**ANNEXE 2 – OUTSOURCING**

**« TABLEAU RÉCAPITULATIF - Infrastructures de tiers et communes au Groupe ING[1] »**

(cf. **article A.9 bis** des « Conditions Générales de la Banque (Retail & Private Banking) »)

**Le présent tableau est applicable à compter du 1 novembre 2024 aux clients du segment Retail & Private Banking. Néanmoins pour les Clients Retail & Private Banking ayant noué et maintenu une relation bancaire avec ING Luxembourg préalablement à cette date, le présent tableau n'entrera en vigueur qu'au 1er janvier 2025.**

| | Description du service | Type de données partagées | Accès aux données |
|---|---|---|---|
| **Services d'accès aux Prestataires de Services de Paiement Tiers dans le cadre de la Directive révisée sur les Services de Paiement (PSD2)** | 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. | 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. | 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. |
| **Services *Know Your Customer* (KYC)** | **PERFORMANCE ET EXAMEN DU DEVOIR DE VIGILANCE À L'ÉGARD DE LA CLIENTÈLE**<br><br>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 bénéficiaires effectifs, 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 | 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. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV et/ou à ses filiales, succursales et/ou sous-traitants aux Pays-Bas, en Pologne et en Slovaquie.<br><br>Ces informations peuvent être stockées sur l'infrastructure informatique en nuage privé IPC (*ING Private Cloud*), gérée par ING Bank NV, dont les serveurs sont situés dans l'Union européenne aux Pays-Bas. |

[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.

| | | | |
|---|---|---|---|
| | leur situation propre au regard des diverses lois et réglementations applicables comme les 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. | | |
| | **VERIFICATION PAR NOM (SCREENING)**<br><br>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.<br><br>Par ailleurs, un screening des mêmes personnes dans les médias est également centralisé au sein du Groupe ING. | 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.<br><br>Pour réaliser le screening dans les médias par « Regulatory Data Corp Ltd » (ou toute autre entité du même groupe) les données transférées sont le prénom, le nom, la date de naissance et le pays de résidence. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV et/ou à ses filiales, succursales, et/ou sous-traitants aux Pays-Bas, en Roumanie, 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.<br><br>Certaines données relatives aux personnes soumises au screening dans les médias peuvent être rendues accessibles au fournisseur basé au Royaume-Uni. Dans ce contexte, le screening par nom et ses résultats sont enregistrés dans une base de données logée sur une plateforme en nuage (*cloud*) d'Amazon Web Services (AWS)* située dans l'Union européenne, dont les serveurs se trouvent en Allemagne et en Irlande. |
| | **VERIFICATION PRÉALABLE DES TRANSACTIONS (PRE-TRANSACTION SCREENING)**<br><br>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. | Cf. « Performance et examen du devoir de vigilance à l'égard de la Clientèle » ci- avant. | 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 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)**<br><br>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. | Cf. « Performance et examen du devoir de vigilance à l'égard de la Clientèle » ci- avant. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV, et/ou à ses filiales, succursales et/ou ses sous-traitants aux Pays-Bas, en Pologne 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. |
| **Services d'exploitation des données** | L'objectif de ce service est de vérifier les rapports obligatoires transmis à la CSSF en vertu des règles relatives au système central de récupération des données électroniques afin d'identifier les erreurs potentielles et d'y remédier. | Cf. « Performance et examen du devoir de vigilance à l'égard de la Clientèle » ci-avant. 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. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle àING Bank NV et à ses sociétés affiliées. |
| **Services de conformité relative aux abus de marché et aux conflits d'intérêts** | L'objectif de ce service est 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. | Le nom et les coordonnées du Client et tout type d'informations fournies dans les conversations enregistrées et les e-mails. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et ses filiales, y compris en Roumanie et aux Philippines.<br><br>Certaines informations peuvent également 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. |

