

L'outsourcing vu sous l'angle du secret bancaire et du RGPD

André Hoffmann

Philippe Dupont

ALJB

3 juillet 2018

Délimitation du sujet

- externalisation vue sous deux angles
 1. secret bancaire nouveau cru (personnes physiques et morales)
 2. protection des données (personnes physiques)
- aspects réglementaires ne seront pas couverts

I.1. Secret bancaire

Définition de l'outsourcing – point de vue réglementaire

- Circulaire 12/552 (181): « La sous-traitance désigne le transfert complet ou partiel de tâches opérationnelles, d'activités ou de prestations de services de l'établissement vers un prestataire externe, qui fait partie ou non du groupe auquel l'établissement appartient. »
 - la protection des données doit être garantie en permanence
 - pas de délégation de responsabilité vers le sous-traitant « sauf concernant la responsabilité du secret professionnel lorsque le sous-traitant agit dans le cadre de l'article 41(5) de la LSF »
 - en fonction des circonstances, il faut voir si le consentement des clients est requis

Un peu d'histoire législative

- Article 458 Code pénal
- 1981: introduction par l'arrière –porte
 - « Par dérogation à l'article 458 du Code pénal... »
- 1993: Article 41 – un secret bancaire autonome
 - projet de loi n° 3600: « En donnant à cette obligation [au secret] une base légale et non conventionnelle, et en assurant son respect par les sanctions pénales de l'article 458 du Code pénal, le législateur lui confère le caractère d'une règle d'ordre public, à laquelle seule la loi peut faire des exceptions. »

Jurisprudence

- pénal:
 - « Le secret bancaire, protégé par les sanctions de l'article 458 du Code pénal et ne pouvant être levé d'après l'article 41, paragraphe 2 de la loi du 5 avril 1993 que par la loi, est d'ordre public. (...) Aucun élément de texte ne permet d'admettre que l'approche retenue dans l'article 458 du Code pénal ne reste entièrement applicable, avec l'interprétation qui a fini par s'en dégager. »
- civil:
 - « Le secret bancaire, protégé par les sanctions de l'article 458 du Code pénal et ne pouvant être levé d'après l'article 41 alinéa 2 de la loi du 5 avril 1993 que par la loi, est d'ordre public. (...) »
 - « L'obligation au secret de la banque est [...] une obligation de résultat. »

[article 6 Code civil: « On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs. »]
- européenne: der Weduve

La CSSF

- du gardien de la forteresse à la modération
- rapports annuels 2003, 2012 et 2013
 - Le « consentement Codeplafi »
 - ❖ Constat: le secret bancaire étant pénalement sanctionné est d'ordre public par nature
 - ❖ Mais par un: consentement permissif spécifique (par opposition à une renonciation générale) le secret peut être levé
 - ❖ Conditions:
 1. Intérêt du client
 2. Spécificité du consentement
 - contenu de l'information
 - destinataire de l'information
 - finalité recherchée
 - durée
 - ❖ (Ces quatre critères ne sont pas nécessairement cumulatifs)
- Circulaire 12/552

Une volonté de réforme combattue

- projet de loi n° 7024
- un long combat confus et d'arrière garde
- un texte de compromis

Le compromis

- des règles organisationnelles
 - article 37-1(5) LSF

- une exception supplémentaire au secret bancaire
 - article 41 (2bis) LSF

- un rappel sur la protection des données
 - article 41 (9) LSF

Les règles organisationnelles

- exigence d'un contrat de service entre l'entité sous-traitante et le sous-traitant
 - déjà repris dans la circulaire 12/552
- la banque qui sous-traite garde l'entière responsabilité du respect de l'ensemble de ses obligations prudentielles
- la banque qui sous-traite doit accepter une possible sous-traitance en cascade par son sous-traitant
- ❖ EBA: draft guidelines on outsourcing arrangements 22.6.2018

Deux cas de figure

1. sous-traitance à une entité réglementée au Luxembourg
2. sous-traitance à une personne autre qu'une entité réglementée au Luxembourg

Sous-traitance à une entité réglementée au Luxembourg

- Quatre conditions liées à la personne du sous-traitant
 1. une personne établie au Luxembourg
 2. soumise à la surveillance de la CSSF, BCE ou du CAA

➤ Quid des succursales?

