Délibération n° 2024-191 du 9 octobre 2024

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« Filtrage et notation des fournisseurs »,

dénommé « KYS – Know Your Supplier ».

présenté par la Société Générale Private Banking (Monaco) SAM

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, susvisée ;

Vu l'Ordonnance Souveraine n° 2.318 du 3 août 2009, modifiée, fixant les conditions d'application de la Loi n° 1.362 du 3 août 2009, modifiée, susvisée ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés d'informations nominatives ;

Vu la demande d'autorisation déposée par Société Générale Private Banking (Monaco) SAM, le 28 juin 2024, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Filtrage et notation des fournisseurs* » ;

Vu la demande d'autorisation de transfert concomitamment déposée par Société Générale Private Banking (Monaco) SAM, le 24 juin 2024, ayant pour finalité « *Filtrage et notation des fournisseurs* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 26 août 2024, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 9 octobre 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Société Générale Private Banking (Monaco) SAM est une société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 96S03214 ayant pour activité « *dans les conditions déterminées par la législation et la règlementation applicables aux établissements de crédit, d'effectuer avec toutes personnes physiques ou morales, tant en Principauté de Monaco qu'à l'étranger : toutes opérations de banque à savoir : recevoir du public des fonds, notamment sous forme de dépôts, consentir des crédits sous des formes quelconques, prendre tous engagements par signature tels qu'aval, cautionnement ou garantie, mettre à disposition et gérer tous moyens de paiements, effectuer toutes opérations de crédit-bail et toutes opérations de location assorties d'une option d'achat* (…) ».

Le responsable de traitement souhaite analyser les documents et informations relatives au fournisseur/prestataire afin d'établir le risque avant l'entrée en relation avec celui-ci, ainsi que pendant toute la durée du contrat (lors de la revue périodique du fournisseur).

Il précise que cette analyse *« inclut la détermination d'une notation en vue d'établir [le profil de risque de chaque fournisseur/prestataire] et les diligences supplémentaires associées à chaque niveau de risque ».*

Le traitement objet de la présente demande porte sur des soupçons d'activités illicites, des infractions et des mesures de sûreté. Il est mis en œuvre à des fins de surveillance. Il relève donc du régime de l'autorisation préalable visé à l'article 11-1 de la Loi n° 1.165, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement soumis a pour finalité « *Filtrage et notation des fournisseurs* ».

Il est dénommé « KYS – *Know Your Supplier* ».

Il concerne les fournisseurs, les prestataires de service ainsi que les collaborateurs.

Le responsable de traitement précise que sont notamment concernés par le présent traitement les fournisseurs/prestataires lorsque la durée du contrat signé ou envisagé est supérieure à 5 ans, à tacite reconduction ou qu'aucune échéance n'est fixée. Sont également concernés les contrats qui dépassent un certain montant fixé par la Banque ainsi que lorsque des contrats sont envisagés avec des fournisseurs présentant des caractéristiques spécifiques (un mandat de représentation, un lien gouvernemental, ou s'il s'agit d'un fournisseur de prestations de services externalisées essentiels).

Le responsable de traitement précise que sont exclus du présent traitement *« les prestataires de services de paiement pour les besoins de transfert d'argent, les distributeurs de produits financiers (courtiers de bourse), les sous conservateurs, correspondants bancaires et les apporteurs d'affaires pour lesquels un dispositif spécifique »* existe et *« tout fournisseur interne au Groupe ».*

En ce qui concerne ce dispositif spécifique, la Commission rappelle que conformément à la Loi n° 1.165 tout traitement automatisé d'informations nominatives doit lui

être soumis selon la modalité adéquate. Ainsi, si ce dispositif est automatisé, elle rappelle que le traitement y afférent doit être soumis à formalité légale.

Enfin, la Commission rappelle s'agissant des collaborateurs de la Banque que ces derniers ne peuvent être concernés par le traitement que de manière incidente et ne doivent pas faire l'objet des mesures de vigilance mises en place dans le cadre du présent traitement.