| | | | |
|---|---|---|---|
| **Swift et Plateformes de Services de Paiement** | **EN GÉNÉRAL**<br><br>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.<br><br>Traiter et exécuter l'ensemble des processus liés aux opérations de paiement entrantes ou sortantes des Clients ainsi que leur stockage et leur archivage. | Les données transférées concernent toutes les données reprises dans les différents champs figurant dans les messages ou systèmes de paiement (Swift ou non), en ce compris, de manière non limitative : la référence Client, l'identité du Client, 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. | 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 Pologne ou en Slovaquie. |
| | **PAIEMENT INSTANTANÉ**<br><br>Outre ce qui précède, traiter et exécuter l'ensemble des processus liés aux opérations de paiement entrantes ou sortantes des Clients ainsi que leur stockage et leur archivage centralisés.<br><br>Tracer et surveiller les opérations de paiements initiées ou reçues au niveau centralisé du Groupe ING pour toutes les entités ING, dont ING Luxembourg.<br><br>Effectuer des tâches dans le cadre de la Vérification du Bénéficiaire (*Verification of Payee - VoP).* | | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses sous-traitants, y compris en Roumanie et aux Philippines, et à ses sous-traitants en Inde et au Royaume-Uni.<br><br>Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et ING Belgique et/ou à leurs sous-traitants en Belgique et aux Pays-Bas, ainsi qu'au prestataire de services Fidelity National Information Services, qui stocke ces informations sur une plateforme en nuage (*cloud)* Microsoft Azure*, avec des serveurs situés en Allemagne et en Irlande et avec un accès à distance potentiel à ces serveurs depuis l'Inde de manière occasionnelle.<br><br>Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et aux prestataires de services EBA Clearing (basé en France) et SurePay (basé aux Pays-Bas), ainsi qu'à l'un quelconque de leurs sous-traitants. |

| | | | |
|---|---|---|---|
| **Portail utilisé pour faciliter la gestion des produits et services offerts aux Clients par la Banque** | 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 employés de vente ING de la Banque d'accéder centralement via ce portail aux différents 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. | 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 :<br>• 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 ;<br>• Services et produits souscrits (comptes courants, comptes épargne, comptes Visa, comptes de crédit…) ;<br>• Paiements (SEPA, ordres permanents, gestion des bénéficiaires, opérations sur comptes…) ;<br>• Documents électroniques signés ou non ;<br>• Documents signés par le Client ;<br>• Proposition et souscription aux produits et/ou services. | 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. |
| **Service Technique** | Assistance informatique de premier niveau aux utilisateurs de la Banque à Luxembourg. | Dans le cadre de ce contrat 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. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) basé à Luxembourg. |
| **Services d'infrastructure technique** | 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.<br><br>Mise à disposition à travers une infrastructure en nuage (cloud computing) gérée par ING Bank NV d'éléments d'infrastructures technologiques et applicatifs permettant de gérer un entrepôt de données.<br><br>Exécution de tâches informatiques opérationnelles ou de maintenance, y compris sur des systèmes informatiques | Les données transférées concernent les mails, l'annuaire de service d'exploitation et la gestion des téléphones portables.<br><br>Les données personnelles de Clients pouvant être transférées comprennent (sans limitation) : référence Client, nom, adresse mail, contenu de l'email, numéro de téléphone, nom de sociétés et pièces jointes.<br><br>Les données transférées dans l'infrastructure privée de *cloud computing* sont les mêmes que celles mentionnées dans les services KYC (*Know Your Customer)* et de gestion des risques de crédit et de marché.<br><br>Les données accessibles 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. | 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.<br><br>La plateforme d'infrastructure et les données sont logées sur une plateforme en nuage (cloud)* de Microsoft Azure dont les serveurs sont localisés dans l'Union européenne, en Autriche, Finlande, Irlande et Pays-Bas.<br><br>Dans ce contexte, certaines 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.<br><br>Le support sur les services d'infrastructure technique et sur la gestion des incidents est également fourni par la filiale d'ING Bank NV en Pologne, les prestataires de services TATA Consultancy Services Netherlands B.V., HCL Technologies B.V. (basé aux |