➤

entités européennes

entités non-européennes

 3. tenue à un secret pénalement sanctionné
 4. un contrat de service couvrant les renseignements communiqués
- Si les quatre conditions sont réunies
 - des informations couvertes par le secret professionnel peuvent être transmises au sous-traitant
 - sans l'accord ou l'information préalable du client

Sous-traitance à une entité non-réglémentée au Luxembourg Conditions de l'exception

1. la personne du sous-traitant:

(i) une entité

- pas une personne physique
- une personne morale
 - ❖ un groupement de personnes sans personnalité morale?
- le pays d'établissement indifférent
- appartenance au groupe ou non indifférente

(ii) soumise par la loi à une obligation au secret professionnel ou qui est liée par un accord de confidentialité

(iii) l'exception vaut pour la société sous-traitante, ses employés et (!) les personnes qui sont à son service

Sous-traitance à une entité non-réglémentée au Luxembourg Conditions de l'exception

2. L'information des clients sur :

- les services sous-traités
- le type de renseignements transmis
- le pays d'établissement des entités sous-traitantes
- ❖ (?) identité des sous-traitants

Sous-traitance à une entité non-réglémentée au Luxembourg Conditions de l'exception

3. Accord du client

- le client
 - « Cette décharge peut se faire par le client seul et vaudra par rapport à toutes les informations qui seront transmises dans le cadre de la sous-traitance » (doc. Parl. 7024⁵)

Sous-traitance à une entité non-réglémentée au Luxembourg Conditions de l'exception

3. Accord du client

- forme de l'accord

- 1. « conformément à la loi »

- ✓ un accord
 - quelle loi?
 - quid du caractère d'ordre public du secret bancaire
 - ✓ principe général
 - ✓ jurisprudence: article 458 du Code pénal

Sous-traitance à une entité non-réglémentée au Luxembourg Conditions de l'exception

3. Accord du client

- forme de l'accord
 - 2. « selon les modalités d'information convenues entre parties »
 - Doc.parl.7024⁵ : les modalités d'information convenues entre parties « telles que prévues notamment dans les conditions générales, des contrats de dépôt, des contrats d'assurance ou autre contrat similaires »
 - Conditions générales – clause de modification par voie d'accord tacite
 - Loi va au-delà des modifications de contrats par accord tacite
 - vise les modalités d'information
 - voir exemples cités dans les travaux préparatoires

I.3. Violation du secret par le sous-traitant

- conséquences pénales
- conséquences civiles
- conséquences réglementaires

➤ **Article 41 (9) LSF**

- *« Sans préjudice de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel »*
- RGPD depuis le 25 mai 2018
- Cumul des obligations

➤ **Données à caractère personnel : Définition**

- *« Toute information se rapportant à une personne physique identifiée ou identifiable »*

➤ **Transfert de données = Traitement**

- Exigence de licéité

Licéité du traitement

Tout traitement de données personnelles n'est licite que dans la mesure où au moins l'une des conditions suivantes est remplie:

- 
- **Consentement** express de la personne concernée
 - Nécessaire à **l'exécution d'un contrat**
 - Nécessaire pour le respect d'une **obligation légale**
 - Nécessaire aux fins des **intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers (mise en balance avec les intérêts et libertés et droits fondamentaux de la personne concernée)
 - Nécessaire à l'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique
 - Nécessaire pour la sauvegarde des intérêts vitaux de la personne concernée ou toute autre personne physique

Sous – traitant : Définition

➤ Définition :

« La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »

- Agit sur instructions écrites du responsable du traitement lequel détermine les finalités et les moyens du traitement
- Pas d'initiatives propres s'il agit comme sous-traitant
- En cas d'outsourcing de services dans ces conditions, le cocontractant de la banque est à qualifier de sous-traitant

➤ Attention

Qualification se fait suivant une analyse factuelle, traitement par traitement

- Une société peut traiter les mêmes données (i) en tant que sous-traitant suivant les stipulations en vertu d'un contrat de sous-traitance avec le responsable de traitement, (ii) en tant que co-responsable du traitement et (iii) en tant que responsable de traitement pour se conformer à ses propres obligations légales (ex. KYC/AML)

