifiant le Client et, le cas échéant, ses mandataires, représentants (légaux) et bénéficiaires effectifs, ainsi que les données requises ou utilisées pour gérer les services et produits et, plus généralement, toutes les données du Client qui sont traitées en lien avec le processus testé (par exemple KYC, Paiement, Fraude, Abus de marché).

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank N.V. (Pays-Bas) et/ou à ses filiales en Slovaquie, aux Philippines et en Roumanie.

Services de recherche complémentaire en cas de compte dormant ou inactif et de coffre-fort inactif

- **Description des services :**

  Utilisation d'un prestataire tiers pour effectuer des recherches complémentaires afin d'obtenir et d'utiliser des informations sur les Clients dormants/inactifs, d'initier des opérations de recherche dans le but de rétablir le contact et d'obtenir des instructions sur la volonté du Client (poursuivre ou mettre fin à la relation avec la Banque).

  Ceci est conforme aux obligations légales de la Banque et à la réglementation applicable en matière de comptes inactifs ou dormants et de coffres de dépôt inactifs.

- **Type de données partagées :**

  Les données transférées concernent toutes les données d'identification du Client, la référence du Client et, le cas échéant, ses mandataires, représentants (légaux) et bénéficiaires effectifs, y compris, entre autres, leurs données d'identification, profession, date et lieu de naissance, numéro de passeport, numéro d'identification national et/ou fiscal, adresse, lieu de résidence, numéro de téléphone, toute donnée publique concernant ces personnes et, de manière générale, toutes les données communiquées lors de l'ouverture du compte ou par la suite en ce qui concerne le processus « Know Your Customer » et la provenance des fonds, ainsi que toutes les informations communiquées à la Banque lors de chaque transaction effectuée sur les comptes ouverts auprès de la Banque à tout moment.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à Dynaslux, un prestataire de services tiers agréé en tant que PSA (Professionnel du Secteur des Assurances), situé au Luxembourg et à ses sous-traitants (y compris Finaca, Arca Conseil, Detectnet, Argene) situés dans l'Union européenne en France.

Procédure de dénonciation

- **Description des services :**

  Afin de se conformer aux exigences réglementaires relatives à la protection des personnes qui signalent des violations du droit européen, la Banque encourage les employés ou d'autres personnes (par exemple les consultants) à signaler de bonne foi un comportement criminel, un comportement contraire à l'éthique ou d'autres fautes commises par la Banque ou en son sein, qu'ils soient soupçonnés ou avérés, en ayant recours à la procédure interne de dénonciation.

  Une plateforme externe sert de canal de signalement, ainsi que de système de gestion des dossiers et de base de données de stockage de tous les signalements reçus par d'autres canaux (par exemple, par email).

- **Type de données partagées :**

  Toute donnée concernant le Client peut être incluse dans les rapports de dénonciation.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Belgium SA (Belgique), ING Bank NV (Pays-Bas) et au prestataire de services Vault Platform Ltd (basé au Royaume-Uni) et ses sous-traitants, y compris Amazon Web Services (AWS), qui sont situés au Royaume-Uni, en Irlande, en Allemagne, en Suède et aux États-Unis.

  Certaines informations peuvent être stockées sur l'infrastructure en nuage (cloud*) AWS*, dont les serveurs sont situés au Royaume-Uni.

Service d'accès aux distributeurs automatiques de billets

- **Description des services :**

  Utilisation d'un prestataire de réseau de distributeur automatique de billets pour que nos clients puissent effectuer des retraits, dépôts et d'autres opérations.

- **Type de données partagées :**

  Les données transférées incluent notamment le numéro de carte, nom, PIN, numéros de comptes, solde de ces comptes ainsi que les détails des opérations effectuées sur les distributeurs automatiques de billets.

- **Accès aux données :**

  Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle au prestataire de services LuxConstellation basé à Luxembourg. Ce dernier stockera les données au Luxembourg chez un Professionnel du Secteur Financier et utilisera le support de sous-traitants établis dans l'Union européenne.