

LUTTE ANTI-CORRUPTION

68 Comment rédiger une procédure d'évaluation des tierces parties efficace ?



DAPHNÉ LATOUR,
avocat à la Cour,
counsel, cabinet ARAGO

CONTEXTE

L'objectif poursuivi par l'article 17, II, 4° de la loi n° 2016-1691 du 9 décembre 2016, dite Sapin 2, qui impose que les entreprises concernées mettent en place « des procédures d'évaluation de la situation des clients, fournisseurs de premier rang et intermédiaires au regard de la cartographie des risques », est de faire en sorte que les sociétés ne s'engagent pas à la légère dans des relations d'affaires, notamment à l'international, avec des tiers dont elles ignorent tout et dont elles pourraient pâtir des pratiques illégales ou inappropriées d'un point de vue éthique.

L'Agence française anti-corruption, dans ses prochaines lignes directrices, ainsi que, le cas échéant, la publication de futurs décrets, apporteront très certainement des précisions, quant au contenu précis et à la portée attendue de ce volet de la loi. Cependant, il est intéressant que la pratique apporte, d'ores et déjà, des éclairages sur la rédaction et la mise en œuvre d'une telle procédure.

COMMENTAIRES

1. Définition et champ d'application

1.1. Définition d'une évaluation préalable

L'évaluation préalable (autrement appelée « due diligence ») peut être définie comme une opération de vérification d'un certain nombre d'éléments objectifs ayant trait notamment à l'intégrité de l'entreprise avec laquelle une société souhaite entrer en relation d'affaires sous quelque forme que ce soit.

1.2. Les personnes et les opérations concernées

1° Les personnes

La loi étant restée assez générale et large quant aux types de personnes devant faire l'objet de vérifications préalables, il appartient à la pra-

tique de les cerner plus précisément, et ensuite à chaque société de les identifier en fonction de ses activités.

Ainsi, l'on peut définir les tierces parties devant faire l'objet de vérifications comme l'ensemble des sociétés tierces appartenant à l'une des catégories suivantes :

- les fournisseurs ;
- les distributeurs ;
- les co-contractants et sous-traitants ;
- les agents, courtiers et autres intermédiaires commerciaux ;
- les associés au sein d'une co-entreprise ou d'un groupement d'intérêt économique ;
- les clients ;
- les conseils/consultants (avocats, experts-comptables, banques, etc.) et bailleurs de fonds ;
- les lobbyistes ; et,
- les autres prestataires de services.

À NOTER

Le stock des tierces parties existantes à la date d'entrée en vigueur de la procédure (et toujours actives, autrement dit auxquelles il est toujours recouru) devra faire l'objet des mêmes mesures de vérification que les tierces parties entrantes, avec un objectif d'apurement de 33 % chaque année pendant 3 ans (en ciblant les tierces parties les plus importantes en volume d'affaires et les plus risquées au vu de la cartographie des risques). Un tableau de tenue statistique du stock restant à écouler devra à cet égard être établi, et l'état d'avancement de la tâche contrôlé mensuellement par le responsable conformité.

2° Les opérations et transactions concernées

À l'égard de ces tierces parties, aucune précision n'est donnée par la loi ou tout décret concernant le type d'opérations pour lesquelles le recours à ces parties prenantes incombe de procéder à des vérifications préalables. Aussi peut-on, d'un point de vue théorique, considérer le type d'opérations visées comme étant le plus large possible, soit

notamment les opérations d'achat/vente de prestations de services et/ou de biens, les acquisitions et/ou cessions de sociétés, les développements, les partenariats et/ou prises de participation.

D'un point de vue pratique cependant, et pour des raisons de coûts financier et humain, la société devra hiérarchiser le type d'opérations pour lesquelles elle procédera à des vérifications, le principal critère de priorisation étant le montant annuel global engagé dans la transaction (avec des seuils à déterminer pour chaque société selon les types d'opérations), étant entendu que plusieurs petites opérations avec la même tierce partie devront être appréhendées sous un angle cumulatif.