Les fonctionnalités sont les suivantes :

- *« évaluation du risque fournisseur sur la base des éléments fournis :*
  - *vérification des listes d'exclusion et d'identification des fournisseurs ;*
  - *notation de la santé financière ;*
- *notation des fournisseurs :*
  - *neutralisation du risque pays local ;*
  - *prise en compte des informations négatives ;*
- *maintenance et gestion du registre des fournisseurs et des contrats ;*
- *plan de revue annuel et exceptionnel ;*
- *contrôle annuel des paiements ;*
- *key Risk Indicator (KRI) ;*
- *conservation des documents relatifs à l'évaluation du fournisseur ».*

Le responsable de traitement indique qu'il procède à l'analyse des informations et documents communiqués par le fournisseur/prestataire. Il précise par ailleurs que des listes internes au Groupe sont également consultées ainsi *que « divers outils publics afin de compléter les informations fournisseur et de pouvoir effectuer l'évaluation du risque fournisseur »*.

A l'aide des résultats de cette analyse la Banque procède au calcul du niveau de risque global du fournisseur en tenant compte de différents critères (risque pays, date de création de l'entreprise, etc.). Le responsable a identifié 4 niveaux de risque allant du risque considéré faible au risque considéré élevé.

En outre, le responsable de traitement indique qu'*« une revue mensuelle des contrats actifs est effectuée afin de vérifier les statuts des contrats pour lesquels une échéance serait arrivée »*. Il précise qu'un fichier Excel est maintenu afin d'effectuer le suivi des fournisseurs à Monaco. Il est indiqué que *« l'accès au dossier et restreint aux personnes habilitées à Monaco »*. La Commission en prend acte et rappelle que le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993.

Sous les réserves évoquées au présent point, la Commission considère que la finalité du traitement est explicite et légitime, conformément à l'article 10-1 de la Loi n° 1.165, modifiée.

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le traitement est justifié par le respect d'une obligation légale à laquelle il est soumis ainsi que par un intérêt légitime qu'il poursuit sans méconnaître ni l'intérêt, ni les droits fondamentaux de la personne concernée.

A cet égard, il expose que la SGPB étant une filiale d'une banque française, elle se doit de respecter des dispositions issues de textes nationaux et internationaux.

Il précise que les principaux textes à respecter sont :

- la Loi française n° 2016-1691 du 9 décembre 2016 (Sapin 2) ;
- la Loi française n° 2017-399 de 27 mars 2017 sur le devoir de vigilance ;
- le UK Bribery Act de 2010 ;
- le US Foreign Corrupt Practices Act de 1977 (FCPA) ;
- le UK Modern Slavery Act de 2015.

Le responsable de traitement indique en outre que *« Sur la base de l'engagement du Groupe SG vis-à-vis du Département de Justice Américain (DoJ) de 2018 (lutte contre la corruption et le trafic d'influence (US Foreign Corrupt Practices Act -FCPA)) et du Parquet National Financier (Article 131-39-2 du Code Pénal), le dispositif Know Your Supplier (KYS) regroupe un ensemble de règles qui doivent permettre de connaître le fournisseur en vue d'évaluer son profil de risque et d'être en mesure de prendre une décision quant à l'entrée en relation commerciale ou au maintien d'une relation commerciale existante ».*

La Commission relève toutefois que la Loi n° 1.362 du 3 août 2009, modifiée prévoit la soumission à son dispositif des clients et dans certains cas de leurs familles, ainsi qu'une certaine catégorie de collaborateurs au moment de l'embauche, mais qu'*a contrario*, aucune de ses dispositions n'impose la mise en place de mesures de vigilance à l'égard des fournisseurs et des prestataires.

Dès lors, elle demande donc que seules les personnes morales soient concernées par la mise en place des mesures de vigilances issues du présent traitement. Elle considère toutefois que des personnes physiques dont les informations sont publiques et liées à la structure vérifiée peuvent indirectement être concernées par le présent traitement, lorsqu'elles ressortent des recherches effectuées, tels que les représentants des personnes morales. La Commission estime que le présent traitement ne peut permettre de soumettre à vérification l'ensemble des personnels des entités vérifiées qui entrent en interaction avec la Banque.

