DELIBERATION N° 2013-109 DU 16 JUILLET 2013 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 ET SUPERVISION DE LA MESSAGERIE ELECTRONIQUE D'ENTREPRISE* » PRESENTE PAR LA LLOYDS TSB BANK PLC REPRESENTEE A MONACO PAR LA LLOYDS TSB BANK PLC

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, modifiée, relative à la protection des informations nominatives ;

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 et son Ordonnance d'application ;

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° 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 fixant les conditions d'application de 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° 4.104 du 26 décembre 2012 modifiant 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 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

Vu la délibération n° 2012-119 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 professionnelle* » utilisés à des fins de contrôle de l'activité des employés ;

Vu la demande d'autorisation déposée par LA LLOYDS TSB BANK PLC, le 1er juillet 2013, relative à la modification du traitement automatisé susvisé ;

La Commission de Contrôle des Informations Nominatives,

Préambule

LA LLOYDS TSB BANK PLC est une société de droit britannique. Conformément aux dispositions de l'article 24 de la loi n° 1.165, mo difiée, elle est représentée en Principauté par LA LLOYDS TSB BANK PLC ayant pour objet *« toutes opérations de banque* ».

Dans le cadre de l'exercice de leurs fonctions, les collaborateurs de LA LLOYDS TSB BANK PLC disposent d'une messagerie professionnelle.

L'exploitation de cette messagerie faisant l'objet d'une supervision, ladite banque soumet la mise en œuvre de ce traitement à l'autorisation de la Commission, en application de l'article 11-1 de la loi n° 1.165, précitée.

I. Sur la finalité et les fonctionnalités du traitement

La finalité du traitement est : « *Gestion et supervision de la messagerie électronique d'entreprise* ».

Les personnes concernées sont « *les collaborateurs, les stagiaires, les prestataires utilisant les postes de travail de LLOYDS Monaco et la messagerie d'entreprise* ».

Toutefois, la Commission considère que sont également concernés les tiers expéditeurs ou destinataires d'emails.

Enfin, les fonctionnalités du traitement sont les suivantes :

- l'envoi et la réception de mails cryptés ou non, avec possibilité d'attacher des pièces jointes cryptées ou non ;
- le transfert et la suppression de mails ;
- la gestion des délégations sur les boites mails individuelles ;
- la gestion des contacts de messagerie et des listes de distribution ;
- la gestion des messages archivés ;
- la constitution de preuves en cas de menaces des intérêts ou de l'image de LLOYDS Monaco ou en cas d'infractions civiles ou pénales ;
- la surveillance des boîtes mails (vérification des fichiers journaux de la messagerie, enregistrement de l'historique des messages sortants), utilisation d'un système tiers de surveillance (Clearswift de l'éditeur Clearswift) qui copie tous les mails sortants vers l'internet afin d'avoir une traçabilité et une protection des données confidentielles, le cas échéant l'attribution de droits de lecture aux unités d'audit interne (sous couvert d'une procédure interne) ;
- la sécurisation du système d'information ;
- la préservation de la confidentialité des données de LLOYDS Monaco.

La Commission constate que le traitement a également pour fonctionnalité de répondre plus précisément aux obligations légales de vigilance et de traçabilité des opérations financières imposées notamment par les lois n° 1.338 du 7 septembre 2007 sur les activités financières, n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption.

Au vu de ces éléments, la Commission constate que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la loi n° 1.165, modifiée.

II. Sur la licéité du traitement

Conformément à l'article 11-1 de la loi n° 1.165, modifiée, les traitements « *mis en œuvre à des fins de surveillance* » ou « *portant sur des soupçons d'activités illicites, des infractions* », doivent pour être licites être « *nécessaires à la poursuite d'un objectif légitime essentiel et [respecter] les droits et libertés mentionnés à l'article premier des personnes concernées (…)* ».

Dans sa délibération n° 2012-119 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle* » utilisés à des fins de contrôle de l'activité des employés, la Commission rappelle que conformément au principe de proportionnalité, le responsable de traitement est tenu de mettre en place une procédure de contrôle graduée, adaptée aux divers niveaux de risques auxquels il est confronté.

Le responsable de traitement a annexé à la présente demande d'autorisation un exemplaire de la charte d'utilisation de la messagerie d'entreprise.

La Commission relève à son examen que si LA LLOYDS TSB BANK PLC détaille effectivement les conditions d'utilisation de ce système ainsi qu'une partie de la procédure de contrôle, le fait de recourir à un « *contrôle gradué* » comme explicité dans la délibération n° 2012-119 précitée n'apparait pas clairement.