REMARQUE

Pour les opérations d'envergure mettant en jeu un nombre important de tierces parties, la société se servira par ailleurs utilement de la notation qu'elle aura établie à l'égard de ses tierces parties afin de déterminer lesquelles feront l'objet de vérifications plus ou moins approfondies selon leur profil respectif de risque d'exposition à la corruption, tenant alors également compte du contexte global de l'opération et des interactions (notamment, en terme de conflits d'intérêts) des différentes tierces parties entre elles. Ce qui demande, en amont, une connaissance, une analyse et une bonne compréhension du dossier par les opérationnels en charge soutenus par le responsable conformité ou chargé d'éthique dédié.

2. Les différents types de vérifications

2.1. Due diligences préliminaires

Pour procéder aux vérifications standards communes obligatoires, la société pourra adresser à toute tierce partie, quel que soit son profil de risque - par ailleurs encore inconnu à ce stade - un questionnaire relatif à son intégrité visant, avant toute recherche complémentaire éventuelle, à mieux la connaître.

Ce questionnaire visera l'obtention d'informations relatives (i) à la société répondante (dénomination, date de création, effectif, filiales, etc.), (ii) à ses dirigeants, actionnaires et éventuels bénéficiaires ultimes, (iii) aux relations éventuelles de ladite société avec des entités et/ou agents publics et/ou personnes politiquement exposées, (iv) au programme de conformité et/ou anti-corruption d'ores et déjà, le cas échéant, mis en place par la société interrogée, et (v) aux condamnations (notamment pénales), sanctions (financières internationales ou pour violation d'embargos) et enquêtes dont la société ou l'un ou plusieurs de ses membres auraient fait l'objet.

2.2. Due diligences basiques

Si l'opérationnel en charge des vérifications en ressent le besoin, notamment en cas (i) d'absence totale de réponse au questionnaire préliminaire, (ii) de réponses trop floues, non pertinentes et/ou inexploitables, ou (iii) de réponses à la véracité douteuse, il pourra procéder à une *due diligence* complémentaire dite « basique », afin de compléter sa connaissance de la tierce partie et d'en affiner ainsi sa notation du profil de risque.

Il pourra ainsi vérifier, notamment mais non exclusivement, les informations suivantes :

- les nom de la société, pays d'immatriculation, date de création, capital social, effectif ;
- la composition des organes de direction (noms, antécédents des personnes (notamment pénaux)) et de l'actionnariat (incluant éventuellement le(s) bénéficiaire(s) ultime(s)) ; et,
- les derniers états financiers audités (comptes de résultats et bilans).

La vérification pourra être faite à l'aide de mots clefs associés au nom de la tierce partie et/ou de ses membres à insérer :

- sur internet, dans des moteurs de recherche (type Google) ;
- dans des bases de données *open source* (infogreffe, societe.com..) ;
- dans des bases de données payantes (telles que LexisNexis, Thomson Reuters, Dow Jones/Factiva, Bureau Van Dijk/Ellisphère, Altares Dun & Bradstreet, parmi lesquelles la société devra choisir en fonction de ses besoins) ;
- dans les listes de sanctions du GAFI, de l'OFAC, de l'Union européenne, des Nations-Unies ; et/ou,
- dans les comptes rendus de réunions et d'entretiens avec les commerciaux et autres représentants des tierces parties pressenties.

2.3. Due diligences approfondies de niveau 1 et 2

Si toutefois un risque éthique fort est identifié et/ou si l'enjeu de l'opération mérite, pour des raisons stratégiques et/ou commerciales et/ou financières que l'on s'y attarde, des *due diligences* complémentaires dites « approfondies » pourront être orchestrées.

