Enjeux et bonnes pratiques

FÉDÉRATION DES TIERS DE CONFIANCE DU NUMÉRIQUE

Sommaire

Introduction

Lors de toute entrée en relation avec un nouveau client/utilisateur, un processus de connaissance/vérification de l'identité de celui-ci s'avère indispensable pour atténuer les risques liés à la fraude à l'identité. De plus, un tel processus répond, de plus en plus souvent, à une contrainte légale, comme en matière de lutte contre le blanchiment d'argent, le financement du terrorisme et la fraude (LCB-FT) dont l'application ne se limite plus au seul secteur financier, ou encore dans le cadre de la lutte contre le travail illégal. Ce processus est communément désigné par le KYC (Know Your Customer).

Si le KYC est crucial pour les personnes physiques, le processus de connaissance des données permettant de vérifier l'identité d'une Personne Morale l'est tout autant, mais les réponses à apporter aux défis soulevés sont beaucoup plus complexes. En effet, les structures des entreprises impliquent souvent des organisations juridiquement disparates (maison mère, filiale, établissement,...), des opérations internationales diverses et un personnel en constante évolution. Cette complexité est exacerbée par des normes variables d'un Etat à l'autre et une vie juridiquement fluctuante (création, restructuration, fusion, liquidation...).

Pour tenir compte de ces réalités, seul un processus de connaissance/vérification des données d'identité qui repose sur un contrôle continu des données à vérifier pourra garantir l'exactitude desdites données. En outre, les coûts associés à l'identification des entreprises sont plus élevés en raison de la nécessité de disposer de ressources importantes et de beaucoup de temps.

Le présent avis d'expert a pour objet de dresser un panorama des éléments à prendre en compte dans ce processus de connaissance/vérification de l'identité des personnes morales. Ce processus est désigné dans le présent document par le KYB (Know Your Business).

Cet avis d'expert ne traite que du KYB relatif aux personnes morales (SARL, SAS,...) et non aux professionnels exerçant leurs activités sous une autre forme juridique (comme ceux relevant du statut des artisans ou des indépendants).

Enfin, le KYB est systématiquement associé à un voire plusieurs KYC de personnes physiques, si celles-ci sont habilitées à agir pour le compte de la personne morale.

Le KYC des personnes physiques représentantes d'une entreprise ne sera pas développé dans ce document. Il est sur ce point renvoyé à l'avis d'expert "KYC: Comment maîtriser et optimiser votre connaissance client" (08/2021).

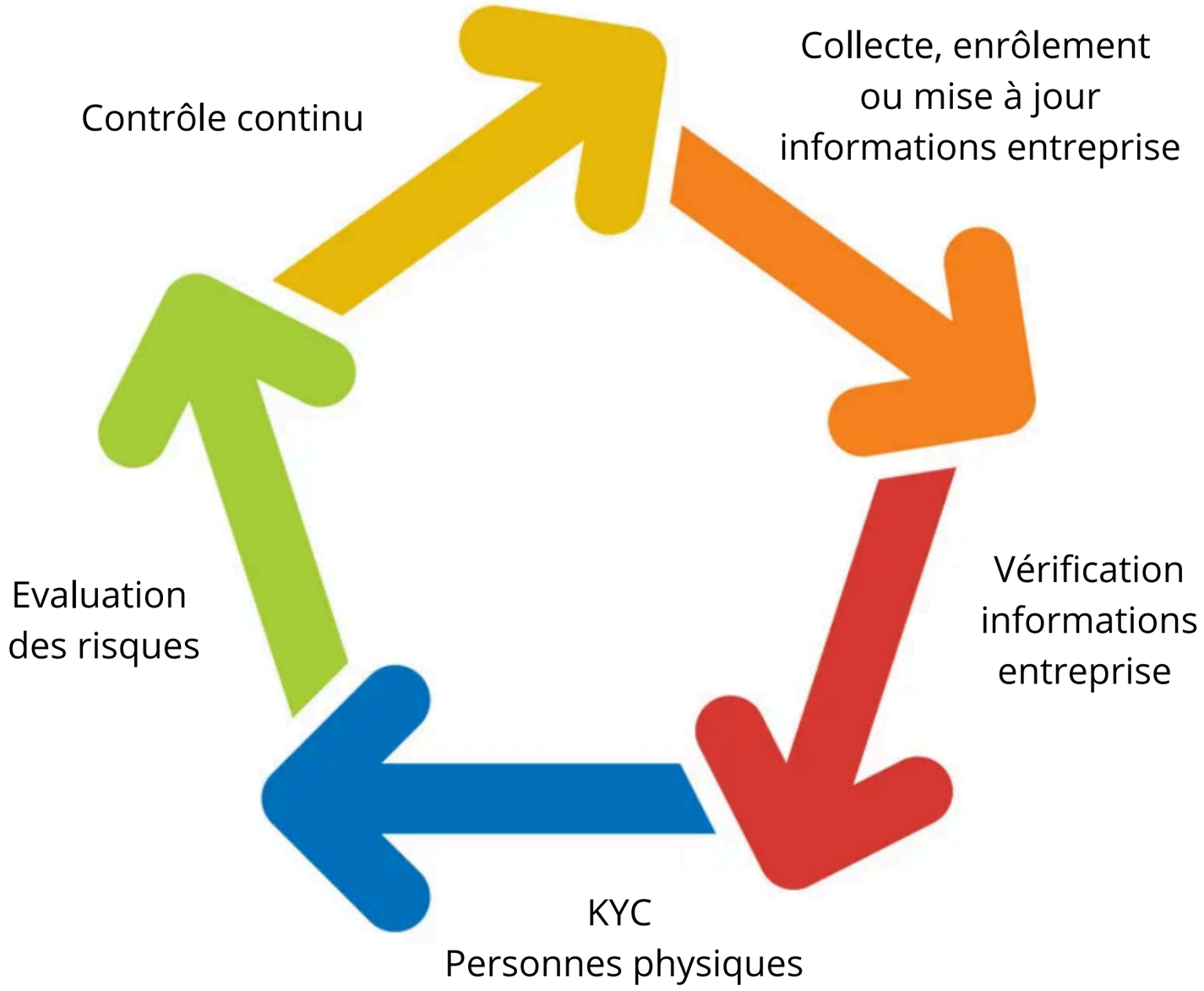
Pour mettre en œuvre des processus efficaces de KYB, il est nécessaire de développer des systèmes de vérification robustes, de s'adapter aux contraintes réglementaires et de tirer parti des technologies de pointe pour améliorer la précision et l'efficacité des contrôles.

