DELIBERATION N° 2016-17 DU 24 FEVRIER 2016 DE LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES PORTANT AUTORISATION A LA MISE EN ŒUVRE DU TRAITEMENT AUTOMATISE D'INFORMATIONS NOMINATIVES AYANT POUR FINALITE « *GESTION DES OBLIGATIONS ISSUES DE LA REGLEMENTATION FOREIGN ACCOUNT TAX COMPLIANCE ACT (FATCA)* », PRESENTE PAR LA SOCIETE GENERALE PRIVATE BANKING (MONACO)

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 du 28 janvier 1981, et son protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, 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 n° 2.693 du 23 mars 2010 relative à la coopération internationale en matière fiscale ;

Vu l'Ordonnance Souveraine n° 2.692 du 23 mars 2010 rendant exécutoire l'Accord entre le Gouvernement de la Principauté de Monaco et le Gouvernement des États-Unis d'Amérique en vue de l'échange de renseignements en matière fiscale, signé à Washington le 8 septembre 2009 ;

Vu la délibération n° 2013-116 de la Commission de Contrôle des Informations Nominatives du 16 septembre 2013 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *la gestion des obligations issues de la règlementation dite « FATCA »* » ;

Vu les obligations mises à la charge des établissements financiers américains et non américains par la règlementation dite « *FATCA* » et issue du Foreign Account Tax Compliance Act du 18 mars 2010 ;

Vu la demande d'autorisation déposée par la Société Générale Private Banking (Monaco), le 15 décembre 2015, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Gestion des obligations issues de la réglementation Foreign Account Tax Compliance Act (FATCA)* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 12 février 2016, conformément à l'article 11-1 de la Loi n° 1.165, susmentionnée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 24 février 2016 portant examen du traitement automatisé susvisé ;

La Commission de Contrôle des Informations Nominatives,

Préambule

La Société Générale Private Banking (Monaco) est une société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 96S03214, ayant pour activité « *d'effectuer (…) tant en Principauté de Monaco qu'à l'étranger : Toutes opérations de banque (…)* ».

Eu égard à son activité, elle estime qu'il lui est nécessaire de se conformer à la règlementation américaine dite « *FATCA* ».

A ce titre, elle s'est enregistrée auprès de l'autorité fiscale américaine (Internal Revenu Service (IRS)) en qualité d' « *institution financière étrangère participante (PFFI)* ». Aussi, elle est tenue de déterminer au sein de sa clientèle les « *personnes américaines* » et d'effectuer un reporting sur les personnes et opérations visées par ladite règlementation auprès de l'IRS.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance. Il est donc soumis au régime de l'autorisation de l'article 11-1 de la Loi n° 1.165, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Gestion des obligations issues de la réglementation Foreign Account Tax Compliance Act (FATCA)* ».

Le responsable de traitement indique que les catégories de personnes concernées sont les « *clients, mandataires, dirigeants, bénéficiaires effectifs, personnes morales et entités* ».

Aussi, à la lecture des informations collectées, la Commission considère que le « *responsable de la relation (CRM – client relationship manager*) » est également une personne concernée en ce qu'elle est visée dans la catégorie « *informations relatives à la relation entre le client et la banque* ».

A cet égard, elle relève que seul est renseigné le « *code CRM* » qui est « *composé des 7 premières lettres du nom et d'un chiffre ou du nom entier suivi des premières lettres du prénom puis d'un chiffre en cas de nom dont le nombre de lettres est inférieur à 7* ».

Le responsable de traitement précise également « *qu'aucune information relative au CRM n'est remontée dans le reporting* ».

Les fonctionnalités sont les suivantes :

- « *répondre aux obligations de l'accord FATCA ;*

- *effectuer un monitoring des comptes et des opérations de la clientèle ;*
- *identifier les comptes avec indice(s) FATCA et les documenter en conséquence ;*
- *communiquer, le cas échéant, les informations à la société-mère ;*
- *calculer et effectuer les retenues sur opérations soumises à ladite règlementation ;*
- *fermer les comptes des clients dits « récalcitrants » dans un délai raisonnable ;*
- *accomplir les formalités y afférentes auprès de l'Internal Revenue Service (IRS) (rapports périodiques …)* ».

