DELIBERATION N° 2012-125 DU 23 JUILLET 2012 DE LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES PORTANT AUTORISATION SUR LA DEMANDE PRESENTEE PAR LA SOCIETE GENERALE PRIVATE BANKING (MONACO) RELATIVE A LA MISE EN ŒUVRE DU TRAITEMENT AUTOMATISE D'INFORMATIONS NOMINATIVES AYANT POUR FINALITE « *GESTION ET SUPERVISION DE LA MESSAGERIE ELECTRONIQUE PROFESSIONNELLE* »

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 du 28 janvier 1981 et son protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives, et son Ordonnance Souveraine d'application ;

Vu la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, et son Ordonnance Souveraine 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, et son Ordonnance Souveraine d'application ;

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 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 Recommandation du Conseil de l'Europe n° R(89)2 du 19 janvier 1989 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;

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 SOCIETE GENERALE PRIVATE BANKING (MONACO) le 4 mai 2012 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Supervision des moyens de communication électronique : sécuriser le système d'information, préserver la confidentialité des données par le contrôle de l'utilisation des messageries électroniques professionnelles* » ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 23 juillet 2012 portant examen du traitement automatisé susvisé ;

La Commission de Contrôle des Informations Nominatives,

Préambule

La SOCIETE GENERALE PRIVATE BANKING (MONACO) (SGPB MONACO) est une société de droit privé exerçant à titre principal des activités bancaires et de gestion du patrimoine pour une clientèle locale et internationale.

Afin de prévenir tous risques inhérents à l'utilisation, par son personnel, d'une messagerie électronique professionnelle, la SGPB MONACO souhaite mettre en œuvre un système de supervision et de contrôle de cette dernière.

A ce titre, en application de l'article 11-1 de la loi n° 1.165 du 23 décembre 1993, modifiée, relatif à la mise en œuvre de traitements automatisés d'informations nominatives « *à des fins de surveillance* » ou « *portant sur des soupçons d'activités illicites, des infractions* », la SGPB MONACO soumet la présente demande d'autorisation concernant le traitement ayant pour finalité « *Supervision des moyens de communication électronique : sécuriser le système d'information, préserver la confidentialité des données par le contrôle de l'utilisation des messageries professionnelles* ».

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Supervision des moyens de communication électronique : sécuriser le système d'information, préserver la confidentialité des données par le contrôle de l'utilisation des messageries professionnelles* ».

Les personnes concernées sont « *les salariés, collaborateurs et prestataires de la SGPB pour lesquels les messageries électroniques sont mises à disposition* ».

A l'analyse du dossier, la Commission constate toutefois que sont également concernés les clients de la SGPB MONACO, ainsi que tout autre tiers émetteur ou destinataire de messages électroniques n'appartenant pas au personnel de cette société.

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

- « *envoi et réception de mails cryptés ou non, avec possibilité d'attacher des pièces jointes cryptées ou non* » ;
- « *classement des mails par répertoire* » ;
- « *transfert et suppression de mails* » ;
- « *gestion de listes de distribution* » ;
- « *gestion des identités, authentifications et habilitations d'accès des utilisateurs à la messagerie, pour contrôler l'utilisation de la messagerie électronique* » ;
- « *dispositifs de sécurité des connexions des agents à leur boite mail : utilisation des ID Notes associés à un mot de passe pour garantir l'identité de l'utilisateur* » ;
- « *attribution par l'utilisateur de droits d'accès à sa boite mail à d'autres personnes* » ;
- « *attribution de droits de lecture de l'ensemble des boites mails de l'entité à la personne en charge de la supervision des moyens de communication électronique* ».

Toutefois, la Commission relève que le traitement a également pour fonctionnalités :

- d'établir et de vérifier les fichiers journaux de la messagerie ;
- d'enregistrer l'historique des messages électroniques entrants et sortants ;
- de gérer les contacts de la messagerie ;
- de gérer les messages archivés ;
- de répondre aux obligations légale de vigilance et de traçabilité des opérations financières imposées aux établissements bancaires et assimilés ;
- de garantir le respect d'un intérêt légitime du responsable de traitement ou de son représentant, tel que visé au point III de la présente délibération ;
- de permettre la constitution de preuves en cas de violation de ces intérêts, ou en cas d'infractions civiles ou pénales.

Elle en prend donc acte.