Si les informations KYB sont inexactes ou compromises, cela peut en effet entraîner des conséquences graves pour l'entreprise (dont la mise en cause de sa responsabilité voire celle de ses dirigeants), avoir des répercussions sur son image de marque et des incidences sur les systèmes financiers et économiques plus larges.

La confiance apportée dans le processus de connaissance/vérification de ses clients personnes morales contribue ainsi à apporter plus de sécurité économique et juridique dans les relations d'affaires en général.

De plus en plus souvent, le KYB est indispensable pour se conformer aux réglementations et lois en vigueur, qui imposent aux entreprises de vérifier l'identité et l'activité de leurs clients et partenaires commerciaux.
Pour répondre à ces différents enjeux, le présent avis d'expert liste les principales réglementations et apporte des pistes en définissant les données essentielles à collecter pour identifier une personne morale et les bonnes pratiques à appliquer pour les vérifier.

KYB



1. Les données d'identification

Chaque secteur d'activité ou type d'usage nécessite le recueil de données d'identification des personnes morales spécifiques, autrement dit un KYB à dimension variable.

A la lecture des différentes réglementations, il apparait néanmoins qu'un dénominateur commun de données peut être extrait.

1.1. Données socles et données complémentaires

Nous pouvons parler de **données socles** relatives à l'identité d'une entreprise ou organisation regroupant les données suivantes :

- Sa dénomination
- Son identifiant (identifiant SIRENE, Numéro de TVA intracommunautaire ou équivalent hors Europe)
- Sa forme juridique
- L'adresse légale de l'entreprise
- Ses activités
- L'identité des représentants légaux (Données Personne Physique, le KYC Personne Physique est obligatoire cf. avis d'expert KYC

S'ajoutent d'éventuelles **données complémentaires** (en fonction du besoin, par exemple règlementaire), dont :

- Noms commerciaux
- Identité des bénéficiaires effectifs (en fonction de la réglementation appliquée)
- Statuts
- Structure de propriété
- Sous-traitants
- En cas de délégation, le mandat (ou chaîne de mandats) et l'identité du mandataire
- Comptes
- Noms de domaines dont l'entreprise est propriétaire
- Autres justificatifs organisation et personnes physiques
- Attestation URSSAF
- …

Si la disparité des types de KYB rend l'exercice complexe pour ceux qui souhaiteraient proposer des offres de services de KYB, **les données socles sont un premier sous ensemble qui fait déjà l'objet d'offres disponibles sur le marché, simplifiant les processus de KYB à réaliser.**

1.2. Des sources authentiques disponibles

Concernant les entreprises, le Kbis atteste de l'existence juridique de l'entreprise et donne une information vérifiée qui fait foi. Il s'agit du seul document officiel prouvant l'identité et l'adresse de la personne (physique ou morale) immatriculée, son activité, ses organes de direction, administration, gestion ou contrôle, ainsi que l'existence ou non d'une procédure collective engagée à son encontre.

Les informations du Kbis sont issues des déclarations des entreprises. Les greffiers, officiers publics et ministériels ayant pour charge de contrôler la validité des actes et documents justificatifs produits. Le greffe du tribunal de commerce vérifie ainsi la légalité et la validité des changement de gérant de société.

De nombreuses pièces sont à fournir pour valider le changement :

- L'assemblée générale ordinaire des associés décidant du changement de dirigeant
- Les statuts à jour si le représentant légal est statutaire
- Une publicité dans un journal d'annonces légales
- Une pièce d'identité en cours de validité du nouveau représentant légal
- Une déclaration sur l'honneur de non condamnation du nouveau dirigeant

Des points de contrôle sont par ailleurs opérés sur ces documents, notamment pour :

- Vérifier dans l'assemblée :
  - Que les éléments d'identité de la société correspondent à ceux mentionnés sur l'extrait Kbis (dénomination sociale, adresse du siège social, numéro d'identification)
  - Que les associés sont présents ou représentés
  - Qu'elle soit signée par les associés
- Vérifier dans la publicité du Journal d'annonces légales que :
  - les informations d'identité de la société sont identiques avec celles du Kbis et de l'AG
  - l'identité du nouveau dirigeant correspond à celle mentionnée dans l'AG, la date d'effet de la nomination du nouveau représentant est également vérifiée

1.3. Exemples de dispositifs de sécurisation à destination des personnes morales

- MonIdenum : ce service d'authentification gratuit opéré par Infogreffe, permet à toute personne ayant activé son identité numérique de s'authentifier sur les services digitaux partenaires. Pour le dirigeant d'entreprise, le service opère un rapprochement avec le registre du commerce et des sociétés, lui permettant d'agir en son nom en toute sécurité.

- Pro Connect : solution proposée par l'Etat pour certifier son identité auprès des services publics. Cependant, ce service gère uniquement l'identification du représentant légal. La solution est donc intéressante pour les entreprises individuelles mais pas pour les entreprises de taille plus importante dans la mesure où les délégations de pouvoir ne sont pas gérées.

