Délibération n° 2019-163 du 20 novembre 2019

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 la Compagnie Monégasque de Banque

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 financiers ;

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, modifiée ;

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 la Compagnie Monégasque de Banque le 6 août 2019 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie électronique d'entreprise* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 4 octobre 2019, 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 novembre 2019 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Compagnie Monégasque de Banque (CMB) est une société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 76S1557, ayant pour activité « *de faire, en tous pays, toutes opérations de banque, de finance, de crédit, d'escompte, de commission, de bourse et de change, pour elle-même, pour le compte de tiers ou en participation et d'une façon générale, sous les seules restrictions résultant des dispositions légales en vigueur, toutes opérations pouvant se rattacher à l'objet social* ».

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 Electronique d'Entreprise* ».

Toutefois, à la lecture du dossier, il appert que le traitement est mis en œuvre à des fins de surveillance par le biais de copie et de contrôle, la Commission modifie la finalité comme suivant : « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle ».*

Les personnes concernées sont les « *collaborateurs du Groupe CMB* » et les « *correspondants externes* ».

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

- *« échange de messages électroniques en interne ou avec l'extérieur ;*
- *transfert, classement (dossiers) et suppression de messages ;*

- *historisation des messages électroniques entrants et sortants ;*
- *intégration en GED de messages et leurs éventuelles pièces jointes issues de correspondance avec la clientèle ;*
- *gestion de la mise en quarantaine des messages suspects ;*
- *gestion des délégations d'accès aux boites mails ;*
- *gestion des contacts de la messagerie électronique ;*
- *gestion des messages archivés ;*
- *génération et exploitation des fichiers de journalisation ;*
- *gestion des habilitations d'accès à la messagerie (droits d'accès, liste de distribution,…) ;*
- *gestion de l'agenda ;*
- *mise en place d'une procédure de contrôle gradué ;*
- *établissement de preuves en cas de litige avec un client/salarié. »*

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, modifiée, 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 :

- *« L'optimisation de l'accomplissement des missions de travail des employés du Groupe CMB ;*
- *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 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 *« qu'afin de préserver ses obligations légales, le Groupe CMB met donc en place des procédures de surveillance et de contrôle de sa messagerie électronique, dans le strict respect des principes de proportionnalité et de transparence ».*

Enfin, 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* ».

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 ;
- adresses et coordonnées : adresse postale, coordonnées téléphoniques (mobile/fixe) ;
- vie professionnelle : fonctions professionnelles ;
- données d'identification électronique : adresse de messagerie électronique ;
- messages : contenu, objet ;
- gestion des contacts : nom, prénom, raison sociale ;
- informations temporelles : date et heure de réception/envoi de messages ;
- logs d'accès : logs de connexion des personnes habilitées à avoir accès au traitement ;
- fichiers journaux : nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format, pièces jointes, noms de domaine expéditeurs de messages, (…) ;
- habilitations : identité des personnes habilités à avoir accès à la messagerie, type de droits conférés, historisation des habilitations.

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

Il précise également que les informations relatives aux données d'identification électronique, aux adresses et coordonnées et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative du personnel* » ou *« la messagerie professionnelle pour ce qui concerne le tiers à l'établissement ».*

Les informations relatives aux messages et à la gestion des contacts ont pour origine le système de messagerie professionnelle.

Enfin, les informations temporelles, les logs d'accès et les fichiers journaux sont générés par le système de messagerie professionnelle.

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 s'effectue par le biais d'une procédure interne accessible en Intranet et d'une charte informatique.

Ces documents n'ayant pas été fournis, la Commission rappelle que les modalités d'information préalable des personnes doivent être conformes aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

D'autre part, l'information préalable des clients se fait par le biais d'un legal disclaimer, cette mention figurant en fin de chaque mail sortant.

A l'analyse de ce document, la Commission considère que les modalités d'information préalable des clients 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 courrier électronique auprès du Data Protection Officer.

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 considère par ailleurs 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. 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.

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 :

- chaque utilisateur : accès à sa propre messagerie dans les conditions ordinaires d'utilisation (consultation, inscription, modification, suppression des emails, fiches contacts, dossiers de messagerie) ;
- audit interne : en charge de la recherche des correspondances et de leur consultation ;
- l'IT Risk Manager : dans son rôle de contrôle des risques IT ;
- le RSSI : dans son rôle de garant de la confidentialité autorisant l'accès à « Black Box » ;
- le département informatique : administrateurs de la messagerie électronique d'entreprise.

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, 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 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 « *Gestion administrative des salariés* » qui a été légalement mis en œuvre.

Le responsable de traitement indique qu'il existe également une interconnexion avec le traitement ayant pour finalité « *Gestion et traçabilité des habilitations informatiques* » qui a 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 chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

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 adresses et coordonnées, à la vie professionnelle, aux données d'identification électronique et à la gestion des contacts sont conservées 3 mois maximum après le départ de l'utilisateur.

Par ailleurs, les logs d'accès, les habilitations et les fichiers journaux sont conservés 1 an maximum.

Enfin, le contenu des messages émis et reçus et les informations temporelles sont archivés jusqu'à ce que la conservation de ces messages ne soit plus nécessaire.

La Commission considère que ces durées de conservation sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Modifie la finalité comme suivant : « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle ».*

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.

Rappelle que :

- conformément à sa délibération n° 2015-111 du 18 novembre 2015, « *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 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.

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 Compagnie Monégasque de Banque 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