Sous-traitance – Règles organisationnelles

➤ **Importance du choix du sous-traitant**

Garanties suffisantes, notamment en termes de connaissances spécialisées, de fiabilité, de ressources et de sécurité

➤ **Obligation de contrat de service (art. 28 RGPD)**

- Art. 37-1(5) et (5bis) LSF
- Obligations contractuelles détaillées
- Autorisation écrite préalable du RT pour la désignation d'un autre sous-traitant + contrat identique



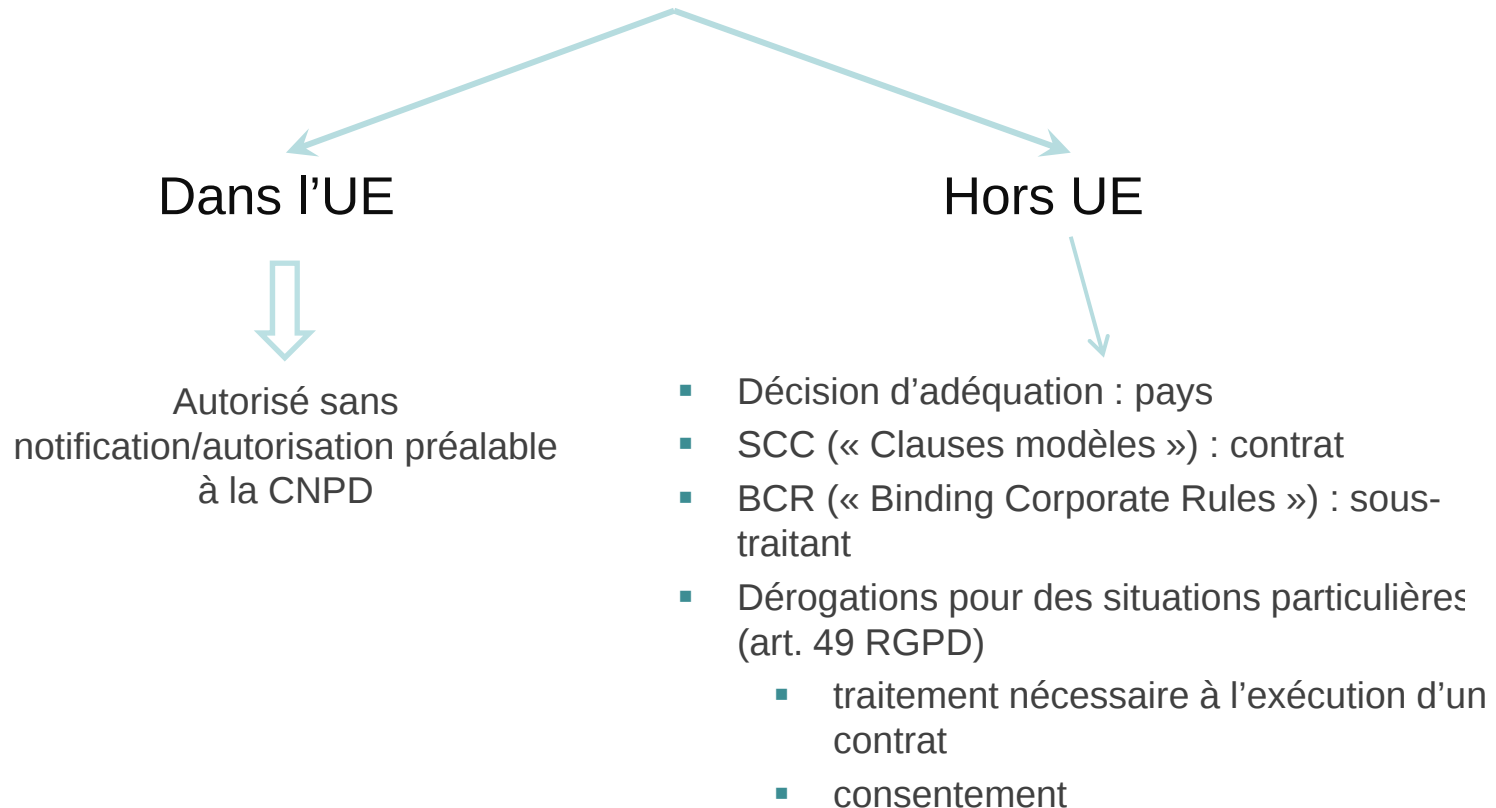
minimisation des données (pseudonymisation)