Elle estime cette procédure proportionnée aux textes de la Principauté et de nature à répondre à la nécessité de disposer d'outils de conformité destinés à prévenir le blanchiment de capitaux.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité : nom et prénom du représentant légal du fournisseur, dénomination sociale, bénéficiaires effectifs, personne politiquement exposée (titre (monsieur/madame), nom, prénom, date de naissance) ;
- coordonnées : adresse de domiciliation/siège social, adresse principale d'activité, pays (siège/fournisseur), fax, personne politiquement exposée (adresse, numéro de téléphone, (fixe/mobile)) ;
- vie professionnelle : personne politiquement exposée : rôle dans l'organisation ;
- caractéristiques financières : secteur d'activité, forme juridique, numéro d'enregistrement, date d'enregistrement, autorité d'enregistrement, montant et date du contrat, date de signature du contrat, date d'échéance du contrat, personne politiquement exposée (fournisseur coté/ régulé) ;
- consommation de biens et services, habitudes de vie : nature des services fournis ;
- données d'identification électronique : email, identifiant des personnes habilitées ;
- informations temporelles : date, heure, action, identifiant connexion, adresse IP, log technique ;

- mesure d'éthique : mesure mise en place par le fournisseur *via* la documentation ou URL (code de conduite, anti-corruption, LCB, RSE, etc.), informations négatives (negative news) ;
- informations faisant apparaître des appartenances politiques : statut de personne politiquement exposée ou hauts fonctionnaires (Senior Public Officials).

Il appert à la lecture du dossier que sont également traitées les données d'identification électronique des collaborateurs ayant accès à l'outil.

Enfin, à l'instar du dossier ayant pour finalité *« Appliquer les mesures de gel des fonds dans le cadre de la lutte contre le financement du terrorisme et des sanctions économiques »*, la Commission rappelle que le recours à des outils publics et notamment aux negative news doit faire l'objet d'un workflow spécifique afin de s'assurer du caractère fiable de la source.

Les informations objet du présent traitement proviennent de la personne concernée (fournisseur ou prestataire de service) à l'exception des informations temporelles qui ont pour origine le système.

La Commission considère que les informations collectées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165, modifiée.

IV. Sur les droits des personnes concernées

- ***Sur l'information préalable des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est assurée au moyen d'une rubrique propre à la protection des données accessible en ligne.

La Commission n'ayant pas été destinataire de ladite mention, elle n'est pas en mesure de se prononcer sur la qualité de l'information dispensée.

Par ailleurs, le responsable de traitement précise que *« les fournisseurs savent qu'une évaluation du risque est effectuée du fait des demandes de documents pour l'entrée en relation et constituer le compte fournisseur en comptabilité »*.

A cet égard, la Commission considère que l'information doit être adaptée au type de relation envisagée notamment pour qu'elle puisse être préalable et rappelle que la mention d'information doit être conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

- ***Sur l'exercice du droit d'accès, de modification et de mise à jour***

Les droits d'accès, de modification, de mise à jour et de suppression s'exercent par voie postale, par courrier électronique envoyé au Service conformité ainsi que sur place.

La Commission rappelle toutefois que l'article 25 alinéa 2 de la Loi n° 1.362 du 3 août 2009, telle que modifiée par la Loi n° 1.549 du 6 juillet 2023, dispose que *« Lorsque des informations nominatives font l'objet d'un traitement aux seules fins de l'application des obligations de vigilance et de l'obligation de déclaration et d'information auprès, selon les cas, du service exerçant la fonction de renseignement financier de l'Autorité ou du Conseil de l'Ordre des avocats-défenseurs et avocats, le droit d'accès s'exerce auprès de la*

Commission de Contrôle des Informations Nominatives, dans les conditions prévues à l'article 15-1 de la loi n° 1.165 du 23 décembre 1993, modifiée.».

A cet égard, le responsable de traitement doit, lorsqu'il s'agit d'informations concernées par ledit article, les soumettre au droit d'accès indirect et la Commission rappelle, le cas échéant, que les personnes concernées doivent être valablement informées qu'elles disposent d'un droit d'accès indirect s'exerçant auprès de la Commission de Contrôle des Informations Nominatives, dans les conditions prévues à l'article 15-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

V. Sur les personnes ayant accès au traitement

Le responsable de traitement indique qu'ont accès au traitement :

- toutes personnes internes au Groupe SG et habilitées ayant accès à l'outil : en consultation ;
- tous collaborateurs de Monaco habilités avec un accès à l'outil : en consultation, modification, suppression ;
- KYS Analyste en Inde : en consultation, modification ;
- KYS Team Leader : en consultation ;
- administrateurs : les administrateurs Groupe habilités disposent d'un accès au système et aux informations dans le cadre de leurs travaux de maintenance de l'outil.

Il est précisé que « *Les données pourront être accessibles à l'équipe de support opérationnel basée en Inde* ».

Par ailleurs, il appert à la lecture du dossier que l'équipe KYS située en Inde, effectue l'analyse de risque pour tout nouveau fournisseur ainsi que pour les revues. Elle réalise également les demandes d'information complémentaires auprès des équipes internes de SG Monaco, les complète et les documente dans l'outil.