2. Principales règlementations en matière de KYB

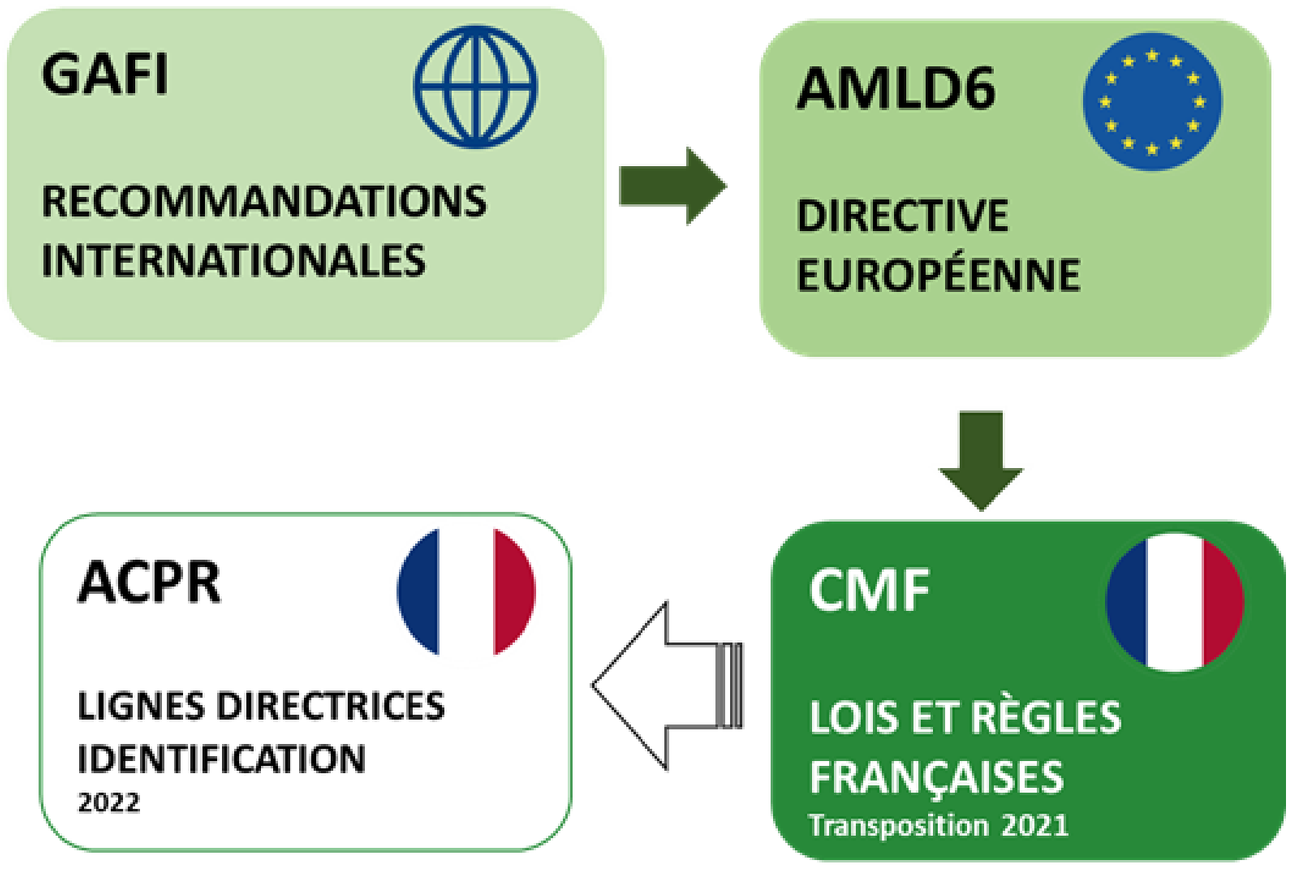
Les mesures de vigilance sur l'enrôlement pour contrer la fraude financière et fiscale sont présentes dans de nombreux textes de lois comme le Code Monétaire et Financier, la loi SAPIN II ou le Code du Travail et cette liste n'est pas exhaustive. En matière de lutte contre le blanchiment d'argent, le financement du terrorisme et la fraude, la réglementation LCB-FT reste l'une des plus précises en matière de pratiques KYB et donne une vision assez étendue des éléments à contrôler.

Si les entités soumises aux contraintes relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (notamment dans les secteurs bancaires, financiers et assurantiels) sont classiquement soumises à des obligations fortes de connaissance et de vérification de leurs clients, en ce y compris les personnes morales, d'autres activités sont concernées par des contraintes de même nature.

2.1. Lutte Contre le Blanchiment de Capitaux (LCB) et le Financement du Terrorisme (FT) et KYB

a) En application du CMF

La Lutte contre le Blanchiment de Capitaux est cadrée par le Groupe d'Action Financière- GAFI (Financial Action Task Force-FATF), organisation intergouvernementale en charge de la surveillance des activités illégales autour notamment du blanchiment d'argent et du financement du terrorisme au niveau mondial. Le GAFI est une référence mondiale en termes de LCB-FT et publie en particulier une liste noire et une liste grise qui identifient les pays à haut risque et ceux sous surveillance.



2

Les pays membres du GAFI sont appelés à mettre en place des process de surveillance renforcée ou appliquer des contre-mesures pour protéger le système financier international contre les risques actuels de blanchiment d'argent, de financement du terrorisme et de financement de la prolifération qui en découlent. L'Europe a transposé ces règles au travers de la directive AMLD6.

En France , le Code Monétaire et Financier (CMF) a intégré dès 2020, des règles d'identification des personnes physiques et morales pour la conformité avec la directive AMLD, en particulier dans la section Identification et vérification de l'identité du client. Pour expliquer aux entités assujetties comment appliquer les règles du CMF, l'ACPR, le régulateur de la Banque de France a publié des « lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle » .
Progressivement, l'application des dispositions du CMF relatives à la vérification de l'identité des clients, notamment afin de lutter contre le blanchiment d'argent, le financement du terrorisme et la fraude, s'est étendue à des secteurs d'activités de plus en plus larges (article L561-2 du CMF).