Ainsi, des *due diligences* approfondies de niveau 1 peuvent être réalisées par des prestataires externes spécialisés, le plus souvent des agences dites d'« intelligence économique », telles que, à titre d'exemples, KROLL, ADIT, SGS, FTI (mais il peut également s'agir de cabinets d'avocats) qui émettent un rapport d'enquête, contenant globalement le même type d'informations que celles mentionnées précédemment, mais avec un degré de détail et d'analyse beaucoup plus important du fait d'une utilisation de sources beaucoup plus larges, fiables et actualisées.

Enfin, les *due diligences* approfondies de niveau 2 sont encore plus détaillées (donc sont plus onéreuses et s'obtiennent dans un délai plus long) et sont, le cas échéant, réalisées par l'envoi d'enquêteurs spécialisés sur place, lorsqu'il s'agit d'une tierce partie située à l'étranger dans un pays où l'opacité rend difficile la collecte traditionnelle d'informations.

3. Notation du caractère à risque des tierces parties

La loi Sapin 2 corèlle la procédure d'évaluation des tierces parties à la cartographie des risques, dont elle doit découler. Ainsi, les vérifications à opérer à l'égard des tierces parties doivent être directement liées au degré d'exposition au risque de corruption desdites tierces parties, qu'il est donc pertinent de noter.

Pour opérer cette notation (qui devra être actualisée), l'opérationnel pourra utiliser une grille comprenant des questions du type de celles figurant ci-dessous, auxquelles il pourra répondre grâce, notamment, au questionnaire préliminaire auquel il aura soumis les sociétés et aux *due diligences* complémentaires basiques qu'il aura lui-même, le cas échéant, réalisées :

N°	Indicateurs de risque	Oui = 1	Non = 0	Non applicable = 0
	La tierce partie opère-t-elle significativement ou principalement dans un (ou plusieurs) pays noté(s) à risque selon l'indice de corruption pays utilisé ?			
	La tierce partie opère-t-elle dans un (ou plusieurs) secteur(s) d'activité jugé(s) à risque ?			

N°	Indicateurs de risque	Oui = 1	Non = 0	Non applicable = 0
	La tierce partie (en tant que personne morale ou l'un de ses membres, personne physique) a-t-elle déjà fait l'objet d'une ou plusieurs condamnations (pénales et/ou civiles et/ou administratives) pour des faits de corruption ou assimilés ?			
	La tierce partie figure-t-elle sur une liste de sanctions ?			
	La tierce partie a-t-elle, à ce jour, mis en place un programme de conformité ou adopté un code de conduite anti-corruption ?			
	L'un (ou plusieurs) des membres des organes sociaux ou actionnaires principaux de la tierce partie est-il (ou sont-ils) affilié(s) à : (i) une personne politiquement exposée, (ii) un agent public (national ou international), ou (iii) une agence gouvernementale ou entité publique de toute nature ?			
	La tierce partie demande-t-elle à ce que le paiement de sa prestation soit opéré sur un compte situé en dehors de son pays d'immatriculation, et notamment dans un pays considéré comme un paradis fiscal ou au profit d'une fondation ?			
	TOTAL			

4. Le traitement à apporter aux données personnelles

À l'instar des interrogations soulevées par la mise en place des dispositifs d'alertes professionnelles (interne et externe) que la loi Sapin II oblige désormais les sociétés, même de seulement plus de 50 salariés, à mettre en place, des difficultés se posent et des incertitudes persistent en matière de traitement des données personnelles recueillies dans le cadre de la mise en œuvre des procédures d'évaluation des tierces parties.

En effet, dans la mesure où les vérifications préalables aboutissent au recueil de données personnelles sensibles, telles que notamment des informations relatives aux « *infractions, condamnations et mesures de sûreté* » dont les personnes physiques et/ou morales, sujets de la vérification, ont pu faire l'objet, toute société qui s'y astreint doit parallèlement s'interroger sur le traitement desdites données, dont elle n'a pas le droit de disposer librement. En effet, l'article 9 de la loi Informatique et Libertés n'autorise que certaines catégories spécifiques de personnes à mettre en œuvre le traitement de ces données. Elle doit donc y être autorisée, en rendre compte, informer les parties concernées de leur droit d'accès et de rectification, et conserver/détruire ces données et/ou les archiver conformément aux prescriptions légales du régulateur, la Commission Nationale Informatique et Liberté (CNIL).