A cet égard, la Commission constate que les fonctionnalités du traitement sont conformes au point V de sa délibération n° 2013-116 du 16 septembre 2013 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *la gestion des obligations issues de la règlementation dite « FATCA ».*

Cependant, elle rappelle, après avoir relevé que le présent traitement effectue des opérations de monitoring notamment sur la détermination d'indices d'américanité, qu'il ne doit pas méconnaitre les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

Aussi, elle considère que la finalité du traitement est « *déterminée, explicite et légitime* », conformément à l'article 10-1 de la Loi n° 1.165, modifiée.

II. Sur la licéité

Eu égard à l'objet social du responsable de traitement, et aux obligations qui lui incombent, la Commission constate que le traitement est licite, conformément aux éléments développés au point III de sa délibération n° 2013-116 du 16 septembre 2013, précitée.

III. Sur la justification du traitement

Le responsable de traitement indique que le traitement est justifié par le consentement des personnes concernées et la réalisation d'un intérêt légitime qui ne méconnaît ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

A cet égard, la Commission observe, conformément au point IV – Justification du traitement - de la délibération n° 2013-116, précitée, « *qu'un traitement ayant pour finalité « la gestion des obligations issues de la règlementation dite « FATCA » » peut être justifié [pour la première phase du traitement qui tend à identifier les « comptes américains » au moyen des indices d'américanité] par un intérêt légitime du responsable de traitement ou de son représentant, tel que :*

- *« le respect de standards internationaux ;*
- *la préservation des intérêts économiques, commerciaux ou financiers du responsable de traitement ou de son représentant ;*
- *la préservation des intérêts de la clientèle du responsable de traitement ou de son représentant* ».

Aussi, la Commission observe que cette justification est conforme au point IV de sa délibération n° 2013-116 susvisée.

Par ailleurs, le responsable de traitement indique que :

- « *préalablement à l'entrée en vigueur de la règlementation FATCA, un courrier d'information a été adressé à l'ensemble de la clientèle de la Banque afin de l'avertir de l'entrée en vigueur et des conséquences sur les relations contractuelles entre le Client et la Banque [nouvelles obligations en matière de connaissance du Client, nouvelles obligations déclaratives pour la Banque] ;*
- une copie de nouvelles conditions générales en vigueur au 01/07/2014 a également été envoyée à chaque Client préexistant ;
- pour les nouveaux Clients, les conditions générales en vigueur à l'entrée en relation s'appliquent [et à ce titre le Client s'engage : à fournir tous les éléments nécessaires à la Banque pour la bonne qualification du Client vis-à-vis de la règlementation FATCA, à avertir la Banque de tout changement de circonstance susceptible de modifier son statut au regard de FATCA, à fournir les autorisation nécessaires au traitement et à la transmission des informations récoltées par la Banque en cas de besoin (reporting à l'IRS, échange d'informations entre entités du Groupe SG etc.)] ».

Il précise également que « *le consentement libre et éclairé de la personne concernée porte sur le traitement de leurs informations nominatives afin de déterminer si elles sont qualifiables de « personnes américaines », la fourniture de documentation aux fins d'apporter le cas échéant la preuve contraire, le fait de permettre à la Société Générale Private Banking de communiquer ces informations à l'autorité fiscale américaine et la possibilité donnée au client de mesurer les conséquences tant de son consentement que de son refus* ».

Aussi, s'agissant du consentement, la Commission effectuera son analyse dans le cadre de la demande d'autorisation de transfert à l'autorité fiscale américaine (IRS), concomitamment soumise.

Au vu de ce qui précède, la Commission considère que le traitement est justifié, conformément à l'article 10-2 de la Loi n° 1.165, modifiée.