Par l'Article L561-4-1 du CMF, les assujettis au CMF doivent suivre les mesures de vigilance relatives à l'identification de leur clientèle en évaluant les risques liés à leurs activités en matière de LCB/FT.

L'Article L561-5 du CMF précise qu'il faut identifier son client et le cas échéant, le/s bénéficiaires effectif/s et ceci avant d'entrer en relation d'affaire. Cette vérification doit être effectuée à partir d'éléments à caractère probant. Dans le cas d'une relation occasionnelle, les mesures de vérification s'appliquent en fonction du risque LCB/FT de l'opération et du montant. Les données doivent être réactualisées (Article L561-5-1 du CMF).

L'Article L561-2 du CMF donne la liste exhaustive des assujettis au CMF qu'ils soient personne morale ou physique. Cette liste couvre des domaines très variés, la liste exhaustive est en annexe.

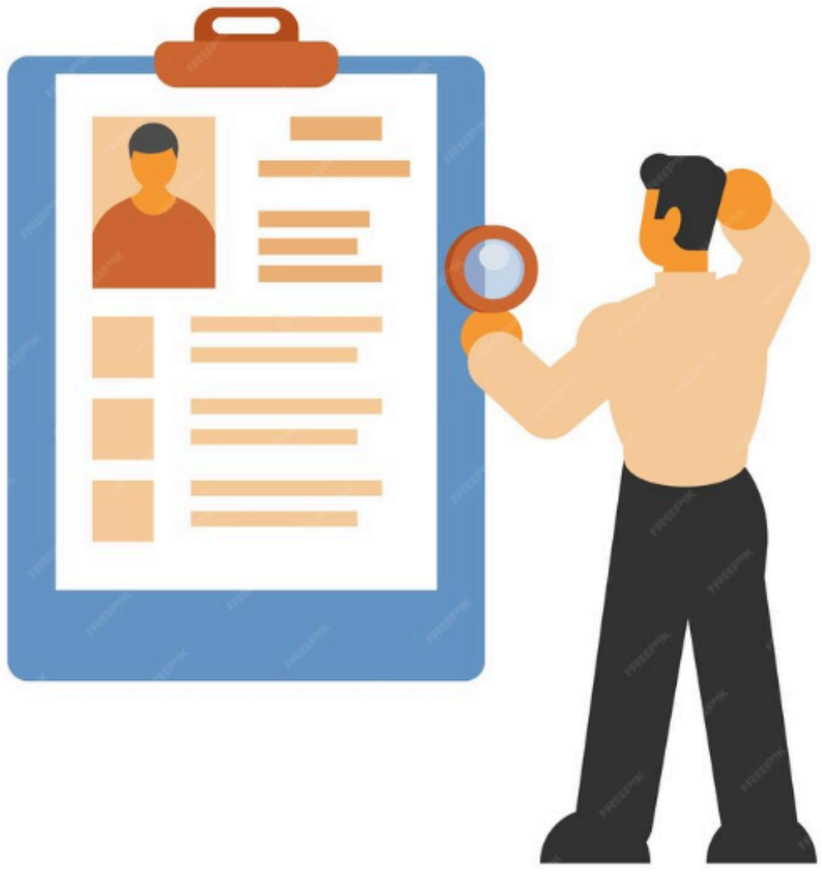
Dans ce chapitre, le document de l'ACPR «lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle» a permis de détailler les mesures du CMF relatives au KYB.

Les sous articles R561-5-1 et R561-5-2 du CMF précisent les mesures de vérification de l'identité du client.
Article L561-5 point 2°) du CMF (chapitre 2.1 du document de l'ACPR) : l'identité d'un client personne morale repose sur la présentation de tout document écrit à caractère probant (KBis ou équivalent au niveau international): documents ou données numériques, en présentiel et distanciel. Un original ne peut être fourni par le client qu'en présentiel, sinon c'est à l'organisme qui traite la demande d'obtenir les copies ou données numériques de l'identité du client auprès d'un registre officiel.

L'article R561-5-1 du CMF prévoient des modalités possibles en présentiel et/ou en distanciel.

Pour tous ces exemples, le KYC de la Personne Physique représentant la Personne Morale doit être réalisé obligatoirement selon les règles du CMF. Il en va de même du KYC du bénéficiaire effectif.

L'Article R561-5-2 du CMF ne s'applique qu'en distanciel. Cet article précise les mesures à respecter si les modalités posées à l'article R561-5-1 du CMF ne peuvent pas être appliquées : c'est-à-dire dans les cas de vérification en distanciel, et sans identité de l'organisation avec un moyen eIDAS ou certifié ANSSI.



b) En application du Code des Postes et des Communications électroniques

Dans un autre domaine, le code des postes et communications électroniques (CPCE) énonce les règles relatives à l'exercice des activités de communication électronique en France, et notamment les obligations des opérateurs (dont les opérateurs télécom) en matière de KYB pour les personnes morales. Plus précisément, les principaux articles du CPCE qui peuvent être pertinents pour le KYB incluent notamment :

- Article L. 33-1 : Obligations en matière de lutte contre le blanchiment d'argent et le financement du terrorisme.
- Article L. 32-1 : Obligations de vigilance et de contrôle des opérateurs de télécommunications envers leurs clients.
- Article R. 133-10 : Dispositions relatives à la vérification de l'identité des clients et à la collecte des informations nécessaires pour le KYB.
- Article R. 133-11 : Mesures de vigilance renforcée à mettre en place en cas de risque accru de blanchiment d'argent ou de financement du terrorisme.

