Délibération n° 2017-181 du 25 octobre 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 de la messagerie électronique à des fins de surveillance* »

présenté par HSBC Private Bank (Monaco) SA

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 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 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 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 HSBC Private Bank (Monaco) SA, le 11 juillet 2017, concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la messagerie électronique à des fins de surveillance* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 8 septembre 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 25 octobre 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

HSBC Private Bank (Monaco) SA est une société monégasque, immatriculée au Répertoire du Commerce et de l'industrie sous le numéro 97S03269 ayant notamment pour objet en Principauté et à l'étranger, pour son compte ou le compte de tiers, directement ou en participation, « *la réalisation de toutes opérations de banque ou connexes telles que définies par la « Loi bancaire » applicable* ».

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 des emails sortants.

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

Le traitement a pour finalité « *Gestion de la messagerie électronique à des fins de surveillance* ».

Les personnes concernées sont les expéditeurs et destinataires des communications électroniques.

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

Pour l'ensemble des personnes concernées :

- l'échange de messages électroniques en interne ou avec l'extérieur ;
- l'historisation des messages électroniques entrants et sortants ;
- la gestion des contacts de la messagerie électronique ;
- la gestion des dossiers de la messagerie et des messages archivés ;
- l'établissement et la lecture des fichiers journaux ;
- la gestion des habilitations d'accès à la messagerie ;
- la gestion de l'agenda.

Pour les employés uniquement (mails sortants) :

- la mise en place d'une procédure de contrôle gradué ;
- le contrôle au moyen d'un logiciel d'analyse du contenu des messages électroniques sortants ;
- l'établissement de preuve en cas de litige avec un employé.

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 du traitement***

Dans le cadre de sa délibération 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 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 […]* ».

Par ailleurs, l'article 23 de la Loi n°1.338 du 7 septembre 2007 stipule que « *les sociétés agréées sont tenues d'observer les règles prudentielles et de bonne conduite définies par ordonnance souveraine* ».

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° 1.338 du 7 septembre 2007 et n° 1.362 du 3 août 2009.

Par ailleurs, le responsable de traitement indique que ce traitement répond à un objectif légitime essentiel puisqu'il permet :

- *« de contrôler le respect des règles internes d'usage des outils de communication électronique ainsi que de son règlement intérieur » ;*
- *« de préserver les intérêts économiques, commerciaux et financiers de la Banque » ;*
- *« de protéger la banque contre tout acte susceptible d'engager sa responsabilité civile ou pénale, ou de lui porter préjudice » ;*
- *« de prévenir la réalisation de faits illicites ».*

La Commission constate par ailleurs que les droits et libertés des personnes concernées sont respectés puisque l'usage de la messagerie professionnelle à des fins personnelles est toléré *et que « les courriers électroniques qui seront identifiés dans leur « sujet » comme étant un « Message Personnel » »* ne seront pas lus.

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* ».

Sous cette condition, 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 traitées

Les informations exploitées aux fins du présent traitement sont :

- identité : nom et prénom ;
- données d'identification électronique : adresse de messagerie électronique ;
- informations temporelles : date et heure de réception/envoi de messages ;
- gestion des alertes : alertes DLP, à savoir émetteur, destinataire et corps des mails externes, nom du compte client lorsqu'il correspond aux critères de détection de la solution DLP ;
- compte client : nom du compte client (crypté avant d'être intégré dans la solution DLP comme critère de détection) ;
- fichiers journaux : tâches d'administration, nombre de messages entrants et sortants, de messages nettoyés, de spams ;
- informations de connexion liées aux Administrateurs système : nom et prénom de l'employé ;
- log d'accès : logs de connexion des personnes habilitées à avoir accès au traitement ;
- gestion des contacts : nom prénom, raison sociale ;
- habilitations : identité des personnes habilitées à avoir accès à la messagerie et à la solution DLP.

Le responsable de traitement indique que les informations relatives à l'identité et aux habilitations des employés ont pour origine le traitement relatif à la « *Gestion des Ressources Humaines* ».

Les informations relatives aux données d'identification électronique, aux informations temporelles et à la gestion des alertes ont pour origine le compte de messagerie.

Les informations relatives au compte client ont pour origine le traitement ayant pour finalité « *Système des informations concernant la clientèle* ».

Les informations relatives aux fichiers journaux, aux connexions des Administrateurs système et aux logs d'accès ont pour origine le serveur DLP.