IV. Sur les informations nominatives traitées

Les informations nominatives traitées sont :

- identité : *Racine (compte) PP/PM [personne physique/personne morale]* : numéro de compte, nom long ou raison sociale, liste et fonction des intervenants, documents d'identité (type et date de validité), documentation FATCA, résidence fiscale QI, type juridique, nationalité, résidence géographique, résidence fiscale ;
Racine (compte) PP : numéro d'identifiant fiscal (TIN number) ;
Racine (compte) PM : type de société, forme juridique, secteur d'activité, numéro d'inscription RCS, numéro d'agrément QI, code NACE, date et lieu d'immatriculation (pays), numéro GIIN, numéro d'identifiant fiscal (TIN number) ;
Intervenants titulaires/mandataires/ dirigeants : titre (M/Mme/Melle), nom, nom de jeune fille, prénom, date de naissance, nationalité, résidence géographique, résidence fiscale QI, résidence fiscale, numéro d'identité fiscale, liste des documents permettant d'identifier la personne (type et date de validité), documentation FATCA signée, numéro interne d'identification (numéro unique), liste des rôles tenus sur d'autres racines (comptes) actifs ou inactifs ;
Intervenant BEE [bénéficiaire économique effectif] : nom, nom de jeune fille, pays de naissance, nationalité, résidence géographique, résidence fiscale QI, résidence fiscale, statut FATCA, liste des documents permettant d'identifier la personne (type et date de validité), documentation FATCA signée, numéro interne d'identification (numéro unique), liste des rôles BEE tenus sur d'autres racines (comptes) actifs ou inactifs.

- situation de famille : *Intervenants titulaires/mandataires/dirigeants* : Etat civil (célibataire, marié, divorcé, veuf).
- adresses et coordonnées : *Racine (compte) PP/PM :* liste des adresses principales et secondaires, usage des adresses pour le courrier (courrier guichet ou courrier expédié), coordonnées téléphonie fixe et mobile/fax/email personnelles et professionnelles, site web ;
- *Intervenants titulaires/mandataires/dirigeants* : adresse personnelle de l'intervenant (si fournie).
- formation-diplômes-vie professionnelle :
  Intervenants titulaires/mandataires/dirigeants : activités professionnelles, retraité (oui/non), profession, employeur, secteur d'activité, fonction, lieu d'activité ;
  Intervenant BEE : secteur d'activité, lieu d'activité.
- caractéristiques financières : montant des revenus, bénéfices, assujettissement à la TVA, devise de référence du compte.
- indices d'américanité : citoyenneté US, lieu de naissance aux USA, adresse d'expédition du courrier ou de résidence aux USA, numéro(s) de téléphone aux USA associé au compte, instruction de transfert domicilié aux USA, pouvoir concédé à un mandataire ayant une adresse de résidence aux USA, statut FATCA.
- informations relatives à la relation entre le client et la banque : date d'ouverture du compte, liste des comptes sur lesquels le client intervient, responsable de la relation (CRM, client relationship manager), type de gestion, restriction sur le fonctionnement du compte (blocage opérationnel pour suivi, compte dormant, interdiction de souscriptions de valeurs américaines etc.), documentation juridique signée.

Les informations appartenant aux catégories « *situation de famille* », « *adresses et coordonnées* » et « *formation-diplômes-vie professionnelle* » ont pour origine exclusive le traitement ayant pour finalité « *Gestion de l'identification et de la vérification des personnes soumises à la loi relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption* », dénommé « *PFO 2* », légalement mis en œuvre. Celles relatives à « *l'identité* » et aux « *indices d'américanité* » proviennent du traitement dénommé « PFO 2 », précité, et de la personne concernée ou son représentant. Les « *caractéristiques financières* » sont issues des traitements ayant pour finalité respective « *Connaissance de la clientèle afin de gérer la relation commerciale* », dénommé « *PFO 1* » et « *Tenue des comptes de la clientèle et les traitements des informations s'y rattachant par les établissements bancaires et assimilés* ». Enfin, les « *informations relatives à la relation entre le client et la banque* » ont pour origine les traitements dénommé « *PFO 1* » et « *PFO 2* », précités.