Ces articles et d'autres dispositions du CPCE définissent les obligations et les responsabilités des opérateurs de télécommunications en matière de KYB et de lutte contre les activités illicites. Il est important pour les opérateurs de de respecter ces règles pour assurer la sécurité et la conformité de leurs services.

2.2.Transparence et lutte contre la corruption

L’article 17 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie dite loi Sapin 2 concerne, à titre principal, les dirigeants d’entreprises et les entreprises dont le chiffre d’affaires est supérieur à 100 millions d’euros et ayant au moins 500 salariés.

Cet article impose aux personnes concernées de mettre notamment en œuvre des mesures et procédures « d'évaluation de la situation des clients, fournisseurs de premier rang et intermédiaires au regard de la cartographie des risques » (article 17, II, 4°). Il résulte de cette disposition un certain nombre de contraintes relatives au KYB qui devront être définies par l’entité concernée selon la cartographie des risques qu’elle est tenue d’établir. Ces mesures doivent donc être adaptées aux risques identifiés et régulièrement réévaluées par l’entité afin de lutter contre la corruption et autres manquements à la probité.

A titre d’illustration, les mesures suivantes, inspirées de celles de la lutte contre le blanchiment de capitaux et le financement du terrorisme, peuvent être mises en place en matière de KYB :

- Vérification sur pièces (originaux ou copies certifiées conformes) de l'identité des personnes morales avec lesquelles elles entretiennent une relation d'affaires. Cette vérification doit être renouvelée régulièrement.
- Collecte d'informations sur les personnes morales avec lesquelles elles entretiennent une relation d'affaires, telles que la nature de l'activité, la structure juridique, les dirigeants, les actionnaires, les bénéficiaires effectifs, etc.

Ces mesures et procédures devront être documentées afin d’être en mesure d’en rapporter la preuve et de démontrer le respect des exigences posées.

2.3. Lutte contre le travail illégal

Dans le secteur du BTP et des Transports, le contrôle de la chaîne de sous-traitance est primordial : en complément des vérifications de premier niveau communes aux autres secteurs, l'entreprise donneuse d'ordre doit en effet vérifier l'ensemble de la chaîne de sous-traitance (1) et notamment les éléments relatifs au Code du travail (2).

Les lois à retenir pour ces deux secteurs :

- Code du travail :
  - Articles D8254-1 à D8254-6 sur les vérifications nécessaires dans le cadre de l'obligation de vigilance des entreprises pour toutes opération d'un montant minimum de 5000€ HT avec les des cocontractants
  - Articles L 8222-1 à L 8222-7 visant à lutter contre le travail dissimulé et imposant la solidarité financière des donneurs d'ordre et des maitres d'ouvrage
- Loi Savary : Décret n°2015-364 du 30 mars 2015 relatif à la lutte contre les fraudes au détachement de travailleurs et à la lutte contre le travail illégal
- Devoir de vigilance : Loi 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre. Vise à prévenir les atteintes graves aux droits humains, aux libertés fondamentales, à la santé et la sécurité des personnes et à l'environnement.

[1] voir fiche technique de la direction des Affaires Juridiques
[2] Voir note de l'URSSAF sur les attestions de caisse de congés payés notamment

2.4. Contrôle de l'activité & Autorisation d'exercer une profession

Un certain nombre de règlementations et notamment le code du Transport, celui du commerce ou de la santé, impose également des contraintes spécifiques liées aux autorisations d'exercer certaines activités. Ainsi, un vendeur doit vérifier que l'activité d'une entreprise acheteuse correspond bien à l'objet de la transaction, lié à la nature des produits (produits réglementés comme les médicaments) ou à la nature de l'activité de l'entreprise vendeuse (par exemple les grossistes ne peuvent pas vendre à des particuliers).

Le Code des Transports et notamment les articles suivants imposent également une vérification des autorisations d'exercer pour les entreprises donneuses d'ordre avant toute entrée en relation :

- Article R1422-1 : imposant l'inscription de tout commissionnaire de transport au registre des commissionnaires de transport
- Article R1422-9 : Préalablement à la conclusion de tout contrat de commission de transport, le commissionnaire de transport doit s'assurer que l'entreprise est habilitée à exercer l'activité demandée.

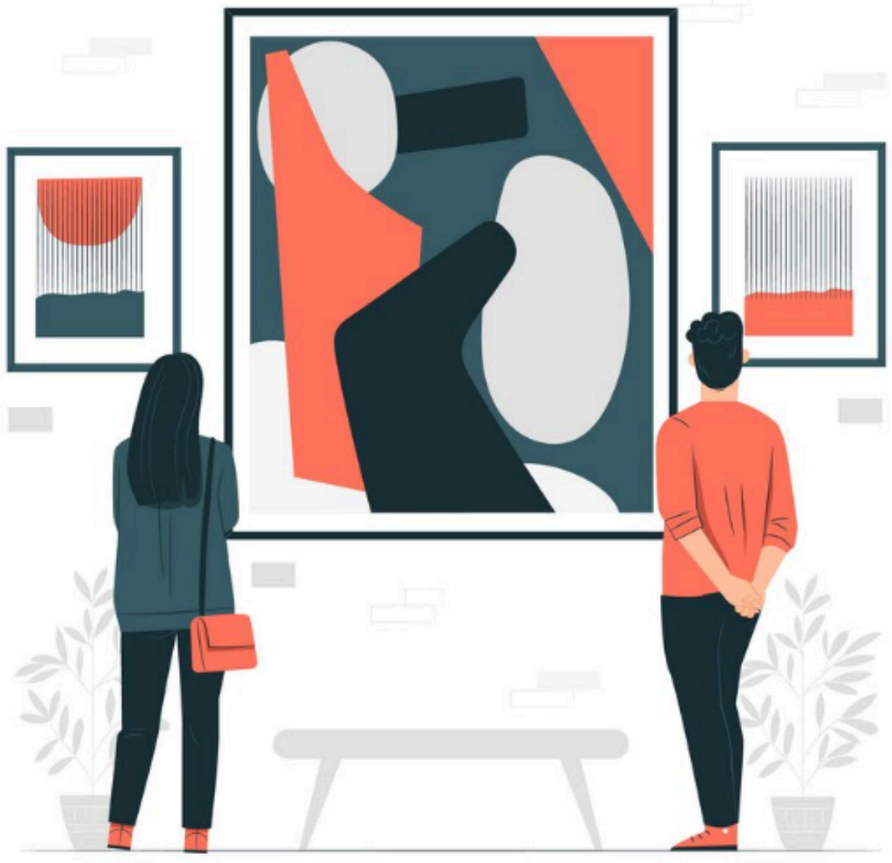
2.5. Lutte contre le trafic de biens culturels