Obligation d'information des personnes concernées

- Informations devant être fournies par le responsable du traitement aux personnes concernées en cas d'outsourcing:
 - Destinataire(s) / Catégorie(s) des destinataires (donc sous-traitants et sous-sous-traitants)
 - Si transfert vers un pays tiers=> le caractère adéquat de la protection / référence aux garanties appropriées et les moyens d'en obtenir une copie
- Information concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples

II. Protection des données

Transfert de données personnelles à l'étranger



La Commission UE peut adopter une « décision d'adéquation ». En 2018:

Suisse
Argentine
Guernesey

Canada
Uruguay
Ile de Man

Israël
Andorre
Jersey

Nouvelle Zélande
Islande
Iles Faeroe

Liechtenstein
Norvège

Consentement sous le RGPD

➤ Définition

Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

- Consentement explicite requis (pas de case pré-cochée)
- Sans information conforme au RGPD, pas de consentement valable!
- Validité du consentement limitée
 - Véritable liberté de choix
 - Possibilité de refuser ou de retirer son consentement sans préjudice (« *Il est aussi simple de retirer que de donner son consentement.* »)
 - Destinataire(s) / Catégorie(s) des destinataires (donc sous-traitants et sous-sous-traitants) à désigner
 - Pas de consentement si traitements globaux

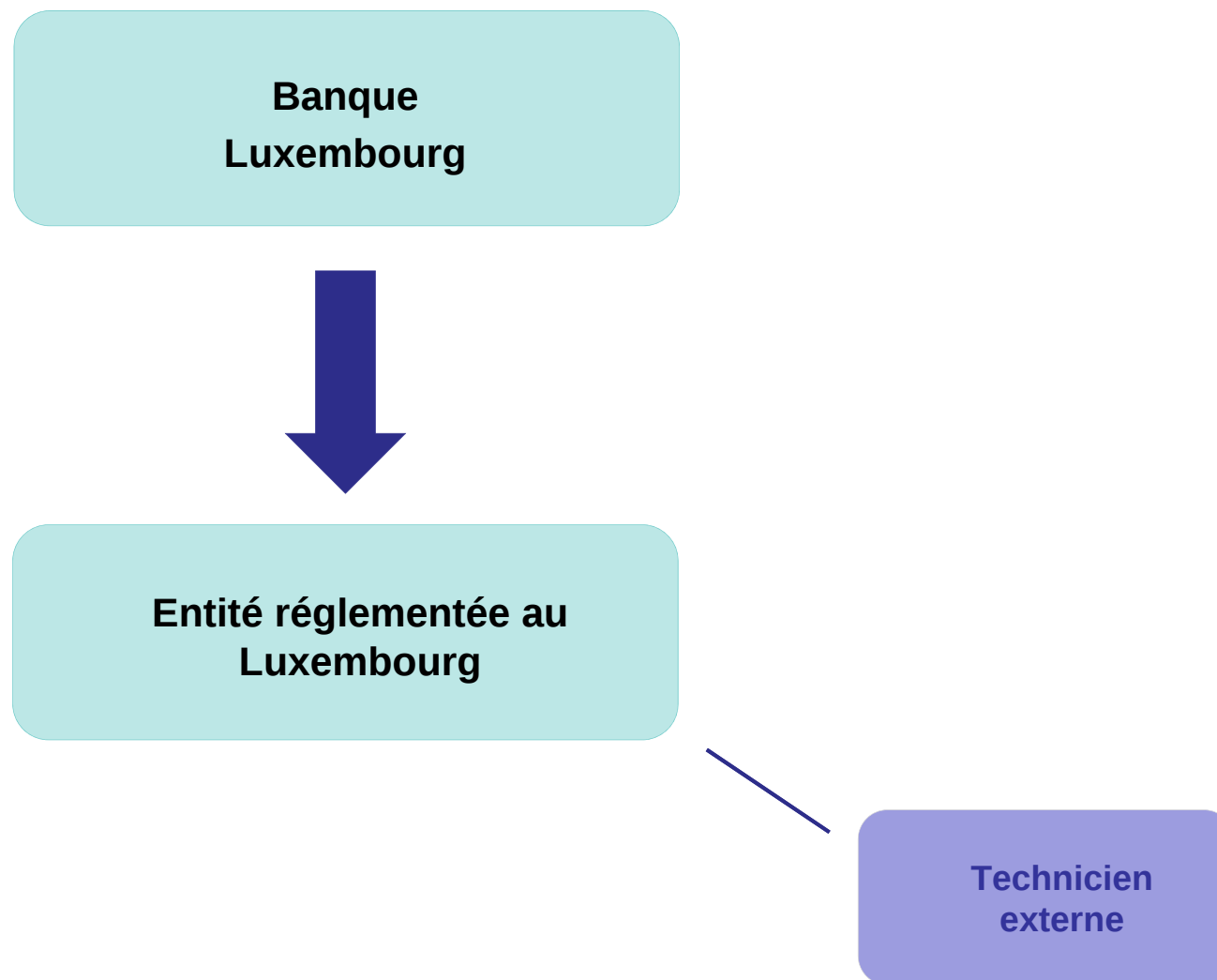
Violation de la protection des données par le sous-traitant