Au vu de ces éléments, la Commission considère qu'il convient de reformuler la finalité proposée par le responsable de traitement, et ce d'autant qu'aux termes de l'article 10-1 de la loi n° 1.165, celle-ci doit être explicite, c'est-à-dire immédiatement intelligible à la seule lecture de son intitulé.

Par conséquent, la Commission demande que la finalité du traitement soit modifiée comme suit : « *Gestion et supervision de la messagerie électronique professionnelle* ».

Par ailleurs elle relève, dans la note de service relative à la supervision des moyens de communication électronique jointe à la demande d'autorisation, que « *le résultat des vérifications et les éventuelles anomalies identifiées sont renseignées par le BCM dans l'outil de suivi des risques. (…) Le résultat des contrôles est archivé par le BCM et conservé pendant une durée de 5 ans* ».

A cet égard, elle rappelle que cet outil est susceptible de constituer un traitement automatisé d'informations nominatives distinct qu'il conviendra, le cas échéant, de soumettre aux formalités légales. Elle prend par ailleurs acte du rapprochement opéré entre ces deux traitements.

Enfin, la Commission rappelle qu'en cas d'interconnexion avec d'autres traitements, tels que la gestion de l'agenda et des plannings, il conviendra d'effectuer une demande d'autorisation modificative, conformément aux dispositions de l'article 9 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.

Ainsi, 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.

En l'espèce, la Commission relève que dans le cadre de la « *Charte d'utilisation des moyens de communication électronique* », la SGPB MONACO indique qu'« *une exploitation statistique des enregistrements est réalisée, sous forme anonyme, pour des motifs opérationnels* ». Cette procédure, qui correspond à la phase 1 décrite par la Commission dans sa délibération n° 2012-119 susvisée, est proportionnée au regard du but recherché, à savoir vérifier le bon fonctionnement du système d'information de la SGPB MONACO.

La SGPB MONACO indique par ailleurs qu'elle « *peut procéder à des audits à caractère nominatif sur les enregistrements informatiques de l'entreprise, suite à un dysfonctionnement, une alerte de sécurité ou une présomption d'une utilisation non conforme des moyens de communication, sous réserve du respect du secret de la correspondance privée (…). En ce cas, les constatations matérielles ont pour but de relever les diverses circonstances qui éclaireront l'entreprise sur l'éventuelle réalisation d'un fait fautif et sur l'identité de son auteur* ».

A cet égard, la Commission demande, conformément aux termes de sa délibération n° 2012-119 susvisée et au principe de proportionnalité, à ce que le responsable de traitement distingue trois phases.

La première permet le contrôle nominatif des seuls fichiers journaux du ou des personnes concernées, à l'exclusion de tout accès au contenu des messages électroniques.

Ce contrôle doit avoir pour but de préserver la sécurité du réseau informatique, garantir son bon fonctionnement, ainsi que détecter tout abus d'usage de la messagerie au regard des règles internes, en cas d'alerte sécurité ou de dysfonctionnement détecté lors de la phase 1.

La seconde phase permet l'accès au contenu même des messages professionnels, dès lors qu'une obligation légale du responsable de traitement le justifie – ce qui peut être le cas en l'espèce, comme indiqué au point III de la présente délibération.

Dans ce cas, la Commission considère que le responsable de traitement peut procéder à une surveillance préalable à tout soupçon, par le contrôle régulier aléatoire de plusieurs personnes sélectionnées par voie d'échantillonnage. En l'espèce, le responsable de traitement indique effectuer des contrôles mensuels et aléatoires, réalisés sur cinq messageries au maximum. Cela semble conforme aux termes de la délibération n° 2012-119.

Enfin, dans le cadre de la troisième phase, la Commission admet que le responsable de traitement puisse contrôler les messages professionnels d'une ou plusieurs personnes déterminées, en cas de soupçons sérieux quant à l'existence d'une violation grave de ses intérêts économiques, commerciaux ou financiers, de faits susceptibles d'engager sa responsabilité civile ou pénale, ou encore de faits illicites commis par un ou plusieurs personnes.

Ainsi, au vu de ces observations, la Commission demande à la SGPB MONACO de modifier sa Charte d'utilisation des moyens de communication électronique, afin d'y intégrer

une procédure de supervision graduée plus détaillée et explicite, conforme au principe de proportionnalité et aux termes de sa délibération n° 2012-119.