Ainsi, elle rappelle que les mesures prises doivent être strictement nécessaires au but recherché, ce qui conduit la Commission à distinguer quatre phases de contrôle, allant de la surveillance globale non nominative de l'usage de la messagerie, au contrôle nominatif du contenu des messages électroniques, décomposées comme suit :

- phase 1 : le contrôle non nominatif global des fichiers journaux de la messagerie (ex. nombre de messages envoyés, format des pièces jointes, volumes, etc.) ;
- phase 2 : le contrôle des fichiers journaux des messageries d'un ou plusieurs employés déterminés ;
- phase 3 : le contrôle du contenu des communications électroniques (archivées ou non) d'un ou plusieurs employés déterminés ou déterminables, sélectionnés aléatoirement (échantillonnage) ou par filtrage automatique ;
- phase 4 : le contrôle du contenu des communications électroniques (archivées ou non) d'un ou plusieurs employés déterminés.

Par conséquent et par souci de clarté, elle demande à ce que la procédure de contrôle soit détaillée sur un document distinct de la charte informatique et portée à la connaissance de chaque utilisateur.

Elle observe également que l'accès au contenu des messages d'un employé ne peut se faire que sous l'autorité du *« Département Risk & Compliance »* qui contacte l'expéditeur du message et lui propose d'accéder à ces derniers en sa présence. En l'absence de disponibilité de l'expéditeur sous 2h ou avec son accord par retour d'email, le message sera lu en son absence. L'expéditeur et le Directeur Principal de la succursale sont informés du résultat du contrôle dans les 2h qui suivent.

Par ailleurs, il appert qu'un usage personnel de la messagerie est toléré. Le respect des droits et libertés des personnes concernées est assuré par l'exclusion de tout accès aux messages marqués « *privés* » qui ne pourront être lus « *uniquement sur autorisation du juge* ». La Commission en prend donc acte.

Enfin, dans le but de limiter l'atteinte portée à la vie privée des employés, tout en permettant d'assurer la continuité des activités, elle demande également à ce que soient définies les procédures d'habilitation d'accès à la messagerie professionnelle en cas d'absence temporaire ou définitive d'un salarié de LA LLOYDS TSB BANK PLC.

A la condition de ce qui précède, la Commission considère que le traitement est licite, conformément aux dispositions légales.

III. Sur la justification du traitement

Le traitement est justifié par le respect d'une obligation légale à laquelle est soumis le responsable de traitement.

A cet égard, la Commission observe que ce traitement *« permet à LA LLOYDS TSB BANK PLC d'apporter une preuve en cas de doute ou de litige aux obligations de vigilance et de traçabilité des opérations financières. Ce traitement est également de nature à protéger ses utilisateurs et son responsable contre toute infraction aux articles 308 et suivants du Code pénal, relatifs au secret professionnel. La mise en œuvre d'un suivi des emails à destination de l'extérieur revêt donc un caractère de protection des utilisateurs de la messagerie et du responsable de traitement lui-même, dont les responsabilités pourraient être engagées en cas de défaut de vigilance ».*

Ainsi, au vu de l'ensemble de ces éléments, la Commission considère que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la loi n° 1.165, modifiée.

IV. Sur les informations traitées

Les informations objets du traitement sont les suivantes :

- identité : adresses de messagerie incluant nom et prénom ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès au traitement (3 niveaux : utilisateurs de la messagerie, département IT, département Risk & Compliance) ;
- historique des messages sortants : expéditeurs/destinataires, contenu des messages, date/heure des messages, log d'échange SMTP, taille du message, nature des pièces jointes, taille des pièces jointes ;
- historique du contenu : contenu des messages et des pièces jointes.

La Commission relève que les informations ont pour origine la messagerie pour ce qui est de l'identité et l'historique du contenu.

Enfin, les informations relatives aux données d'identification électronique et à l'historique des messages sortants sont générées par le système informatique.

La Commission considère que ces informations 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 des personnes concernées***

L'information préalable des personnes concernées est effectuée au moyen d'un document spécifique (« *La charte d'utilisation de la messagerie électronique d'entreprise* »), dont une copie a été annexée à la demande d'autorisation, et d'un email.

A cet égard, la Commission rappelle que conformément à l'article 14 de la loi n° 1.165, modifiée, les personnes concernées doiven t être informées de :

- l'identité du responsable de traitement ;
- la finalité du traitement ;
- l'identité des destinataires ou des catégories de destinataires des informations ;
- l'existence d'un droit d'accès et de rectification des informations les concernant.

