Délibération n° 2017-217 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 et supervision des habilitations informatiques, des applications et de l'utilisation des moyens informatiques* »

présenté 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° 1.338 du 7 septembre 2007 sur les activités financières, 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, 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 ou non automatisés d'informations nominatives ;

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 et supervision des habilitations informatiques, des applications et de l'utilisation des moyens informatiques* » ;

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 son organisation interne et afin d'assurer la sécurité informatique de son réseau, cette société souhaite mettre en place un système d'habilitations.

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 et supervision des habilitations informatiques, des applications et de l'utilisation des moyens informatiques ».*

Les personnes concernées sont « *Le personnel de Citi Global Wealth Management SAM* ».

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

- l'authentification au système d'information et exercice de la fonction ou des missions pour lesquelles les employés ont été recrutés ;
- la gestion des évolutions de droits, des mobilités internes et des départs ;
- la mise à jour des comptes systèmes dans le cadre de changement d'informations administratives ;
- la réalisation de l'ensemble des tâches d'activation, de désactivation, de suppression de comptes ou de mise à jour des listes de diffusion de messagerie électronique, des listes de contrôle d'accès et des groupes de privilèges auxquels le collaborateur appartient ;
- les revues de contrôles périodiques afin de s'assurer de la conformité des droits délivrés par rapport aux demandes et aux règles édictées en matière d'accès à l'information ;
- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux (antivirus, pare feux, sondes anti-intrusion, proxies).

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

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 la société Citi Global Wealth Management S.A.M. « *bénéficie de l'agrément de la Commission de Contrôle des Activités Financières au titre de l'article 1er de la loi n° 1.338 du 7 septembre 2007 sur les activités financières » et qu'elle est « par conséquent soumise aux dispositions de l'article 33 de cette loi qui prévoit que toute personne physique qui, à un titre quelconque, participe à l'administration, à la direction ou à la gestion d'une société agréée ou qui est employée par celle-ci est tenue au secret professionnel dans les conditions et sous les peines prévues à l'article 308 du Code pénal ».*

La Commission note également qu'à ce titre « *ce traitement est justifié au regard de la confidentialité des données qu'est amené à traiter* » le responsable de traitement et qu'il « *permet de préserver les intérêts de la société ainsi que ceux de ses employés et des clients* ».

Enfin, elle relève que les employés recevront « *une notification préalable à la mise en service de l'utilisation des habilitations informatiques* ».

La Commission 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, numéro de matricule interne ;
- formation, diplômes, vie professionnelle : poste ;
- données d'identification électronique : compte utilisateur ;
- informations temporelles : connexion au système, données accédées, horodatage, logs de connexion ;
- 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 et aux données d'identification électronique ont pour origine le service des Ressources Humaines.

Il indique également que les informations temporelles et les données filtrées ont pour origine le système.

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'un document spécifique, à savoir la « *note d'information concernant la protection des données* ».

A l'analyse de ce document, la Commission considère que les modalités d'information préalable des personnes sont conformes 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***

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 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 responsables informatiques du groupe Citigroup en France : en création, suppression ou modification des habilitations informatiques ;
- les personnels techniques du Groupe Citigroup en France ; Allemagne, Royaume-Uni et aux Etats-Unis 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 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, 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***

Les informations sont susceptibles d'être communiquées à la Direction de la Sûreté Publique.

La Commission estime que la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

La Commission considère donc que ces transmissions sont conformes aux exigences légales.

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.

La Commission en prend acte.

Il indique également que le présent traitement est à rapprocher et/ou interconnecter avec l'ensemble des traitements automatisés de l'établissement.

A cet égard, la Commission estime que le présent traitement pourra également être interconnecté à tous traitements futurs mis en place par le responsable de traitement à des fins de sécurité.

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.

Cependant, les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

La Commission 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 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 les informations nominatives relatives à l'identité, à la formation, à la vie professionnelle, aux diplômes et aux données d'identification électronique sont conservées jusqu'au départ du salarié.

Les informations relatives à l'horodatage sont conservées 1 an.

Enfin, les informations relatives aux données filtrées sont conservées 5 ans.

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

Après en avoir délibéré, la Commission :

Rappelle que :

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

- 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 ;

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

- les Services de Police monégasque ne pourront avoir communication des informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

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

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 et supervision des habilitations informatiques, des accès aux applications et de l'utilisation des moyens informatiques* ».**

Le Président

Guy MAGNAN