| | | | |
|---|---|---|---|
| | reposant sur l'informatique en nuage (cloud computing).<br><br>Utilisation de prestataires de service tiers pour soutenir les services d'infrastructure technique, le suivi des travaux de production et la gestion des incidents. | | Pays-Bas) et Cognizant Worldwide Limited (basé au Royaume-Uni) ainsi que leurs sociétés affiliées en Inde, qui peuvent occasionnellement avoir accès aux données du client. |
| **Sécurité informatique (IT)** | Mise à disposition de service de maintenance et de support des applications de la Banque hébergés dans les infrastructures.<br><br>Gestion du système de sécurité informatique, en particulier la détection et la gestion des incidents de sécurité. | Les données transférées concernent les mails, l'annuaire de service d'exploitation et la gestion des téléphones portables du personnel ING. Les données transférées peuvent ainsi 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).<br><br>Pour la gestion du système de sécurité informatique, les données concernées 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. | 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), dont le centres de données sont localisés dans l'Union Européenne au Luxembourg, et à ING Bank NV (Pays-Bas) et/ou ses sous-traitants en Pologne. |
| **Services relatifs à l'impression et à la gestion documents Clients** | Service de mise en page et d'impression et de numérisation des documents Clients. | 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 services souscrits. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) localisé à Luxembourg dans le cas de la dématérialisation des documents et de leur impression, ainsi qu'à ING Belgique pour la mise en page de différents types de documents Clients. |
| **Gestion des archives physiques** | 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. | 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.<br>Les données utilisées pour le suivi des archives (à des fins de consultation) et pour leur destruction. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un Professionnel du Secteur Financier (PSF) localisé à Luxembourg et avec un entrepôt localisé au Luxembourg.<br>Le PSF ne gère que le contenant et non le contenu. |

| | | | |
|---|---|---|---|
| **Service de gestion du risque crédit** | Orchestration et stockage de manière centrale des demandes et 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.<br><br>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). | Les données transférées concernent toutes les données du Client relatives à la demande de crédit initiale, une modification ou toute autre évènement 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, le cas échéant les informations détaillées sur le bien immobilier utilisé pour garantir la demande de crédit (y compris son adresse) et toutes autres informations financières détenues par la Banque relatives 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).<br><br>Pour les entités juridiques uniquement, les données transférées incluent les données financières du Client, notamment le bilan, chiffre d'affaires et nombre d'employés.<br><br>De plus et pour les entités juridiques uniquement, les données transférées incluent les données personnelles Client 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.<br><br>Pour les particuliers, 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. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à Nexvia (un prestataire de services basé au Luxembourg), à ING Bank NV (Pays-Bas) et à ses sous-traitants aux Pays-Bas, en Belgique, en Pologne et/ou en Slovaquie.<br><br>La plateforme centrale et les données sont hébergées et 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.<br><br>La plateforme d'infrastructure et les données transmises à Nexvia au Luxembourg sont hébergées et stockées sur une plateforme de nuage (*cloud*)* Amazon Web Services, dont les serveurs sont situés dans l'Union européenne en Irlande. |
| **Services de gestion des risques de marché** | Suivi et modélisation des risques de marché en général, reporting internes et exportation des risques de taux et de liquidité de la Banque. | 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. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) ou auprès de ses filiales en Belgique, en Pologne et aux Philippines. |