L'Inde ne disposant pas d'un niveau de protection adéquat au sens de la Loi n° 1.165 du 23 décembre 1993, la licéité de ces communications d'informations nominatives sera analysée dans la demande d'autorisation de transfert de données concomitamment soumise à la Commission.

La Commission rappelle par ailleurs qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, la liste nominative des personnes ayant accès au traitement doit être tenue à jour et précise que cette liste doit lui être communiquée à première réquisition.

Sous ces réserves, la Commission considère que ces accès sont justifiés.

VI. Sur les rapprochements et les interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement est interconnecté avec les traitements légalement mis en œuvre ayant pour finalités respectives :

- « *Gestion des fichiers de fournisseurs* » ;
- « *Gestion et traçabilité des habilitations informatiques* » ;
- « *L'accès de Société Générale Global Solution Center Pvt. Ltd. (SGGSC) sise en Inde à des fins de maintenance et de support des éléments d'infrastructure* ».

A l'analyse du dossier il appert que le traitement est également rapproché avec les traitements, légalement mis en œuvre suivants :

- *« Gestion de la messagerie professionnelle » ;*
- *« Appliquer les mesures de gel des fonds dans le cadre de la lutte contre le financement du terrorisme et des sanctions économiques »*.

La Commission considère que ces interconnexions et ces rapprochements sont conformes aux exigences légales.

VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation particulière.

Cependant, les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

En outre, la Commission rappelle que la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

Elle rappelle par ailleurs que les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.

La Commission rappelle enfin que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

VIII. Sur la durée de conservation

Le responsable de traitement indique que l'ensemble des informations objet du présent traitement sont conservées « *5 ans après la fin de la relation* » à l'exception des informations temporelles qui sont conservées *« 6 mois après départ du collaborateur ».*

A l'égard de cette dernière durée de conservation, la Commission rappelle que les logs de connexion doivent être conservés pendant une durée comprise entre 3 mois minimum et 1 an maximum. Elle fixe par conséquent la durée de conservation de ces informations à 1 an.

Enfin, la Commission relève qu'aucune durée de conservation n'est prévue pour les données d'identification électronique des collaborateurs. Elle considère que ces informations sont susceptibles d'être conservées tant que la personne est habilitée à avoir accès à l'outil. Elle fixe en conséquence la durée de conservation.

Après en avoir délibéré,

Considère que :

- l'information doit être adaptée au type de relation envisagée notamment pour qu'elle puisse être préalable ;

- des personnes physiques dont les informations sont publiques et liées à la structure vérifiée peuvent indirectement être concernées par le présent traitement, lorsqu'elles ressortent des recherches effectuées, tels que les représentants des personnes morales.

Estime que le présent traitement ne peut permettre de soumettre à vérification l'ensemble des personnels des entités vérifiées qui entrent en interaction avec la Banque.

Rappelle que :

- si le dispositif spécifique mis en place par la Banque, pour les prestataires de paiement pour les besoins de transfert d'argent, les distributeurs de produits financiers (courtiers de bourse), les sous conservateurs, correspondants bancaires et les apporteurs d'affaires est automatisé, le traitement y afférent doit être soumis à formalité légale ;

- le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993 ;

- les collaborateurs de la Banque ne peuvent être concernés par le traitement que de manière incidente et ne doivent pas faire l'objet des mesures de vigilance mises en place dans le cadre du présent traitement ;

- les documents d'information préalable des personnes concernées doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- les personnes concernées doivent être valablement informées qu'elles disposent d'un droit d'accès indirect s'exerçant auprès de la Commission de Contrôle des Informations Nominatives, dans les conditions prévues à l'article 15-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, pour les informations qui y sont soumises ;

- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit lui être communiquée à première réquisition ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé. ;

- la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception ;

- les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.

Demande que les personnes concernées par les mesures de vigilances soient limitées conformément au point II de la présente délibération.

Fixe la durée de conservation des :

- données d'identification électronique des collaborateurs à la période pendant laquelle la personne est habilitée à avoir accès à l'outil ;

- logs de connexion à l'outil à 1 an.

A la condition de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par la Société Générale Private Banking (Monaco) SAM du traitement automatisé d'informations nominatives ayant pour finalité « *Filtrage et notation des fournisseurs* ».**

Le Président

Robert CHANAS