Délibération n° 2017-219 du 20 décembre 2017

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

« *Gestion, stockage et supervision de la messagerie électronique de l'entreprise* »

présentée par Citi Global Wealth Management S.A.M.

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 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° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;

Vu la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, 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 ;

Vu l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée, susvisée ;

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, modifiée, susvisée ;

Vu l'Arrêté Ministériel n° 2012.199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers ;

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 ou non automatisés d'informations nominatives ;

Vu la délibération n° 2015-111 du 18 novembre 2015 de la Commission de Contrôle des Informations Nominatives du 16 juillet 2012 portant recommandation sur les traitements automatisés

d'informations nominatives ayant pour finalité « *Gestion de la messagerie électronique utilisée à des fins de surveillance ou de contrôle* » ;

Vu la demande d'autorisation déposée par Citi Global Wealth Management S.A.M. le 11 octobre 2017 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion, stockage et supervision de la messagerie électronique de l'entreprise*» ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 7 décembre 2017, 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 20 décembre 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Société Citi Global Wealth Management S.A.M. est une entité figurant dans le périmètre du Groupe américain Citigroup Inc., immatriculée au répertoire du Commerce et de l'Industrie sous le numéro 08S04740, qui a pour objet social « *la réception et la transmission d'ordres sur les marchés financiers portant sur des valeurs mobilières ou des instruments financiers à terme, pour le compte de tiers* ».

Dans le cadre de l'exercice de leurs fonctions, les collaborateurs de cette société disposent d'une messagerie professionnelle faisant l'objet d'une supervision.

Le traitement objet de la présente demande 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 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Ce traitement a pour finalité « *Gestion, stockage et supervision de la messagerie électronique de l'entreprise ».*

Les personnes concernées sont « *L'ensemble des expéditeurs et destinataires des communications électroniques* ».

Enfin, le responsable de traitement indique que les fonctionnalités sont les suivantes :

- échanges de messages électroniques en interne et avec l'extérieur ;
- échanges de messages électroniques instantanés en interne (contrôlés par un modérateur) ;
- historisation des messages électroniques entrants et sortants ;
- gestion des contacts de la messagerie électronique ;
- gestion des dossiers de la messagerie et des messages archivés ;
- établissement et lecture de fichiers journaux ;
- gestion des habilitations d'accès à la messagerie ;
- stockage des données sur le serveur ;
- contrôle ayant pour but la détection des crimes et délits visés aux articles 218-1 et 218-2 du Code pénal ;
- contrôle ayant pour but la détection de fuites d'informations confidentielles ;
- contrôle ayant pour but la détection de tout message pouvant contenir des informations relatives à d'éventuels délits d'initiés et abus de marché ;

- établissement de preuves d'éventuels faits de divulgation d'informations confidentielles, de délit d'initié ou d'abus de marché aux fins de procédures de sanction ;
- interconnexion avec l'agenda.

La Commission constate ainsi que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

➢ *Sur la licéité*

Dans le cadre de sa recommandation n° 2015-111 du 18 novembre 2015, la Commission rappelle les conditions de licéité d'un traitement de messagerie professionnelle, au sens de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

Elle relève notamment que les articles 6 à 11 de l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 prévoient notamment que toute société agréée doit « *disposer d'une organisation administrative et comptable, ainsi que des mécanismes de sécurité et de contrôle interne et externe adéquats, notamment en ce qui concerne les opérations pour compte propre et les opérations personnelles de leurs salariés* » et « *être structurée et organisée de façon à restreindre au minimum tout risque de conflits d'intérêts* », qu'elle doit « *respecter des règles de bonne conduite destinées à garantir la protection des investisseurs et la régularité des opérations* », qu'elle doit « *s'abstenir de toute initiative qui aurait pour objet ou pour effet de privilégier leurs intérêts propres au détriment des intérêts de leurs clients* » et qu'elle doit « *mettre en place une organisation interne adéquate permettant de justifier en détail l'origine et la transmission des ordres* » et « *pour chaque ordre, pouvoir apporter la preuve de la date de sa réception, ainsi que de celle de sa transmission* ».

Par ailleurs, l'article 4 de la Loi n° 1.362 du 3 août 2009 dispose que les organismes bancaires « *doivent exercer une vigilance constante à l'égard de la relation d'affaires en examinant les transactions […] conclues pendant toute sa durée […]* ».

La Commission considère donc que le traitement est licite au sens de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

➢ *Sur la justification*

Le responsable de traitement indique que le traitement est justifié par « *le respect d'une obligation légale à laquelle est soumis le responsable de traitement ou son représentant* », et par « *la réalisation d'un intérêt légitime poursuivi [par lui et qui] ne méconnait ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée* ».