| | | | |
|---|---|---|---|
| **My ING – Web Banking** | My ING, afin d'offrir une plateforme de Web-Banking sur les applications internet et mobiles iOS/Android. | Les données transférées incluent entre autres, l'identité du Client et les données nécessaires pour gérer son activité journalière notamment :<br>• Authentification (certificat LuxTrust), sécurité et prévention contre la fraude ;<br>• Données personnelles et consentements ;<br>• Présentation des produits (comptes courant, comptes épargne, comptes visa, comptes crédit…) ;<br>• Paiements (SEPA, ordre permanent, gestion des bénéficiaires) ;<br>• Système d'alertes (email et notifications) ;<br>• Agrégation des comptes ;<br>• Messagerie sécurisée ;<br>• Documents électroniques ;<br>• Proposition et souscription à des produits et/ou services. | 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) et à ING Bank NV et/ou à ses sous-traitants aux Pays-Bas, en Belgique, ou en Pologne. |
| **Services liés aux lettres d'audit (pour les entreprises uniquement)** | Harmoniser et automatiser la demande, la création et l'envoi des lettres d'audit.<br>Plateforme basée sur le Web permettant aux auditeurs de demander des lettres d'audit directement à ING. | Les données transférées comprennent entre autres :<br>• 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 e-mail<br>• Les données relatives aux employés du Client, telles que le prénom et le nom de famille, l'adresse e-mail, le numéro de téléphone et l'adresse IP (données de signature électronique)<br>• Les données relatives à l'auditeur du Client, telles que l'adresse e-mail, le numéro de téléphone et l'adresse IP (données de signature électronique). | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses filiales 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.<br>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** | Mise à disposition de canaux de communication digitaux sécurisés tels que (appel audio, chat, et messaging).<br><br>Ces canaux utilisent des services dans le *cloud* Internet *. | Les données transférées concernent les informations nécessaires à l'établissement de la communication et à la reconnaissance vocale :<br>• Adresse IP<br>• N° de téléphone<br>• Adresse email<br>• Photo ou vidéo<br>• Traitement automatique du langage naturel (NLP, reconnaissance vocale)<br><br>Les communications sont enregistrées et conservées par ING et peuvent servir en tant que moyen de preuve conformément aux Conditions Générales applicables.<br><br>L'exploitant des services *cloud** n'a accès qu'aux données techniques selon le canal (et non au contenu décrypté des communications) :<br>• Adresse IP<br>• 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. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV et/ou à ses sous-traitants aux Pays-Bas, en Belgique ou en Pologne.<br><br>La plateforme d'infrastructure et les données sont hébergées dans une plateforme de nuage (*cloud*)* d'Amazon Web Services (AWS) et Google toutes deux situées dans l'Union européenne en Irlande et en Allemagne. |
| **Multiline (pour les entreprises uniquement)** | 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. | Les données transférées incluent entre autres, l'identité du Client et les données nécessaires pour gérer ses comptes de manière journalière et notamment :<br>• Authentification (certificat LuxTrust…), sécurité et prévention contre la fraude ;<br>• Données liées à ses comptes : consultation de solde et de liste de transactions ;<br>• Paiements (SEPA, ordre permanent, gestion des bénéficiaires). | 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 « Paiement instantané ». |
| **Services centraux liés aux transactions sur instruments financiers conclues de gré-à-gré** | Toutes les transactions sur instruments financiers conclues de gré-à-gré entre le Client et la Banque sont centralisées sur les plateformes d'ING Bank NV (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 | 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 (le cas échéant), l'adresse email et les détails de la transaction. | Dans ce contexte certaines informations peuvent être accessibles de manière confidentielle à ING Bank NV (Pays-Bas) et/ou à ses filiales ou ses succursales localisée en Belgique, en Slovaquie, au Royaume-Uni, à Singapour, en Inde et aux Philippines. |