De prime abord lorsque l'on pense à l'acquisition d'un objet d'art, on visualise l'acheteur ayant un coup de cœur sur une œuvre dans une galerie, pour l'apposer fièrement sur les murs de sa maison. Or les personnes morales qui acquièrent des objets d'art sont plus nombreuses que l'on ne le pense et ce notamment grâce à une fiscalité avantageuse (cf. article 238 bis AB du Code Général des Impôts).

Personne morale certes, mais acheteur tout de même, ce qui impose au même titre que pour les personnes physiques, la mise en place de procédures de connaissance du client.

Le marché de l'Art est régi majoritairement par deux catégories de contraintes légales à savoir :

- Le travail obligatoire de recherche de provenance dans le cadre de la loi contre le trafic de biens culturels, imposant au professionnel de connaître l'origine du bien afin d'en établir une traçabilité la plus complète possible.
- L'application de la Directive UE 2018/843 transposée en droit français le 12 Février 2020 par l'Ordonnance N°2020-115 visant à lutter contre le blanchiment de capitaux et financement du terrorisme.



Dès lors que l'acheteur, qu'importe sa nature juridique, dépasse un montant d'achat de 10.000 euros (vente unique ou cumulées), les professionnels du marché de l'Art doivent s'assurer et formaliser au travers d'écrits, que l'opération ne rentre pas dans le cadre d'une opération de blanchiment ou de financement du terrorisme.

Les professionnels du marché de l'Art doivent aussi s'informer et renseigner entre autres, la méthode de paiement utilisée, le pays de domiciliation de l'entreprise mais également le secteur d'activité de la société acheteuse. En effet, la Direction Générale de Douanes et Droits Indirects vise par exemple comme secteur d'activité à risque : le BTP, la logistique ou encore l'informatique (liste non exhaustive).

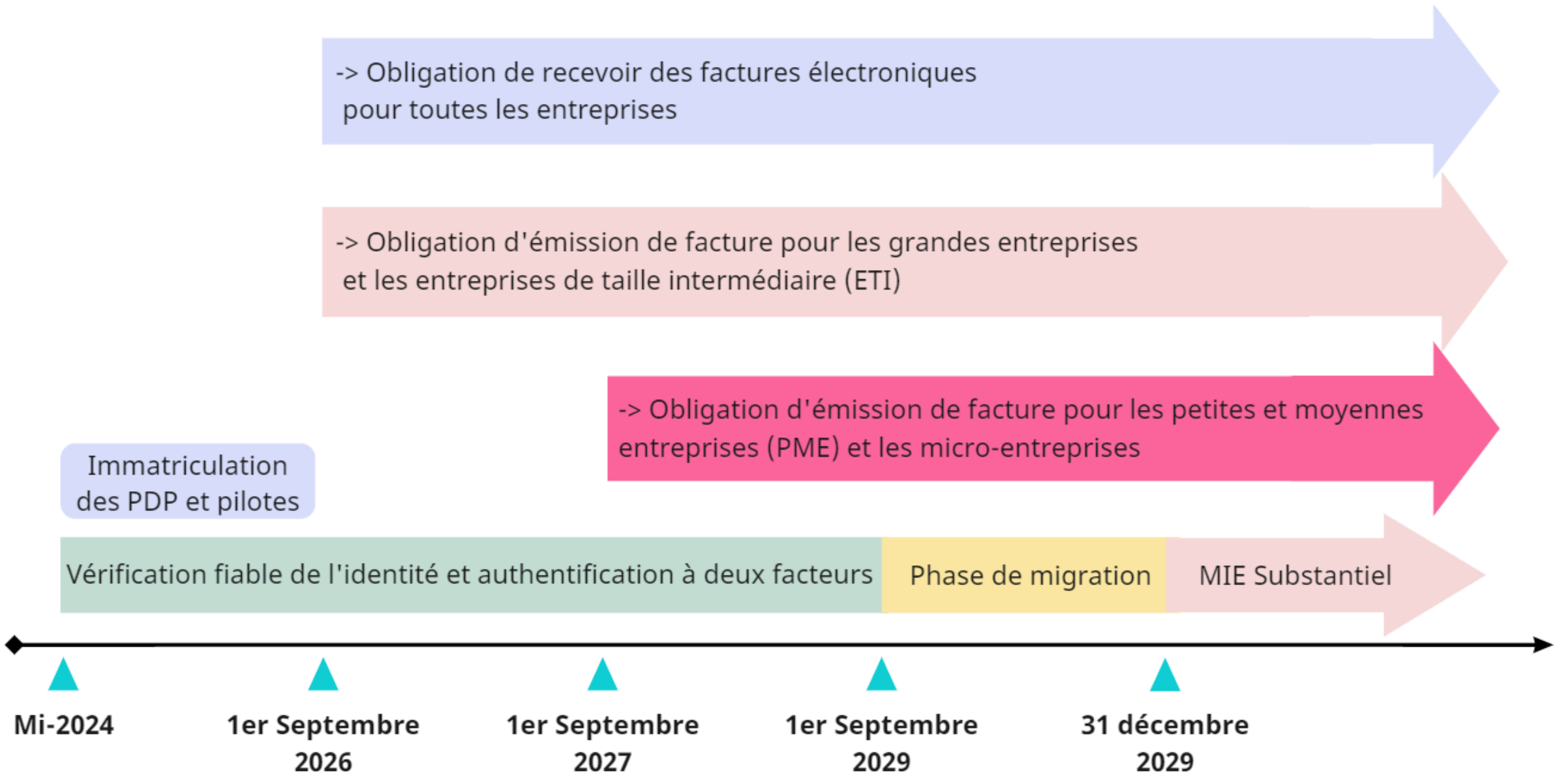
Au sein du marché de l'Art, outre les formes habituelles de personnes morales, on rencontre particulièrement les intermédiaires. Agissant parfois sous la forme de société, ils s'impliquent dans la vente apportant à son bénéfice, leur connaissance et expertise. On retrouve parmi eux, les opérateurs de ventes volontaires, les courtiers en œuvres d'art, les intermédiaires innommés, etc. On rencontre également des sociétés proposant des services de leasing rentrant sous le coup des vérifications des professionnels du marché de l'Art, tant sur la partie recherche de provenance, que sur la partie lutte anti-blanchiment.