Enfin les informations relatives à la gestion des contacts ont pour origine la base de contacts spécifique à chaque utilisateur.

Aussi, la Commission considère que les informations traitées 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 des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est effectuée par le biais d'un document informatif spécifique à l'utilisation d'internet remis aux employés, par le biais du manuel des employés et par le biais des conditions générales.

Après examen des documents qui ont été joints, la Commission demande que l'information préalable des personnes concernées comporte l'ensemble des mentions de l'article 14 de la Loi n°1.165 du 23 décembre 1993.

Elle rappelle par ailleurs que cette information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, et notamment les tiers extérieurs.

A cet égard, la Commission recommande l'insertion d'une mention d'information au bas de tout message électronique sortant afin d'informer lesdits tiers de la finalité du traitement, ainsi que de leurs droits.

- ***Sur l'exercice du droit d'accès des personnes concernées***

Le droit d'accès s'exerce par courrier électronique, par voie postale ou sur place.

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

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, la Commission considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-116 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous ces conditions, la Commission 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 du 23 décembre 1993.

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

- ***Sur les accès au traitement***

Le responsable de traitement indique que les personnes ayant accès au traitement sont :

- ***dans le cadre de la messagerie :***

- les utilisateurs de la messagerie : consultation, modification et inscription de leurs messages ;
- Lotus Notes Team Suisse pour la gestion des utilisateurs : inscription, modification, consultation et maintenance ;
- Lotus Notes Team Monaco pour la création des bases mail : inscription, modification et maintenance.

- ***dans le cadre du système DLP*** :

- IT SEC (Security) Suisse pour la gestion des accès : inscription, modification, consultation et maintenance ;
- ISR (Information Security Risk) Suisse pour la configuration du système et des règles : inscription, modification, consultation et maintenance ;
- ISR (Information Security Risk) Monaco et IT SEC (Security) Monaco pour le traitement des alertes : modification, consultation, et maintenance ;
- BIRO (Business Information Risk Officer) Monaco : consultation des alertes en cas d'escalade d'un incident ;

- BRCM (Business Risk Control Management) Monaco : consultation des alertes en cas d'escalade d'un incident ;
- CRO (Chief Risk Officer) Monaco : consultation des alertes en cas d'escalade d'un incident ;
- le prestataire : maintenance, accès possible lors de la mise à jour de version (accès privilégié temporaire).

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

La Commission 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 communications d'informations***

Compte tenu des fonctionnalités du traitement, la Commission rappelle que, conformément à sa délibération n°2015-111 du 18 novembre 2015, 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 obtenir communication des 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 trois traitements ayant respectivement pour finalité « *Gestion des informations concernant la clientèle* », « *Gestion et administration des comptes utilisateurs* » et « *Gestion des Ressources Humaines* ».

La Commission constate que ces trois traitements ont été légalement mis en œuvre.

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 rappelle néanmoins que 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.

Elle rappelle également 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 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 les informations relatives aux habilitations sont conservées trois mois après la fin du contrat de travail du salarié.

Par ailleurs, les informations relatives aux fichiers journaux et aux logs d'accès sont conservées une année maximum.

Enfin, les informations relatives à l'identité, les informations d'identification électronique, les informations temporelles, la gestion des alertes, les informations relatives au compte client, les informations de connexion liées aux Administrateurs système, et les informations relatives à la gestion des contacts sont conservées 5 ans, conformément à la politique d'archivage mise en place.

Concernant les informations de connexion liées aux Administrateurs système, la Commission rappelle toutefois, conformément à sa délibération n° 2015-111 du 18 novembre 2015 que ces informations ne peuvent être conservées sous une forme permettant l'identification de la personne concernée que pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour lesquelles elles ont été collectées.

Aussi, au regard des fonctionnalités du présent traitement, elle fixe la durée de conservation desdites informations collectées à 1 an.

Sous cette condition, elle considère que ces durées sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Considère :

- qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations ;

- 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.

Rappelle que :

- l'information des personnes concernées doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, et notamment les tiers extérieurs ;

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

- les Autorités Judiciaires ne peuvent avoir communication des informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

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

Demande que l'information préalable des personnes concernées comporte l'ensemble des mentions de l'article 14 de la Loi n°1.165 du 23 décembre 1993.

Fixe la durée de conservation des informations de connexion liées aux Administrateurs système à 1 an.

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 HSBC Private Bank (Monaco) SA**, **du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle à des fins de surveillance ou de contrôle ».***

Le Président

Guy MAGNAN