Ainsi, concrètement, pour se mettre en conformité, une société, par l'intermédiaire de son CIL, ou directement, doit faire une « demande d'autorisation préalable à la mise en œuvre de traitements automatisés de données à caractère personnel » sur le site de la CNIL en rem-

plissant un formulaire en ligne par lequel elle indiquera, notamment (i) le service chargé de la mise en œuvre du traitement et son lieu d'implantation physique, (ii) la finalité poursuivie par le traitement (dont son fondement juridique et, le cas échéant, le nom du logiciel utilisé aux fins du recueil des données), (iii) si les données feront l'objet d'un transfert hors Union européenne, et (iv) les modalités mises en œuvre en vue du respect des droits, notamment d'accès et de rectification, des personnes fichées.

La CNIL dispose ensuite d'un délai de 2 mois pour instruire la demande, faute de quoi son absence de réponse est assimilable à un refus. Il est donc important pour la société d'être proactive dans le traitement de sa demande pour ne pas avoir à la renouveler.

À l'issue de son instruction, si la CNIL autorise la demanderesse, elle émet une délibération aux termes de laquelle elle se prononce au regard (i) de la finalité poursuivie par le traitement (le traitement doit répondre à un intérêt légitime tel qu'évalué par ses soins et être conforme à l'article 7 de la loi Informatique et Libertés), (ii) des données traitées (qui doivent être adéquates, pertinentes et non excessives au regard de la finalité poursuivie), (iii) des destinataires des données, (iv) de l'information et du droit d'accès accordé aux personnes concernées, et (v) des mesures prises aux fins de préserver la sécurité et la confidentialité des données.

5. Les étapes de la procédure

Même s'il n'existe pas une seule et unique méthodologie à respecter et que chaque société pourra adapter sa procédure à son organisation interne, ses ressources et ses besoins, la procédure de vérifications préalables pourrait être découpée en suivant les cinq étapes ci-dessous.

Étape 1. - L'opérationnel fait remplir le questionnaire préliminaire au représentant de la tierce partie et ensuite examine l'authenticité des pièces justificatives avant de les télécharger et stocker dans la base de référencement de ladite partie au moment de l'ouverture du compte y associé.

Étape 2. - L'opérationnel établit, grâce au questionnaire et, le cas échéant à une *due diligence* complémentaire basique, une notation du caractère à risque de la tierce partie et décide, selon le résultat, de procéder, soit à aucune vérification complémentaire, soit, en accord avec le responsable conformité, à une *due diligence* complémentaire approfondie de niveau 1 ou 2.

Étape 3. - L'opérationnel, en accord avec le responsable conformité, tire concrètement toutes les conséquences de ce qu'il a découvert au travers des différents types de *due diligences* qu'il a effectuées, soit en refusant l'entrée en relation avec une tierce partie présentant des garanties de conformité trop faibles, soit en imposant dans la relation des mesures de mitigation du risque de corruption (telles que l'insertion de clauses anti-corruption ou de conformité plus larges, assorties de droits de sortie avec pénalités).

Étape 4. - Le responsable conformité centralise, intégralement dans l'entreprise et/ou partiellement chez le prestataire fournissant le logiciel de base de données, les rapports de *due diligences* qui ont été réalisés (qui devront idéalement être actualisés annuellement), notamment pour pouvoir en faire la preuve auprès de toute autorité de régulation qui en ferait la demande. Les durées de conservation et d'archivage desdits rapports auront été déterminées en fonction de l'autorisation accordée par la CNIL.

Étape 5. - Le département d'audit devra établir et réaliser un (ou des) plan(s) annuel(s) de contrôle interne de l'effectivité du respect de la procédure.