| | | | |
|---|---|---|---|
| | réglementation MIFID 2 (y inclus MIFIR). | | |
| **Services centraux liés aux positions acquises en instruments financiers sur les marchés européens** | Afin d'identifier les actionnaires, à la demande de l'émetteur concerné, transmettre les informations relatives aux assemblées générales, faciliter l'exercice des droits des actionnaires et répondre aux obligations réglementaires de la Banque liées à SRD II (Shareholder Rights Directive UE 2017/828, telle que modifiée). | Les données transférées incluent notamment : la référence Client, le nom du Client, l'adresse postale, l'adresse e-mail, l'identifiant unique (TIN, LEI), la position détenue de la valeur concernée ainsi que le choix du Client en cas de vote à l'assemblée générale. | Outre les informations transmises à l'émetteur concerné conformément à SRDII (y compris pour les services de vote par procuration) 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 et authentification des transactions par internet** | Gestion complète du traitement des cartes de crédit ou de débit (y compris 3D Secure) :<br>• 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.)<br>• la surveillance des transactions suspectes ou frauduleuses<br>• la gestion des réclamations au niveau du réseau Visa<br>• la gestion des transactions de commerce électronique par authentification 3D Secure. | Les données transférées incluent notamment 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.<br><br>Les données gérées par les prestataires incluent les informations cartes, les moyens d'authentification associés (dont le certificat LuxTrust) et le détail des opérations effectuées avec ces dernières. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas), à ses sociétés affiliées en Pologne y inclus leur sous-contractant IT Card S.A. 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. |
| **Service de gestion des évènements marketing** | Utilisation d'une plateforme externe afin de collecter l'enregistrement électronique des invités, Clients et prospects aux évènements marketings organisés par ING Luxembourg. | 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 :<br>• Nom<br>• Prénom<br>• Nom de la société pour les personnes morales<br>• Adresse E-mail<br>• Numéro de téléphone (optionnel) | 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** | 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. | 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. ) au sein du groupe. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas), ING Belgique ou d'autres filiales dans le monde qui participent au produit de gestion de trésorerie souscrit. |
| **Production des cartes de crédit ou de débit** | Gestion de la production des cartes de crédit ou de débit et de leur livraison aux Clients/porteurs de cartes. | Les données transférées comprennent notamment la référence Client, le nom et prénom du client ou du porteur de la carte, son IBAN, l'adresse et les informations liées à la carte de débit ou de crédit. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV (Pays-Bas) ou ses sociétés affiliées en Pologne et/ou ou à leur partenaire Thales (ou ses filiales) en France et/ou en Allemagne.<br><br>La plateforme centrale et les données sont hébergées et 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. |
| **Service de Plateforme de partage de signature** | Utilisation d'une plateforme afin de collecter des signatures électroniques relatives à la documentation légale entre la Banque et ses Clients. | 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, son numéro de téléphone (afin de permettre l'envoi de sms) et de son adresse email. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un fournisseur d'infrastructure en nuage (*cloud*)* fourni par Adobe et hébergé par Amazon Web Services (AWS)* dont les serveurs sont situés dans l'Union européenne, en Irlande et en Allemagne. |
| **Rapports réglementaires consolidés de la Banque** | Consolidation des rapports réglementaires COREP (*Common Reporting Framework)* et EBA (*European Banking Authority*). | Les données transférées sont, en particulier, la référence Client, le nom du Client, son LEI, son numéro d'identification national pour les 20 expositions de risque de crédit les plus importantes. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV et à ses sous-traitants au Pays-Bas, dont PwC.<br><br>Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à un fournisseur d'une infrastructure en nuage (*cloud*)* fournie par Solvinity et hébergée par Solvinity. Les données demeureront en Union européenne, dans les bases de données de Solvinity aux Pays-Bas. |
| **Système de traduction automatisé** | Outil d'aide à la traduction via de l'intelligence artificielle. | 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. | Dans ce contexte, certaines 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. |

| | | | |
|---|---|---|---|
| **Infrastructure des mails des employés ING Luxembourg et archivage** | Mise à disposition de l'infrastructure de messagerie exchange Online O365 pour l'entité Luxembourgeoise gérée par ING Bank NV (Pays-Bas).<br><br>Cette infrastructure dispose d'un archivage géré par ING Bank NV (Pays-Bas) de tous les emails envoyés vers et depuis les boîtes aux lettres (mailbox) ING. Exchange O365 est une infrastructure de type *cloud computing* gérée par ING Bank NV (Pays-Bas). | Les données transférées concernent toutes les données qui sont liées aux traitements de tous les mails tous les emails envoyés vers et depuis les boîtes aux lettres (mailbox) ING (des employés ou non ) (internes et externes) ainsi que leurs pièces jointes. Cela concerne aussi le calendrier des employés, les contacts et toutes les fonctionnalités liées à la messagerie. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV aux Pays-Bas sur une plateforme 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) privé IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union Européenne aux Pays-Bas.<br><br>L'archivage de cette messagerie sera aussi accessible de manière confidentielle par ING Bank NV (Pays-Bas). |
| **Infrastructure de stockage de données SharePoint** | Mise à disposition d'une infrastructure de partage de données type Microsoft SharePoint pour ING Luxembourg gérée par ING Bank NV. SharePoint est une infrastructure de type *cloud computing* gérée par ING Bank NV (Pays-Bas). | Les données transférées peuvent contenir potentiellement tous types de données et informations (personnelles), documents et contrats collectés et/ou traités par la Banque avec ses Clients dans le cadre de ses activités. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV aux Pays-Bas 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)** | 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.<br><br>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. | 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.<br><br>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. | 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.<br><br>Dans ce contexte, certaines informations peuvent être stockées l'infrastructure en nuage (*cloud*) IPC, gérée par ING Bank NV et dont les serveurs sont situés dans l'Union européenne aux Pays-Bas. |
| ***Services d'offboarding*** | Les outils et les technologies facilitant le processus par lequel la relation des clients avec la Banque prend fin (aussi appelé le "offboarding"). | Les données transférées comprennent la référence du Client, son nom, ses adresses postale et électronique, ses numéros de téléphone, son identifiant unique (TIN, LEI), sa date et son lieu de naissance, le solde de son compte, son numéro de compte, et en général toutes les données communiquées à la Banque lors de l'ouverture d'un compte et pendant toute la durée de la gestion de la relation avec le Client. | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank NV aux Pays-Bas, au prestataire de services Xlinq BV basé aux Pays-Bas, et au prestataire de services ABBYY Europe GmbH basé en Allemagne.<br><br>Les informations sont aussi stockées sur une plateforme en nuage (cloud)* Microsoft Azure dont les serveurs sont situés dans l'Union européenne aux Pays-Bas et en Irlande. |

