Délibération n° 2018-053 du 18 avril 2018

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 de la messagerie professionnelle à des fins de surveillance* »

présenté par la Barclays Bank PLC (succursale de Monaco)

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° 1.362 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, 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 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 la Barclays Bank PLC (succursale de Monaco) le 16 janvier 2018 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion et supervision de la messagerie professionnelle à des fins de surveillance* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 14 mars 2018, 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 18 avril 2018 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Barclays Bank PLC (succursale de Monaco) représente à Monaco la Barclays Bank PLC, le responsable de traitement, sis à Londres au Royaume Uni. Elle a pour objet social « *la réalisation de toutes opérations de banque et connexes, telles que définies par la Loi bancaire* ».

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 étant 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 de la messagerie professionnelle à des fins de surveillance ».*

Les personnes concernées sont les « *Expéditeurs et destinataires de communications électroniques* ».

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

- échange de messages électroniques en interne ou avec l'extérieur ;
- 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 ;
- gestion de l'agenda ;
- mise en place d'une procédure de contrôle gradué ;
- contrôle au moyen d'un logiciel d'analyse du contenu des messages électroniques sortants ;
- établissement de preuves en cas de litige avec un client/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***

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 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 de la Loi n° 1.362 du 3 août 2009 précitée.

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

- l'optimisation de l'accomplissement des missions de travail de ses employés ;
- la sécurité et le bon fonctionnement technique du réseau ou système informatique ;
- le contrôle du respect des règles internes d'usage des outils de communication électronique ;
- la préservation des intérêts économiques, commerciaux et financiers de la banque ;
- la protection contre tout acte susceptible d'engager sa responsabilité civile ou pénale, ou de lui porter préjudice ;
- la prévention de faits illicites.

Le responsable de traitement précise également que les droits et libertés des personnes concernées sont respectés puisque « *Barclays Bank PLC (succursale de Monaco) tolère l'usage de la messagerie professionnelle à des fins personnelles et s'interdit d'accéder au contenu des 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. <u>Sur les informations nominatives traitées</u>

Le responsable de traitement indique que les informations nominatives traitées sont :

- **Informations traitées par la messagerie électronique :**

- <u>identité</u> : nom, prénom, identifiant ;
- <u>messages</u> : contenu, objet, dossiers de classement ou d'archivage ;
- <u>gestion des contacts</u> : nom, prénom, raison sociale ;
- <u>informations temporelles</u> : date et heure de réception/envoi de messages ;
- <u>données d'identification électronique</u> : adresse de messagerie électronique ;
- <u>logs d'accès</u> : logs de connexion des personnels habilités à avoir accès au traitement ;
- <u>fichiers journaux</u> : nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format, pièces jointes, noms de domaine expéditeurs de messages ;
- <u>habilitations</u> : identité des personnes habilitées à avoir accès à la messagerie, type de droits conférés, historisation des habilitations.

Les informations relatives à l'identité ont pour origine le traitement ayant pour finalité « *Gestion du personnel* ».

Les informations relatives aux messages et à la gestion des contacts ont pour origine l'utilisateur de la messagerie.

Enfin, les informations relatives aux informations temporelles, aux données d'identification électronique, aux logs d'accès, aux fichiers journaux et aux habilitations ont pour origine le compte de messagerie.

- **Informations traitées par le logiciel de prévention contre la fuite des données :**

- identité : identifiant de l'utilisateur, données clients utilisées pour alimenter le logiciel de scanning (nom, prénom, email, adresse) ;
- messages : contenu, objet ;
- informations temporelles : date et heure de l'alerte, date et heure des actions effectuées par les équipes dans le cadre du traitement des incidents ;
- données d'identification électronique : adresse de messagerie électronique de l'expéditeur et du destinataire, numéro de poste de l'expéditeur ;
- logs d'accès : logs de connexion au système, logs d'accès et de modification des données dans le cadre de l'utilisation de la plateforme technique.

Les informations relatives à l'identité ont pour origine le système de messagerie et le traitement ayant pour finalité « *Tenue de la clientèle* ».

