Délibération n° 2018-022 du 21 Février 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 et de contrôle* »

présenté par BNP Paribas Wealth Management 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° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financier ;

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 BNP Paribas Wealth Management Monaco le 7 novembre 2017 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 et de contrôle* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 5 janvier 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 21 février 2018 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

BNP Paribas Wealth Management Monaco est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 91S02724, ayant entre autres pour objet « *en Principauté de Monaco 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.

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 de la messagerie professionnelle à des fins de surveillance et de contrôle* ».

Les personnes concernées sont les employés, les clients et les tiers.

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

- échange de messages électroniques en interne ou avec l'extérieur ;
- établissement d'un historique 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 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 34 de l'Arrêté Ministériel n° 2012-199 du 5 avril 2012 dispose que « *le responsable du contrôle permanent s'assure de […] l'application de procédures garantissant la prise en compte conforme des instructions de la clientèle et des opérations diverses sur instruments financiers […]* ».

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 5 avril 2012.

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

- 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 le contrôle « *de l'utilisation des messageries électroniques professionnelles est réalisé dans le respect de la correspondance privée* ».

Il indique par ailleurs que l'appréciation « *du caractère privé d'un message relève de la responsabilité de son émetteur* » et que « *seront considérés comme privés ceux comportant, à l'émission ou à la réception, une des mentions suivantes : PRIVE, PRIVATE, dans leur titre* ».

Enfin, la Commission relève que les personnels chargés de la supervision des moyens de communication électronique, et du contrôle de l'utilisation des messageries électroniques, « *sont tenus par un devoir de confidentialité* » et que dans ce cadre, « i*ls ne doivent divulguer aucune information, et encore moins celles couvertes par le secret de la correspondance privée ou qui relèvent de la vie privée des employés* ».

A cet égard, elle 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* ».

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

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

- identité : nom, prénom, identifiant ;
- données d'identification électronique : adresse de messagerie électronique ;
- messages : contenu de la messagerie et des messages, objet, dossiers de classement et d'archivage, pièces jointes ;
- gestion des contacts : nom, prénom, raison sociale ;
- informations temporelles : date et heure de réception/envoi de messages ;
- logs d'accès : identifiants de connexion, logs de connexion des personnels habilités à avoir accès au traitement ;
- fichiers journaux : statistiques sur nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format, pièces jointes, noms de domaine expéditeurs de messages ;
- alertes : réception des alertes automatiques DLP.

Le responsable de traitement indique que les informations relatives à l'identité ont pour origine le traitement ayant pour finalité « *Gestion administrative du personnel* ».

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

Enfin, les logs d'accès, les fichiers journaux et les alertes sont générés par le système.

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 employés se fait « *au travers de différentes procédures diffusées dans l'Intranet* » dans l'Intranet, que celle des clients se fait par le biais des conditions générales et celles des tiers externes (destinataires de mails) se fait par le biais d'une mention figurant en bas de chaque mail sortant.

A l'analyse de ces documents, 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 auprès du Service Réclamations pour les clients et les tiers, et auprès du Chief Operating Officer pour les employés.

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.

Sous cette condition, la Commission constate 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 :

- les utilisateurs de la messagerie et les délégataires habilités par ces utilisateurs : en inscription, consultation et modification ;
- les administrateurs système du Service Informatique de la maison mère : en inscription, consultation et modification dans le strict cadre de leurs missions de contrôle, techniques et de maintenance système ;
- le service sécurité de la maison mère : en inscription, consultation et modification dans le strict cadre de leurs missions de contrôle, techniques et de maintenance système ;
- le coordinateur sécurité de Monaco et son suppléant (traitement des alertes DLP) : en inscription, consultation et modification dans le strict cadre de leurs missions de contrôle, techniques et de maintenance système.

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

La Commission constate 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 est 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'une interconnexion ou d'un rapprochement avec le traitement ayant pour finalité « *Gestion administrative du personnel* » qui a été légalement mis en œuvre.

La Commission relève qu'il existe également une interconnexion avec le traitement lié à la téléphonie sur le lieu de travail qui n'a pas fait l'objet de formalité auprès de la Commission.

A cet égard, elle demande que ce traitement 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 les informations relatives à l'identité, aux données d'identification électronique et à la gestion des contacts sont conservées 1 mois maximum après le départ de l'utilisateur.

Par ailleurs, les alertes et les fichiers journaux sont conservés 1 an maximum.

Enfin, les messages, les informations temporelles et les logs d'accès sont archivées jusqu'à ce que la conservation de ces informations ne soit plus nécessaire.

Concernant les informations temporelles et les logs d'accès, la Commission demande toutefois que ceux-ci ne soient conservés qu'un an maximum.

Après en avoir délibéré, la Commission :

Constate que la liste nominative des personnes ayant accès au traitement est tenue à jour.

Rappelle que :

- la liste nominative des personnes ayant accès au traitement doit 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.

Demande que le traitement lié à la téléphonie sur le lieu de travail lui soit soumis dans les plus brefs délais.

Fixe à 1 an maximum la durée de conservation des informations temporelles et des logs d'accès.

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 BNP Paribas Wealth Management Monaco du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle* ».**

Le Président

Guy MAGNAN