A cet égard, la Commission observe que ce traitement permet au responsable de traitement de respecter notamment les obligations découlant des Lois n° 1.314 du 29 juin 2006, n° 1.338 du 7 septembre 2007 et n° 1.362 du 3 août 2009, ainsi que de l'Arrête Ministériel n° 2012.199 du 15 avril 2012.

Par ailleurs, le responsable de traitement indique que ce traitement répond à un objectif légitime essentiel puisqu'il permet d'assurer « *la sécurité et le bon fonctionnement technique du réseau et de son système informatique* », de contrôler le « *respect des règles internes d'usage des outils de communication électronique ainsi que de son règlement intérieur* », de préserver ses « *intérêts économiques, commerciaux ou financiers* » et de se protéger « *contre tout acte susceptible d'engager sa responsabilité civile ou pénale, ou de lui porter préjudice* ».

Le responsable de traitement précise également que les droits et libertés des personnes concernées sont respectés puisque l'usage de la messagerie professionnelle à des fins personnelles est toléré et qu'il est interdit d'accéder aux messages dont l'objet contient des mots clés tels que « *privé* », « *[PRV]* » ou « personnel » afin de ne pas violer le secret de la correspondance privée.

A cet égard, la Commission rappelle, conformément à sa délibération n° 2015-111 du 18 novembre 2015, que « *seule une autorisation du juge peut permettre à l'employeur d'accéder licitement aux messages privés de ses employés lorsque ces derniers n'ont pas autorisé l'employeur à lire leurs messages privés, et cela même si l'employeur a des motifs légitimes de suspecter des actes de concurrence déloyale ou toute autre atteinte portée à ses intérêts ou à la Loi* ».

Elle considère donc que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations nominatives traitées

Les informations nominatives traitées sont :

- identité : nom, prénom, nom de la société, numéro de matricule interne ;
- formation, diplômes, vie professionnelle : fonction professionnelle, titre ;
- caractéristiques financières : portefeuille, n° de compte, RIB, IBAN, BIC ;
- consommation de biens et services, habitudes de vie : achat et vente sur les marchés boursiers, achats de biens et services auprès des fournisseurs ;
- données d'identification électronique : contact et adresse email ;
- informations temporelles : connexion au système, données accédées, horodatage, logs de connexion ;
- messages (entrants et sortants) : contenu, objet, dossier de classement, date et heure ;
- fichiers de journalisation : nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format, pièces jointes, noms de domaine expéditeur de messages ;
- données filtrées : contenu des fichiers transmis.

Le responsable de traitement indique que les informations relatives à l'identité, à la formation, aux diplômes, à la vie professionnelle, aux données d'identification électronique, aux messages et aux données filtrées ont pour origine la personne concernée.

A cet égard, la Commission considère que les informations relatives à l'identité, à la formation, aux diplômes, à la vie professionnelle et aux données d'identification électronique des collaborateurs ont pour origine le traitement ayant pour finalité « *Gestion administrative du personnel de Citi Global Wealth Management SAM* ».

Le responsable indique également que les informations relatives aux caractéristiques financières ont pour origine le client et le personnel.

Les informations relatives à la consommation de biens et services et aux habitudes de vie ont pour origine le client, le personnel et les fournisseurs.

Enfin, les informations temporelles et les fichiers de journalisation ont pour origine le système de messagerie.

Aussi, 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 du 23 décembre 1993.

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 se fait par le biais d'une mention ou clause particulière intégrée dans un document remis à l'intéressé.

L'ensemble de ces documents n'ayant pas été joint, la Commission rappelle que ceux-ci doivent impérativement comporter toutes les mentions prévues à l'article 14 de la Loi n°1.165 du 23 décembre 1993.

Par ailleurs, concernant plus particulièrement l'information du personnel, elle recommande au responsable de traitement ou à son représentant, si cela n'est déjà fait, de mettre en place une charte d'usage des outils de communication électronique, venant préciser, notamment :

- les procédures de contrôle et de surveillance mises en œuvre ;
- la ou les finalités de ces procédures ;
- les personnes habilitées à avoir accès au traitement ;
- la durée de conservation des données collectées ;
- les modalités d'exercice par les personnes de leurs droits d'accès à leurs données.

En outre, afin de limiter l'atteinte portée à la vie privée des utilisateurs, la Commission recommande également au responsable de traitement ou à son représentant de définir dans la charte susmentionnée, la procédure d'accès à la messagerie électronique par les personnes habilitées, en cas d'absence temporaire ou définitive de l'utilisateur, et ce afin d'assurer la continuité des activités.