En outre, afin de limiter l'atteinte portée à la vie privée des employés, tout en permettant d'assurer la continuité des activités, la Commission recommande de définir 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 SGPB MONACO.

Enfin, elle prend acte des mesures prises par le responsable de traitement afin de garantir le respect du secret des correspondances privées.

III. Sur la justification du traitement

Le responsable de traitement indique tout d'abord que le traitement est justifié par le consentement des personnes concernées.

Toutefois, comme rappelé par la Commission dans sa délibération n° 2012-119 susvisée, le consentement des personnes concernées ne peut pas justifier la mise en œuvre du traitement dont s'agit. En outre, le consentement des tiers expéditeurs ou destinataires de messages n'a pas pu être obtenu par le responsable de traitement.

Cette justification doit donc être écartée.

Le responsable de traitement indique par ailleurs que le traitement est justifié par la réalisation d'un intérêt légitime, sans que soient méconnus les libertés et droits fondamentaux des personnes concernées.

A cet égard, il mentionne plusieurs objectifs susceptibles de contribuer à la réalisation de cet intérêt légitime, à savoir la prévention des risques pour l'activité de la SGPB MONACO par :

- la sécurisation du système d'information ;
- la préservation « *de la confidentialité des données et des informations auxquelles l'entité et le personnel accèdent dans le cadre de leurs activités* » ;
- le « *respect des instructions internes [et] des règles de sécurité de l'entité* » ;
- la « *sécurité des échanges d'informations financières et/ou économiques relatives aux projets ou à la conception, la fabrication, la production, les caractéristiques et tarifications des services et produits proposés par l'entité* ».

Ainsi, la Commission relève que ces objectifs sont conformes aux termes de sa délibération n° 2012-119.

Le responsable de traitement indique en outre que les droits et libertés des personnes concernées sont respectés, dans la mesure où « *les contrôles sont effectués par un contrôleur dûment habilité* » dans le cadre de procédures portées à leur connaissance par le biais de la Charte et de la note de service précitées. Dans tous les autres cas, « *les accès en consultation à leur messagerie sont octroyés par les agents eux-mêmes* ». Les modalités d'information des personnes concernées sont analysées au point V de la délibération.

Enfin, le responsable de traitement indique que le traitement permet de répondre aux obligations légales et réglementaires auxquelles il est soumis, de même que son personnel.

A ce titre il fait référence au secret bancaire. Toutefois, le secret professionnel est une obligation générale à tout milieu professionnel. Il y a aurait donc atteinte au principe de proportionnalité si la Commission acceptait, sur ce fondement, la supervision systématique des messageries électroniques.

C'est pourquoi, comme rappelé dans sa délibération n° 2012-119, la Commission estime qu'il convient de justifier ce type de procédure par des obligations légales spécifiques et sectorielles, à savoir les obligations de vigilance et de traçabilité des opérations financières imposées aux établissements bancaires et assimilés.

Ces obligations sont issues, notamment, des textes suivants :

- la Loi n° 1.338 du 7 septembre 2007 sur les activités financières et son Ordonnance Souveraine d'application ;
- 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, et son Ordonnance Souveraine d'application ;
- la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ainsi que 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.

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

Aux termes de la demande d'autorisation, les informations objets du traitement sont les suivantes :

- identité : nom, prénom, initiales ;
- adresses de messagerie : adresse de messagerie professionnelle, adresses de messagerie générique, adresses de messageries des interlocuteurs ;
- données d'identification électronique : identifiants de connexion ;
- utilisation de la messagerie : répertoires, pièces jointes et fichiers crées dans la messagerie hors archives locales, contenu de la messagerie et des messages (hors messages privés), date et heure de réception/envoi de messages.

Par ailleurs, à l'analyse du dossier, la Commission observe que sont également collectées les informations suivantes, notamment :

- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès au traitement, y compris les utilisateurs de la messagerie ;
- fichiers journaux : nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format et nature des pièces jointes, noms de domaine expéditeurs de messages, (…) ;
- habilitations : identité des personnes habilitées à avoir accès à la messagerie, type de droits conférés et leur historique.

Elle en prend donc acte.

La Commission constate que ces informations découlent du fonctionnement même de la messagerie, pour ce qui est de l'identité des personnes, des adresses de messagerie,

des données afférentes à l'utilisation de la messagerie ou aux habilitations d'accès conférées. En ce qui concerne les logs de connexion et les fichiers journaux, ceux-ci sont générés par le système informatique.