Par ailleurs, la Commission relève que s'agissant du « *responsable de la relation (CRM – client relationship manager)* » seul est renseigné le « *code CRM* » qui est « *composé des 7 premières du nom et d'un chiffre ou du nom entier suivi des premières lettres du prénom puis d'un chiffre en cas de nom dont le nombre de lettres est inférieur à 7*».

A la lecture des informations exploitées, la Commission estime qu'elles sont nécessaires aux fins de vérifier les éventuels indices d'américanité des personnes concernées tels que définis au II de la délibération n° 2013-116, précitée.

En conséquence, elle 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.

V. 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 mention sur le document de collecte et une mention ou clause particulière intégrée dans un document remis à l'intéressé.

A la lecture de la documentation jointe, la Commission considère que les personnes concernées ne sont pas clairement informées, conformément à l'article 14 de la Loi n° 1.165, modifiée, de la finalité exacte et des catégories de destinataires du traitement dont s'agit.

Enfin, et observant que ladite documentation concerne les clients de la banque, elle rappelle que ladite information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit.

Elle demande donc que soit assurée l'information préalable de l'ensemble des personnes concernées conformément à l'article 14 de la Loi n° 1.165, modifiée.

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

Le responsable de traitement indique que le droit d'accès est exercé par la voie postale auprès du Responsable Déontologie et Compliance. Le délai de réponse est de 30 jours. Les droits de modification, mise à jour ou suppression des données, sont exercés suivant les mêmes modalités.

La Commission constate que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 la Loi n° 1.165, modifiée.

VI. Sur les personnes ayant accès au traitement et les communications d'informations

- ***Sur les accès au traitement***

Le responsable de traitement indique que :

- concernant les informations liées à l'identification clients et à l'indice d'américanité seul le personnel habilité du Service Fichier Central a accès aux informations en inscription, modification, mise à jour et consultation dans le cadre des fonctions qui leur sont reconnues ;
- le personnel habilité du Service Déontologie-Compliance et les CRM (Customer Relationship Managers) ont accès aux informations en consultation uniquement ;
- concernant le module reporting (FITAX), seuls les utilisateurs du service fiscalité et la DSI ont accès aux informations en inscription, modification, mise à jour et consultation.

Il précise qu' « *une liste des personnes habilitées à avoir accès aux informations est tenue à jour* ».

Par ailleurs, la Commission constate que « *l'outil choisi pour réaliser le reporting FATCA des clients de SGPB Monaco est l'application FITAX. Comme PFO, cette application est hébergée au Luxembourg [par] SGBT [Société Générale Bank & Trust] Luxembourg* ».

Elle en déduit que la Société Générale Bank & Trust (Luxemburg) dispose également d'un accès au traitement et aux informations.

A cet égard, elle rappelle, conformément au point VIII de sa délibération n° 2013-116 du 16 septembre 2013, que « *l'accès aux informations objets du traitement doit être limité aux seules personnes qui, dans le cadre de leurs attributions, peuvent légitimement en avoir connaissance au regard de la finalité du traitement ou du but recherché* ».

Aussi, elle considère que ces accès sont justifiés.

- ***Sur les communications d'informations***

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées à la Direction de la conformité à Paris, aux Autorités judiciaires et administratives locales (Monaco) dans le cadre des missions qui leur sont légalement conférées et à l'Internal Revenue Service (IRS) aux Etats-Unis d'Amérique.

La Commission rappelle que lors d'une réunion plénière du 15 avril 2015, elle a déterminé une position de principe aux termes de laquelle les transferts d'informations nominatives vers un Pays ou un organisme n'assurant pas un niveau de protection adéquat doivent, en toutes hypothèses, lui être soumis en la forme d'une demande d'autorisation de transfert, indépendamment du fait qu'ils relèvent de l'alinéa 1er ou 2ème de l'article 20-1 de la Loi n° 1.165, modifiée.