Dans le cadre de sa délibération n° 2012-119, elle indique en outre qu'en cas de contrôle de la messagerie professionnelle, « *une telle obligation d'information relève d'un souci de transparence envers les employés, ainsi que de loyauté dans la relation de travail* ».

A cet égard, elle relève qu'en l'espèce, les documents d'information précités destinés à l'attention des collaborateurs de LA LLOYDS TSB BANK PLC ne sont pas conformes aux dispositions de l'article 14 de la loi dont s'agit.

Elle demande donc à ce qu'ils soient impérativement complétés.

Par ailleurs, elle demande également à ce qu'un « *disclaimer »* comportant ces mêmes mentions soit intégré en bas de chaque email, de manière à informer les clients et des tiers expéditeurs ou destinataires des messages de leurs droits et de prévoir à ce titre les modalités de l'exercice de ces derniers.

- ***Sur l'exercice des droits d'accès, de rectification et d'opposition***

Les droits d'accès et de suppression s'exercent par courrier électronique auprès de *l'IT Manager & Security Officer* de LA LLOYDS TSB BANK PLC. Le délai de réponse est de 30 jours.

Enfin, la Commission observe que les messages archivés peuvent faire l'objet d'un contrôle ultérieur.

Elle demande, par conséquent, à ce qu'un droit de suppression effectif soit instauré pour les collaborateurs à l'égard de ces messages dits « *privés* ».

Sous cette condition, elle considère 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, modifiée.

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

- ***Sur les destinataires***

Il appert à l'examen des documents annexés que les informations collectées dans le cadre du traitement sont susceptibles d'être communiquées *« aux autorités compétentes dans le cas d'une suspicion d'activité de blanchiment ».*

Par conséquent, la Commission estime qu'une communication à la Direction de la Sûreté Publique peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, elle rappelle qu'en cas de transmission, les Services de police ne pourront avoir accès aux informations objets du traitement que dans le strict cadre de leurs missions légalement conférées.

De même, elle considère que le SICCFIN peut être rendu destinataire des informations dans le cadre des dispositions de 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.

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

Les personnes habilitées à avoir accès au traitement sont :

- le Département Risk & Compliance (consultation seule avec log) ;
- le Département IT (accès complet avec log).

Un prestataire a également accès au traitement pour la maintenance de l'équipement.

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

En ce qui concerne le prestataire, la Commission rappelle néanmoins que conformément aux dispositions de l'article 17 de la loi n° 1.165, modifiée, ses accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service.

Elle rappelle enfin qu'en application de l'article 17-1 de la loi n° 1.165, modifiée, la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et doit pouvoir lui être communiquée à première réquisition.

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'observations particulières.

La Commission rappelle néanmoins 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.

VIII. Sur la durée de conservation

Le responsable de traitement indique que les informations nominatives collectées sont conservées et archivées pour une durée de 10 ans à compter de la réception des messages.

La Commission constate que ce délai est conforme aux exigences légales notamment prévues par la loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et au délai de prescription s'y rapportant, conformément aux dispositions de l'article 12 du Code de procédure pénale.

Enfin, elle rappelle que dans le cadre de l'ouverture d'une procédure judiciaire, toute information nécessaire, notamment à des fins probatoires, pourra être conservée jusqu'au terme de la procédure.

Après en avoir délibéré,

Rappelle que :

- en cas de transmission, les Services de police ne pourront avoir accès aux informations objets du traitement que dans le strict cadre de leurs missions légalement conférées ;

- conformément à l'article 17-1 de la loi n° 1.165, modifiée, la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et doit pouvoir être communiquée à la Commission à première réquisition ;

Demande que :

- la procédure de contrôle soit détaillée dans un document distinct de la charte informatique et portée à la connaissance de chaque utilisateur ;

- soient définies les procédures d'habilitation d'accès à la messagerie professionnelle en cas d'absence temporaire ou définitive d'un collaborateur ou de tout autre membre du personnel de LA LLOYDS TSB BANK PLC.

- de compléter les documents internes relatifs à la messagerie électronique d'entreprise annexés afin de répondre aux exigences de l'article 14 de la loi n° 1.165, modifiée ;

- d'insérer une mention d'information au bas de tout message électronique sortant, afin d'informer les clients et les tiers de la finalité du traitement ainsi que de leurs droits, et de prévoir à ce titre les modalités de l'exercice de ces derniers ;

- d'instaurer un droit de suppression pour les collaborateurs de LA LLOYDS TSB BANK PLC à l'égard des messages d'ordre « *privé* » ;

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 LLOYDS TSB BANK PLC., du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie électronique d'entreprise* ».**

Le Président,

Michel Sosso