Ainsi, et au vu de sa délibération n° 2012-119, 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*

Le responsable de traitement indique que l'information préalable des personnes concernées est effectuée via une mention particulière intégrée dans un document d'ordre général accessible en ligne, ainsi que par une procédure interne accessible en Intranet.

Il s'agit de la Charte d'utilisation des moyens de communication électronique précitée, qui est « *diffusée sur l'Intranet et accessible à tous* » ; ainsi qu'une note de service « *diffusée et intégrée dans la base de procédures accessible à tous* ».

A cet égard, la Commission rappelle que conformément à l'article 14 de la loi n° 1.165, modifiée, les personnes concernées doivent être informées des éléments suivants :

- 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* ».

Ainsi, la Commission demande à ce que la Charte susmentionnée vienne préciser, notamment :

- les procédures de contrôle et de surveillance mises en œuvre, suivant les règles définies au point II de la présente délibération ;
- 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.

Elle relève qu'en l'espèce, les deux documents précités (Charte et note de service) ne contiennent pas l'ensemble de ces éléments. Elle demande donc à ce qu'ils soient complétés en ce sens.

Enfin, la Commission relève qu'aucune information n'est prévue à l'attention des personnes concernées qui ne font pas partie du personnel de la SGPB MONACO, tels que les clients et tiers expéditeurs ou destinataires de messages électroniques. Elle demande donc l'insertion d'une mention d'information au bas de tout message électronique sortant, afin d'informer ces personnes de la finalité du traitement, ainsi que de leurs droits. Par ailleurs, une mention d'information pourra être prévue dans les clauses contractuelles signées avec les clients.

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

Le responsable de traitement indique dans la note de service que les droits d'accès, de rectification et d'opposition des membres du personnel de la SGPB MONACO s'exercent par courrier électronique ou sur place, auprès du Service Déontologie/Compliance. Le délai de réponse est de 30 jours.

En ce qui concerne plus particulièrement le droit d'opposition, il est indiqué que « *[le personnel de la SGPB MONACO peut] s'opposer, sous réserve de justifier d'un motif légitime, à ce que des informations nominatives les concernant soient prises en compte dans le processus de supervision de leur messagerie électronique, étant entendu que cette opposition peut conduire la Banque à mettre à leur disposition une boîte de messagerie professionnelle générique et non personnelle* ». Ces dispositions sont conformes à l'article 13 de la loi n° 1.165, modifiée.

En outre, il appert que seul le titulaire de la messagerie électronique peut modifier, mettre à jour ou supprimer le contenu de sa messagerie.

La Commission constate que ces modalités d'exercice des droits du personnel de la SGPB MONACO sont conformes aux exigences légales.

En ce qui concerne les clients ainsi que les tiers à la SGPB MONACO, aucune modalité n'est prévue. La Commission demande donc à ce que conformément aux exigences légales, ces modalités soient précisées dans le cadre de la mention insérée en bas des messages électroniques sortants à l'attention de ces personnes.

VI. Sur les personnes ayant accès au traitement

Aux termes de la demande d'autorisation, les personnes habilitées à avoir accès, en seule consultation, aux messageries sont :

- les supérieurs hiérarchiques des personnes concernées par le traitement ;
- les services Déontologie, Juridique et Contentieux ;
- les agents habilités par le propriétaire de la messagerie lui-même.

Concernant les agents susvisés, la Commission demande à ce que les conditions et hypothèses dans lesquelles ceux-ci peuvent accéder à la messagerie de leurs collègues de travail soient précisées. En effet, de tels accès ne sauraient, sans violer le principe de proportionnalité, être permanents, et devraient être réservés aux cas d'absence temporaire ou définitive du collaborateur ou de l'employé concerné, aux fins d'assurer la continuité de ses activités dans l'intérêt de la SGPB MONACO.

En ce qui concerne les supérieurs hiérarchiques, il est précisé dans la note de service que ceux-ci sont présents en cas de contrôle d'une messagerie électronique « *dans tous les cas autres que le besoin de surveillance permanente* » définie au point 4.1 de ladite note, exercée quant à elle par le Service Déontologie, avec délégation vers le BCM.

Aucune indication n'est portée en ce qui concerne les droits d'accès conférés aux services Juridique et Contentieux. Toutefois, il ressort de l'analyse du dossier qu'il s'agit en l'espèce non pas d'accès au traitement, mais de communication de données pour la gestion de dossiers de nature litigieuse, voire contentieuse. La Commission en prend donc acte.