Aussi, la licéité des communications d'informations nominatives à l'Autorité Fiscale Américaine (IRS) sera analysée dans la demande d'autorisation de transfert concomitamment soumise.

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

Le responsable de traitement indique que le traitement dont s'agit fait l'objet d'interconnexions avec les traitements ayant pour finalité respective « *Connaissance de la clientèle afin de gérer la relation commerciale », dénommé « PFO 1 »*, « *Gestion de l'identification et de la vérification des personnes soumises à la loi relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption* », dénommé « *PFO 2* », et « *Tenue des comptes de la clientèle et les traitements des informations s'y rattachant par les établissements bancaires et assimilés* », légalement mis en œuvre.

Par ailleurs, il dispose qu'il est également interconnecté avec un traitement ayant pour finalité la gestion des accès et des habilitations, « *non encore déposé auprès de la CCIN* ».

En conséquence, la Commission demande que le traitement ayant pour finalité la gestion des accès et des habilitations lui soit soumis dans les plus brefs délais.

VIII. 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'observations.

La Commission relève cependant que l'architecture technique repose sur des équipements de raccordements (switchs, pare-feux) de serveurs et périphériques qui doivent être protégés par un login et un mot de passe réputé fort et les ports non utilisés doivent être désactivés.

Elle rappelle de plus que, conformément à l'article 17 de la Loi n° 1.165, modifiée, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement 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.

IX. Sur la durée de conservation

Le responsable de traitement indique que les informations sont conservées pour « *les personnes concernées dont les comptes ont été identifiés : jusqu'à la fin de la sixième année civile suivant celle ayant donné lieu aux obligations déclaratives* ».

A cet égard, la Commission rappelle que, suivant le point X de sa délibération n° 2013-116 du 16 septembre 2013, précitée, elle considère que :

- la liste des personnes concernées dont les comptes ont été identifiés et la documentation y afférente sont conservées jusqu'à la fin de la sixième année civile suivant celle ayant donné lieu aux obligations déclaratives ;
- la liste des personnes non concernées par la règlementation dite « *FATCA* », à l'issue des opérations de monitoring, ne pourra être conservée chaque année, que pour la durée nécessaire aux fins d'effectuer les diligences issues de la règlementation dite « *FATCA* » et sans jamais excéder la période d'établissement des déclarations prescrites par l'accord signé avec l'autorité fiscale, de sorte à ce que les établissements ne conservent ni ne transmettent aucune « *liste négative* » des personnes non assujetties à l'impôt américain ;
- la durée de conservation des informations pourra être étendue dans les conditions de l'article 9 de la loi n° 1.165 du 23 décembre 1993, modifiée.

Aussi la Commission considère que la durée de conservation des informations est conforme aux exigences légales.

Après en avoir délibéré, la Commission :

Considère que le « *responsable de la relation (CRM – client relationship manager)* » est également une catégorie de personnes concernées par le présent traitement.

Rappelle que :

- le présent traitement, en ce qu'il effectue des opérations de monitoring notamment sur la détermination d'indices d'américanité, ne doit pas méconnaitre les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée ;

- les serveurs et périphériques doivent être protégés par un login et un mot de passe réputé fort et les ports non utilisés doivent être désactivés.

Demande que :

- demande donc que soit assurée l'information préalable de l'ensemble des personnes concernées conformément à l'article 14 de la Loi n° 1.165, modifiée ;

- le traitement ayant pour finalité la gestion des accès et des habilitations lui soit soumis dans les plus brefs délais.

A la condition de la prise en compte des éléments qui précèdent,

La Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre, par la Société Générale Private Banking (Monaco), du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des obligations issues de la réglementation Foreign Account Tax Compliance Act (FATCA)* ».**

Le Président

Guy MAGNAN