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

Le droit d'accès s'exerce par voie postale.

A cet égard, la Commission rappelle que la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande.

Elle constate ainsi que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

V. Sur les personnes ayant accès au traitement et les destinataires

- ***Sur les personnes ayant accès au traitement***

Les personnes habilitées à avoir accès au traitement sont :

- le personnel de Citi Global Wealth Management S.A.M. : en création, modification, consultation et suppression pour sa propre messagerie ;
- le Compliance Officer de Citi Global Wealth Management S.A.M. : en consultation ;
- les équipes du Groupe Citigroup en charge de veiller à l'intégrité des marchés financiers : en consultation ;
- les équipes du Groupe Citigroup aux Etats-Unis en charge de prévenir les fuites de données confidentielles : en consultation ;
- les personnels techniques du Groupe Citigroup en France en charge du système d'information : en consultation dans le cadre exclusif de leurs fonctions liées au fonctionnement et à la sécurité du système.

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

La Commission rappelle toutefois que les accès des équipes du Groupe Citigroup aux Etats-Unis en charge de prévenir les fuites de données confidentielles sont conditionnés à l'obtention préalable de l'autorisation de la Commission concernant le transfert des données nominatives issues de ce traitement vers les Etats-Unis, déposé concomitamment.

Elle rappelle par ailleurs qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993 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.

- ***Sur les destinataires***

Compte tenu des fonctionnalités du traitement, la Commission considère, conformément à sa délibération n° 2015-111 du 18 novembre 2015, que le Service d'Information et de Contrôle des Circuits Financiers (SICCFIN) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires d'informations nominatives traitées.

Elle considère par ailleurs que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, la Commission rappelle qu'en cas de transmission, ces Autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

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

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion avec le traitement ayant pour finalité « *Gestion administrative du personnel de Citi Global Wealth Management SAM* », légalement mis en œuvre, et d'un rapprochement / interconnexion avec un traitement ayant pour finalité « *Gestion des habilitations informatiques et accès aux applications* », déposé concomitamment.

La Commission en prend acte.

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.

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

Elle rappelle que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception, conformément à la délibération n° 2015-111 du 18 novembre 2015.

La Commission rappelle également 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 traitement indique que les informations temporelles et les fichiers de journalisation sont conservés 1 an.

La Commission en prend acte et considère que ces durées sont conformes aux exigences légales.

Le responsable de traitement indique également que les informations relatives à l'identité, à la formation, à la vie professionnelle, aux caractéristiques financières, à la consommation de biens et services, aux habitudes de vie, aux données d'identification électronique et aux données filtrées sont conservées 5 ans.

A cet égard, la Commission rappelle toutefois, conformément à la délibération n° 2015-111 du 18 novembre 2015, que les informations relatives à l'identité, à la formation, aux formations, à la vie professionnelle et aux données d'identification électronique ne doivent être conservées que trois mois maximum après le départ de l'utilisateur.

Par ailleurs, elle demande, conformément à la délibération n° 2015-111 du 18 novembre 2015 qu'une politique d'archivage soit mise en place pour le contenu des messages émis et reçus jusqu'à ce que la conservation desdits messages ne soit plus nécessaire.

Après en avoir délibéré, la Commission :

Considère :

- que le SICCFIN et la CCAF peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires des informations du traitement ;

- que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire.

Rappelle que :

- la réponse à une demande de droit d'accès doit intervenir dans le mois suivant réception de la demande ;

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

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

- les accès des personnels du Groupe Citigroup aux Etats-Unis sont conditionnés à l'obtention préalable de l'autorisation de la Commission concernant le transfert des données nominatives issues de ce traitement vers les Etats-Unis ;

- les équipements de raccordement (switchs, routeurs, pare-feux) de serveurs et périphériques doivent être protégés par un login et un mot de passe réputé fort et les ports non utilisés doivent être désactivés ;

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

Fixe la durée de conservation pour les informations relatives à l'identité, à la formation, aux formations, à la vie professionnelle et aux données d'identification électronique à 3 mois maximum après le départ de l'utilisateur.

Demande, s'agissant du contenu des messages émis et reçus, qu'une politique d'archivage soit mise en place jusqu'à ce que la conservation desdits messages ne soit plus nécessaire.

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 Citi Global Wealth Management S.A.M. du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion, stockage et supervision de la messagerie électronique de l'entreprise*».**

Le Président

Guy MAGNAN