- le sous-traitant au sens RGPD
- le sous-traitant / responsable du traitement
- le co-responsable du traitement

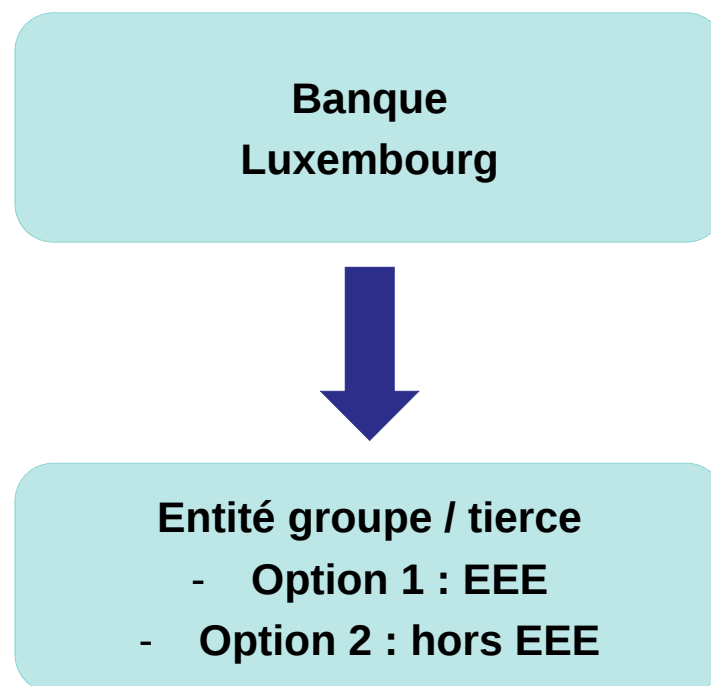
Conclusion

- Notion de sous-traitance différente
- Consentement art. 41 LSF >< consentement art. 49 RGPD
- Différence de régime de responsabilité
- Respect obligations d'information RGPD
 - Transfert UE possible
- Transfert hors UE : adéquation pays ou garanties appropriées