| | | | |
|---|---|---|---|
| **Service de création de rapports conformément à la réglementation relative au système électronique central concernant les informations sur les paiements (CESOP)** | Outil mis en place par ING Bank N.V. pour ses filiales, dont ING Luxembourg, aux fins 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 (EU) 2020/284 modifiant la directive 2006/112/CE, telle que transposée en droit luxembourgeois, et le Règlement (EU) 2020/283 modifiant le règlement (UE) no 904/2010, tels que le cas échéant amendés. | Les données transférées concernent de manière non limitative :<br>• Le code BIC ou tout autre code d'identification d'entreprise qui identifie le prestataire de service de paiement en charge du reporting,<br>• le nom ou la raison sociale du bénéficiaire,<br>• le numéro d'identification TVA ou tout autre numéro fiscal national du bénéficiaire,<br>• le numéro IBAN ou tout autre identifiant qui identifie le bénéficiaire et le lieu où il se trouve,<br>• l'adresse du bénéficiaire,<br>• s'il agit d'un paiement ou d'un remboursement,<br>• la date et heure du paiement ou remboursement de paiement,<br>• le montant et monnaie du paiement ou du remboursement de paiement,<br>• le code pays de l'Etat Membre d'origine du paiement,<br>• le code pays de l'Etat Membre de destination du remboursement,<br>• les informations utilisées pour déterminer l'origine ou la destination du paiement ou du remboursement de paiement,<br>• toute référence qui identifie le paiement, et<br>• le cas échéant, toutes les informations indiquant que le paiement est initié dans les locaux du commerçant.<br>Les informations transmises varient en fonction de la méthode de paiement utilisée. 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). | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank N.V. (Pays-Bas). .<br><br>Les informations sont logées sur une infrastructure en nuage (*cloud*) IPC, gérée par ING Bank NV, dont les serveurs sont situés dans l'Union européenne aux Pays-Bas. |
| **Service de création de rapports conformément à la réglementation FATCA et CRS** | Outil mis en place aux fins de générer les rapports relatifs aux obligations FATCA/CRS et lettres d'information afin de se conformer à la réglementation afférente. | Les données transférées concernent :<br>▪ Nom et prénom des personnes physiques<br>• Adresse postale<br>• Numéro Client<br>• Date de naissance<br>• Compte bancaire<br>• Solde du compte<br>• Données financières<br>• Produits et services utilisés<br>• Numéro(s) d'identification fiscale<br>• Résidence(s) fiscale(s)<br>• Statuts FATCA et CRS | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank N.V. (Pays-Bas).<br><br>Les informations sont logées 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. |

| | | | |
|---|---|---|---|
| **Processus de contrôle interne** | Identifier, suivre et évaluer les contrôles afin de s'assurer qu'ING Luxembourg agit en conformité avec les politiques, procédures, contrôles et normales minimales internes d'ING, et aux lois applicables. | 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). | Dans ce contexte, certaines informations peuvent être rendues accessibles de manière confidentielle à ING Bank N.V. (Pays-Bas) et/ou à ses sociétés affiliées en Slovaquie, aux Philippines et en Roumanie. |
| **Services de recherche complémentaire en cas de compte dormant ou inactif et de coffre-fort inactif** | 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. | 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. | 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** | 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.<br><br>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 e-mail). | Toute donnée (à caractère personnel) concernant le Client peut être incluse dans les rapports de dénonciation. | 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.<br><br>Certaines informations peuvent être stockées sur l'infrastructure en nuage (*cloud*) AWS*, dont les serveurs sont situés au Royaume-Uni. |