Enfin, elle observe que les administrateurs système du Service Informatique disposent de tous les droits d'accès à ce traitement, dans le strict cadre de l'accomplissement de leurs missions techniques et de maintenance du système.

En outre, la Commission prend acte que conformément à la Charte, « *ils sont tenus par un devoir de confidentialité. Dans ce cadre, ils ne doivent pas divulguer ces informations lorsqu'elles sont couvertes par le secret de la correspondance privée ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni la sécurité ni l'intérêt de l'entreprise* ».

Toutefois, elle appelle l'attention du responsable de traitement sur le fait qu'aucune des personnes susvisées ne pourra avoir accès aux contenus des messages électroniques identifiés comme privés.

Ainsi, sous réserve des observations de la Commission formulées aux points II et V de la présente délibération, la Commission constate que les accès susvisés sont conformes aux exigences légales.

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 jusqu'à la fin de la relation de travail.

De manière contradictoire, il est néanmoins indiqué dans la Charte que « *les traces et messages pourront être conservés pendant une durée maximale d'un an, sauf si des dispositions légales ou réglementaires venaient à imposer aux entreprises des délais de conservation plus longs* ».

Ainsi, conformément aux termes de sa délibération n° 2012-119, la Commission fixe les délais de conservation maximums suivants :

1. 5 ans lorsqu'il s'agit de vérifier si le personnel respecte les régulations internes de la SGPB MONACO – cette durée correspondant au délai de prescription en matière prudhommale (article 2092 bis du Code civil) ;
2. 10 ans si le contrôle a pour but la détection de crimes ou délits visés aux articles 218-1 et 218-2 du Code pénal – conformément au délai de prescription prévu à l'article 12 du Code de procédure pénale.

En tout état de cause, la Commission recommande l'adoption d'une durée de conservation moindre dès lors que les données ne sont plus nécessaires à la réalisation de la finalité pour laquelle elles ont été initialement collectées, conformément aux dispositions de l'article 10-1 de la loi n° 1.165, modifiée.

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 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 ;

- qu'en ce qui concerne la justification du traitement, ni le consentement des personnes concernées, ni l'obligation de secret bancaire ne peut justifier la mise en œuvre du traitement dont s'agit ;

- que le principe du secret des correspondances, qui s'étend au lieu de travail, doit impérativement être respecté, ce qui implique qu'aucune des personnes habilitées à avoir accès au traitement ne peut accéder aux contenus des messages électroniques identifiés comme privés ;

- que 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 ;

- qu'en cas d'interconnexion avec d'autres traitements, tels que la gestion de l'agenda et des plannings, ou l'outil de suivi des risques, il conviendra d'effectuer une demande d'autorisation modificative, en application de l'article 9 de la loi n° 1.165, ainsi que toute formalité légale afférente à la mise en œuvre de ces traitements ;

Demande à la SGPB MONACO :

- de modifier sa Charte d'utilisation des moyens de communication électronique, afin d'y intégrer une procédure de supervision graduée plus détaillée et explicite, conforme au principe de proportionnalité tel qu'interprété dans sa délibération n° 2012-119 ;

- de compléter en outre cette Charte ainsi que la note de service annexée afin de répondre aux exigences de l'article 14 de la loi n° 1.165, modifiée, et au principe de transparence posé par la Commission dans cette même délibération n° 2012-119 ;

- 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 droits ;
- de préciser les conditions et hypothèses dans lesquelles les collaborateurs et employés sont habilités à avoir accès à la messagerie de leurs collègues de travail ;

Fixe les délais de conservation maximums suivants :

- 5 ans lorsqu'il s'agit de vérifier si le personnel respecte les régulations internes de la SGPB MONACO ;

- 10 ans si le contrôle a pour but la détection de crimes ou délits visés aux articles 218-1 et 218-2 du Code pénal ;

Recommande l'adoption d'une durée de conservation moindre dès lors que les données ne sont plus nécessaires à la réalisation de la finalité pour laquelle elles ont été initialement collectées, conformément aux dispositions de l'article 10-1 de la loi n° 1.165, modifiée ;

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 SOCIETE GENERALE PRIVATE BANKING (MONACO), du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie électronique professionnelle* ».**

Le Président,

Michel SOSSO