Le devoir de conformité des professionnels du marché de l'Art est tout aussi exigible face aux personnes morales à travers les procédures KYB que face aux personnes physiques.

2.6. Lutte contre la fraude à la TVA

La fraude à la TVA serait comprise entre 20 et 25 milliards d'euros par an en France selon une estimation de l'Insee. La facturation électronique qui sera progressivement obligatoire à compter de 2026 selon la taille des entreprises devrait permettre de contribuer de manière significative à la lutte contre la fraude à la TVA notamment en améliorant la traçabilité des transactions, en automatisant les contrôles, en réduisant les erreurs et en simplifiant les contrôles fiscaux.

Le Décret relatif à la généralisation de la facturation électronique a été publié le 25 mars 2024. Il prévoit notamment que les factures électroniques transitent via une plateforme de dématérialisation partenaire (PDP), dont l'accès se fera, en cible, au moyen d'une identité de niveau substantiel ou élevé, associée à la vérification de la qualité et des habilitations de cette personne physique à agir pour le compte de la personne morale émettrice ou réceptrice de factures. Dans l'attente de la cible, avec une vérification d'identité de niveau eIDAS substantiel, différentes étapes sont planifiées, dont voici l'illustration :

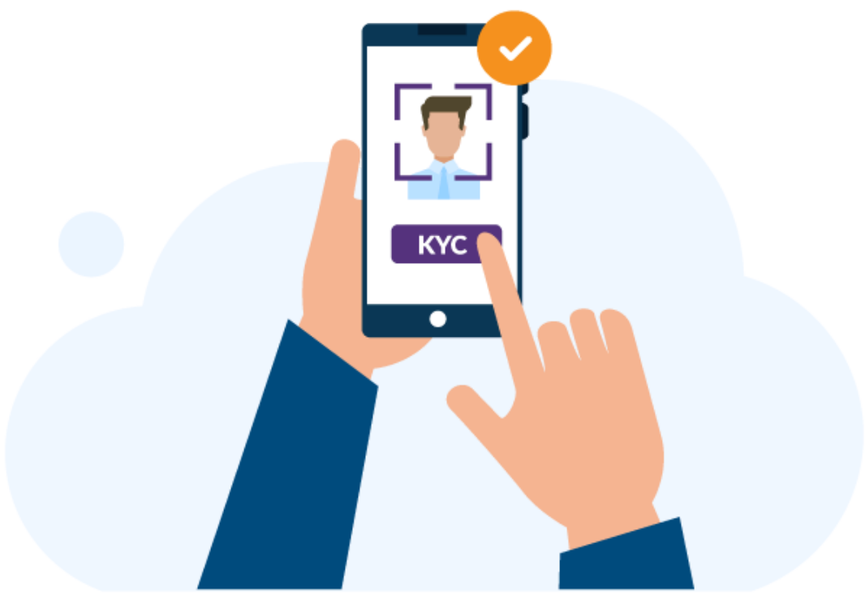


3. Bonnes pratiques et mise en application

La réalisation du processus KYB implique généralement plusieurs étapes et bonnes pratiques pour garantir une diligence raisonnable et se conformer aux réglementations en vigueur. Les travaux d'Open Data menés par l'Etat, depuis plusieurs années, ont d'ores et déjà donné naissance à plusieurs API qui permettent de réaliser des contrôles de connaissance et/ou de cohérence lors d'un process de KYB.

Voici quelques bonnes pratiques à considérer :

- Rechercher/vérifier les informations communiquées par la Personne Morale à partir de sources officielles, ne pas « faire confiance » à celui qui s'enrôle. La vérification des données d'identification d'une Personne Morale peut être ainsi effectuée avec l'aide de différentes sources, notamment :
  - Au niveau français :
    - Infogreffe, registre officiel des données Personnes Morales en France
    - Le Registre National des Entreprises (RNE) nouvellement créé répertorie les informations relatives à toutes les entreprises situées sur le territoire français. Il regroupe l'ensemble des activités commerciale, artisanale, libérale et agricole.
    - Base Sirene : il s'agit d'une base de données mise à disposition gratuitement par l'Etat et référençant les entités implantées en métropole, dans les DOM et les collectivités d'Outre-Mer. Cependant cette base ne contient pas les informations sur le représentant légal.
    - Consultation d'un support habilité à recevoir des annonces légales (SHAL), c'est-à-dire soit un journal d'annonces légales (JAL) soit un service de presse en ligne (en vérifiant l'habilitation de ces supports), par exemple le portail de la publicité légale des entreprises (PPLE et Actulegales.fr).
  - Au niveau européen :
    - le portail E-justice permet de rechercher l'existence d'une société et de récupérer les informations et documents relatifs à cette société (Portail e-Justice européen - Registres du commerce – rechercher une entreprise dans l'UE (europa.eu).
    - Le portail LEI permettant de vérifier le code Legal Entity Identifier : LEI Europa - Outil de validation gratuit du code LEI pour entreprises de l'UE (lei-europa.eu)
- Vérifier le numéro de TVA intracommunautaire via le portail VIES