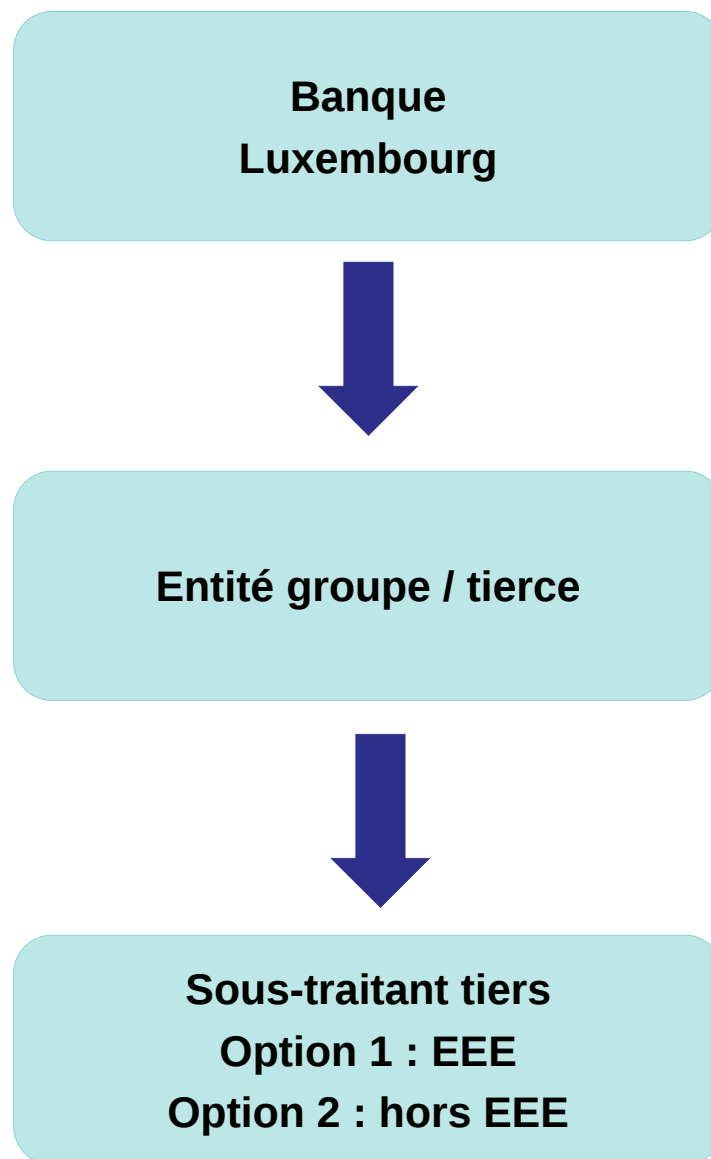
III. Exemples pratiques



III. Exemples pratiques

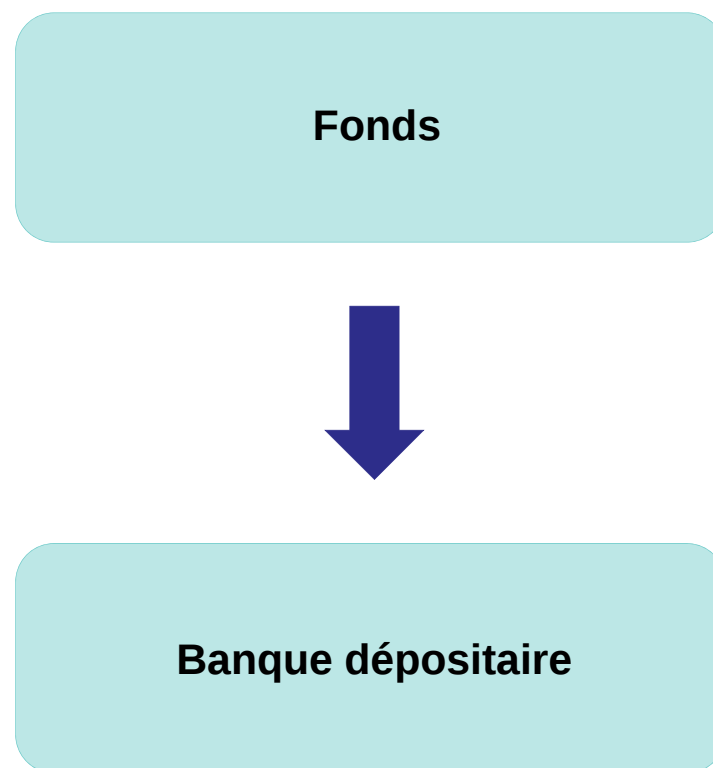


III. Exemples pratiques



III. Exemples pratiques

Sous-traitance KYC



**Merci pour
votre attention**