Les informations relatives aux messages, aux informations temporelles, aux données d'identification électronique et aux logs d'accès ont pour origine le système de messagerie.

La Commission considère ainsi 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 est effectuée par le biais d'un document spécifique, d'une mention clause ou clause particulière intégrée dans un document remis à l'intéressé et d'une procédure interne accessible en intranet.

Ces documents n'ayant pas été joints à la demande, la Commission rappelle que ceux-ci doivent impérativement comportés l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Elle recommande par ailleurs 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 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.

Elle rappelle enfin 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, de modification et de mise à jour***

Le droit d'accès s'exerce par voie postale ou sur place auprès du Chief Operating Officer.

La Commission 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 :

Dans le cadre de la messagerie :
- les utilisateurs de la messagerie: en inscription, consultation et modification dans le cadre de l'utilisation de leur messagerie ;
- le Service Technology : tous droits dans le strict cadre de l'accomplissement de leurs missions de contrôles techniques et de maintenance système ;
- les Services d'audit et de contrôle : consultation dans le strict cadre de l'accomplissement de leur mission de contrôle.

Dans le cadre de la prévention contre la fuite de données :
- les Services d'audit et de contrôle : consultation des incidents ;
- le Service Cyber & Information Security : consultation et traitement des incidents ;
- le Service Technology : maintenance et paramétrage du logiciel.

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 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***

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires dans le cadre de leurs missions légalement conférées.

La Commission considère 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.

Par ailleurs, elle estime 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.

Elle considère donc que de telles 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'un rapprochement avec le traitement ayant pour finalité « La *tenue des comptes de la clientèle afin de proposer des services bancaires* » et d'une interconnexion avec le traitement ayant pour finalité « *Gestion du personnel* » qui ont été légalement mis en œuvre.

Il indique également une interconnexion avec un traitement lié au système d'habilitations informatiques.

Ce traitement n'ayant pas fait l'objet de formalité auprès d'elle, la Commission demande que celui-ci lui soit soumis dans les plus brefs délais.

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 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 de traitement indique que toutes les informations traitées par le logiciel de prévention contre la fuite des données sont conservées 1 an.

Pour les informations traitées par la messagerie électronique, il indique que la gestion des contacts est conservée 3 mois après le départ de l'utilisateur.

Par ailleurs, il indique que les informations temporelles, les logs d'accès, les fichiers journaux et les habilitations sont conservés 1 an.

La Commission en prend acte.

Le responsable de traitement indique enfin que les informations liées à l'identité, aux messages et aux données d'identification électronique sont conservées 10 ans.

La Commission relève à cet égard que lesdites informations ne peuvent être conservées que pour une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées.

En conséquence, elle fixe, conformément à sa délibération n° 2015 -111 du 18 novembre 2015, les durées de conservation de données ainsi que suit :

- s'agissant de l'administration de la messagerie électronique (identité et données d'identification électronique), 3 mois maximum après le départ de l'utilisateur ;

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

Après en avoir délibéré, la Commission :

Rappelle que :

- l'information préalable des personnes concernées doit impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n°1.165 du 23 décembre 1993 ;

- 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 lui être communiquée à première réquisition ;

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

- les Autorités judiciaires ne peuvent avoir accès aux 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.

Recommande :

- l'insertion d'une mention d'information au bas de tout message électronique sortant afin d'informer les tiers extérieurs de la finalité du traitement, ainsi que de leurs droits ;

- la mise en place d'une charte d'usage des outils de communication électronique.

Demande que le traitement lié au système d'habilitations informatiques lui soit soumis dans les plus brefs délais.

Fixe les durées de conservation de données suivantes :

- s'agissant de l'administration de la messagerie électronique (identité et données d'identification électroniques), 3 mois maximum après le départ de l'utilisateur ;

- s'agissant du contenu des messages émis et reçus, la Commission demande 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 la Barclays Bank (succursale de Monaco) du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance* ».**

Le Président

Guy MAGNAN