- Vérifier les données complémentaires :
  - L'adresse légale de l'entreprise : s'il n'existe pas de base officielle régalienne centralisant les adresses d'entreprises, de nombreux services existent aujourd'hui sur le marché pour permettre de contrôler les informations et documents transmis par une société cliente :
    - Vérification du CEV (cachet électronique visible ou 2d-Doc) sur les factures ou attestations de contrats énergie/télécom pour certains facturiers
    - Demander 2 justificatifs de domicile si nécessaire pour contrôler la cohérence des informations
    - Faire appel à des services de vérification d'adresse
    - Utiliser les services d'envoi lettre recommandée physique avec AR
  - Ses activités
    - Recueil des statuts auprès d'Infogreffe ou de sociétés privées spécialisées (services payants)
  - L'identité des représentants légaux
    - Vérifier la liste des représentants légaux fournie via le Kbis
    - Vérifier la liste des mandataires : Aucun registre officiel n'existe en France mais des sociétés privées proposent des services de vérifications de mandats

Il est rappelé que selon les contraintes juridiques et le niveau de granularité de connaissance du client imposés par les textes ou le besoin de sécurité juridique recherchée dans le cadre de la relation d'affaires concernée, le KYB pourra voire devra être complété par le KYC du représentant et/ou du mandataire de la personne morale concernée (cf. avis d'expert KYC).

Par ailleurs, la mise en place de procédures de surveillance continue est obligatoire pour pouvoir réévaluer périodiquement le profil de risque de la société et effectuer des mises à jour du processus KYB en conséquence, notamment en cas de changements significatifs dans la structure ou les activités de la société.

Enfin, il est important de noter également que la traçabilité de tous les contrôles réalisés est primordiale : en cas d'audit ou de contrôle d'une autorité de tutelle, les sociétés assujetties doivent en effet être en mesure de prouver que tout a été mis en œuvre pour réaliser les vérifications règlementaires obligatoires.

4. Perspectives

L'identité numérique des personnes morales fait actuellement l'objet de plusieurs projets européens dans l'objectif de permettre la reconnaissance et le partage de cette identité sur des critères communs et de façon sécurisée.

Projet Registre européen des Personnes Morales

Le projet BRIS, Business Registers Interconnection System, visant à l'interconnexion des registres du commerce sur une plateforme unique a vu le jour en juin 2017. Infogreffe est l'opérateur français. Cette plateforme est accessible depuis le portail juridique de l'Europe : Portail e-Justice européen - Registres du commerce – rechercher une entreprise dans l'UE (europa.eu).

Cette plateforme couvre tous les pays de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège. Les liens vers les sites nationaux sont accessibles via le site.

L'interconnexion des registres des bénéficiaires effectifs n'a pas encore abouti. En effet seules la Grèce, l'Islande et l'Autriche sont interconnectées sur la plateforme européenne.
Les Pays-Bas sont l'un des rares pays à avoir un registre des entreprises intégrant les procurations/délégations.

Portefeuille Européen d'Identité Numérique (PEIN ou EUDI Wallet)

En juillet 2021, la Commission européenne a élaboré une proposition de modification du Règlement 910/2014 sur l'identification et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit Règlement eIDAS.

Compte tenu des différents constats menés sur l'application de ce Règlement et de l'état du marché de l'identité numérique qui est au cœur de la confiance dans la société numérique, la fourniture de portefeuille d'identité numérique au niveau des Etats membres a été proposée.

4

L’objectif est de permettre aux citoyens, aux résidents de l’Union européenne et aux personnes morales de disposer d’une identité numérique sécurisée, interopérable et reconnue par tous les Etats membres.

Le portefeuille européen d’identité numérique (PEIN) est défini comme : « un moyen d'identification électronique qui permet à l'utilisateur de stocker, de gérer et de valider en toute sécurité des données d'identification personnelle et des attestations électroniques d'attributs afin de les fournir aux parties utilisatrices et aux autres utilisateurs des portefeuilles européens d'identité numérique, et de signer au moyen de signatures électroniques qualifiées ou d'apposer des cachets au moyen de cachets électroniques qualifiés; » (définition issue de l’article 3. §42 du Règlement 2024/1183 du 11 avril 2024).

Le PEIN permettra ainsi, notamment aux personnes morales (utilisateur de PEIN), de prouver leur identité et de partager leurs documents, leurs données d’identification et leurs attestations d’attributs, d’un niveau de garantie substantiel ou élevé, avec des organismes des secteurs public et privé (les parties utilisatrices du PEIN). Il devrait donc permettre de réaliser un KYB.

Si la fourniture d’un PEIN de niveau élevé par les Etats membres est obligatoire, son utilisation par les utilisateurs restera volontaire.

Les PEIN devraient constituer le futur socle de l’identité numérique, y compris pour les personnes morales. Le déploiement des premiers wallets est attendu pour 2027.

Comité de rédaction :

- Laila Bendiab
- Anne Cantero
- Rémi Lefort
- Stéphane Mavel
- Hélène Roizin

Entreprises participantes :

- Société d'avocats Caprioli et Associés
- Eunomart
- IDnow
- Syrtals
- Vialink

FÉDÉRATION DES TIERS DE CONFIANCE DU NUMÉRIQUE

5, impasse Gomboust - 75001 Paris
fntc-numerique.com
infos@fntc-numerique.com

Février 2025