Délibération n° 2024-176 du 9 octobre 2024

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 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° 1.314 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 relative aux 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° 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'Ordonnance Souveraine n° 7.065 du 26 juillet 2018 portant modification de l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la loi n° 1.362 du 3 août 2009, modifiée, relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

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 délibération n° 2018-053 du 18 avril 2018 de la Commission de Contrôle des Informations Nominatives ayant pour finalité « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance* » présenté par Barclays Bank PLC (succursale de Monaco) ;

Vu la demande d'autorisation déposée par Barclays Bank PLC (Succursale de Monaco) le 12 juin 2024 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 9 août 2024, 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 9 octobre 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Barclays Bank PLC est une société anglaise établie à Monaco par sa succursale enregistrée au RCI sous le numéro 68S01191, ayant pour activité « *la réalisation de toutes opérations de banque et connexes, telles que définies par la Loi bancaire* ».

Par délibération n° 2018-053 du 18 avril 2018, la Commission a autorisé 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 Barclays Bank PLC (succursale de Monaco).

Les modalités d'exploitation de ce traitement ayant évolué, le responsable de traitement souhaite aujourd'hui le remplacer par le présent traitement.

La Commission en prend acte.

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 électronique professionnelle 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 sont les suivantes :

- 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 de fichiers journaux ;
- la gestion des habilitations d'accès à la messagerie ;
- la gestion de l'agenda ;
- la mise en place d'une procédure de contrôle gradué ;
- le contrôle au moyen d'un logiciel d'analyse du contenu des messages électroniques ;
- l'établissement de preuves en cas de litige avec un client/employé ;
- la mise en place d'un système d'antivirus.

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 :

- 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* ».

Sous cette réserve, elle considère 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 les suivantes :

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

- identité : nom, prénom, identifiant ;
- messages : contenu, objet, dossiers de classement ou d'archivage ;
- gestion des contacts : nom, prénom, raison sociale ;
- informations temporelles : date et heure de réception/envoi de messages ;
- données d'identification électronique : adresse de messagerie électronique ;
- logs d'accès : logs de connexion des personnels habilités 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 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 ont pour origine le compte de messagerie et les habilitations le traitement ayant pour finalité « *Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle d'accès au Système d'Information* ».

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

- identité : nom, prénom, identifiant ;
- 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 : identifiants de connexion (adresse électronique) ;
- 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 ;
- habilitations : 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 système de messagerie et le traitement ayant pour finalité « *Tenue des comptes clientèle* ».

Les informations relatives aux messages et les informations temporelles ont pour origine le DLP.

Les logs d'accès ont pour origine le système de messagerie.

Enfin, les données d'identification électronique et les habilitations ont pour origine le traitement ayant pour finalité « *Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle d'accès au Système d'Information* ».

- **Informations traitées par le logiciel d'analyse des menaces sur chaque compte des employés sur le cloud :**

- identité : nom, prénom, identifiant ;
- informations temporelles : date et heure des activités sur le Cloud et sur les ordinateurs portables, date et heure des alertes, date et heure des alertes traitées par les équipes de sécurité ;
- données d'identification électronique : identifiants de connexion (adresse électronique) ;
- 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 ;
- habilitations : identité des personnes habilitées à avoir accès à la messagerie, type de droits conférés, historisation des habilitations ;
- autres données : intitulé du fichier/email faisant l'objet d'une alerte.

Les informations ont pour origine le logiciel et le traitement ayant pour finalité « *Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle d'accès au Système d'Information* ».

- **Informations traitées par le logiciel d'analyse et de détection des différentes menaces par email :**

- informations temporelles : date et heure de l'e-mail ;
- autres données : adresse email de l'envoyeur, adresse email du récipiendaire, objet de l'email, adresse IP, nom de l'éventuelle pièce jointe, URLs potentielles dans les emails, contenu de l'email.

Les informations ont pour origine toutes les personnes ayant envoyé un email à un employé de Barclays Bank PLC.

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 rubrique propre à la protection des données personnelles accessible en ligne, d'une mention particulière intégrée dans un document d'ordre général 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 comporter 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 l'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, par courrier électronique ou sur place.

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.

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, elle considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer en cas de doute 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° 2015-113 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 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 :

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 ;
- les administrateurs IT Barclays Groupe : 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, paramétrage du logiciel ;
- le Service Compliance et Control Delivery : consultation et traitement des incidents uniquement en cas d'absence et d'indisponibilité du Service Cyber & Information Security afin d'assurer et de garantir la continuité du service ;
- les administrateurs IT Barclays Groupe : tous droits dans le strict cadre de l'accomplissement de leurs missions de contrôles techniques et de maintenance système.

Dans le cadre de l'analyse des menaces sur les ordinateurs des employés :

- les administrateurs IT Barclays Groupe : 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 Monaco.

Dans le cadre de la détection des malwares relatifs aux emails entrants :

- les équipes Ops Cyber Team : consultation et analyse des alertes dans le cadre de leur mission d'analyse lorsque les emails reçus ont été placés en quarantaine ;
- le personnel habilité du prestataire : maintenance de l'outil en cas de défaillance constatée (uniquement sur autorisation préalable des administrateurs de Barclays).

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

La Commission relève toutefois que certains des administrateurs IT Barclays Group et des équipes Ops Cyber Team sont situés en Inde et aux Etats-Unis.

De même, le personnel du prestataire peut être situé dans un pays situé partout dans le monde.

Aussi, certains de ces pays ne disposant pas d'un niveau de protection adéquat au sens de la Loi n°1.165 du 23 décembre 1993, la licéité de ces communications d'informations nominatives sera analysée dans les deux demandes d'autorisation de transfert concomitamment soumises.

La Commission rappelle enfin 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 l'Autorité Monégasque de Sécurité Financière (AMSF) 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.

Le responsable de traitement indique enfin des communications ponctuelles et spécifiques peuvent être effectuées, concernant la clientèle résidente française, à la Direction des Services Fiscaux, à la Direction des Douanes et à l'Autorité de contrôle prudentiel et de résolution (ACPR) dans le cadre de leurs missions de contrôle et d'inspection, selon la règlementation fiscale en vigueur.

Au vu de ce qui précède, la Commission considère que de telles transmissions sont conformes aux exigences légales.

VI. Sur les interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement fait l'objet de quatre interconnexions avec les traitements ayant respectivement pour finalité « *Gestion du personnel* », « *Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle d'accès au Système d'Information* », « *Mise en place d'un dispositif de surveillance, de détection et d'alerte des menaces internes et externes à la cybersécurité de Barclays Bank PLC* » et « *Traitement des valeurs mobilières et autres instruments financiers* », légalement mis en œuvre.

Il indique par ailleurs un rapprochement entre ce traitement et le traitement ayant pour finalité « *Tenue des comptes de la clientèle* », légalement mis en œuvre.

La Commission relève par ailleurs à l'étude du dossier que ce traitement est interconnecté avec le traitement ayant pour finalité l'accès sécurisé à l'Internet.

Elle considère que ces interconnexions et rapprochements sont conformes aux exigences légales.

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 les durées de conservation

Le responsable de traitement indique que les informations collectées dans le cadre de la messagerie sont conservées 10 ans, à l'exception de la gestion des contacts qui est conservée 3 mois après le départ de l'utilisateur, des logs d'accès et des fichiers journaux qui sont conservés 1 an et des habilitations qui sont conservées 15 mois.

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.

La Commission tient par ailleurs à rappeler que lors du départ définitif d'un salarié sa boite email nominative doit être *« bloquée »* c'est à dire qu'elle ne doit plus pouvoir recevoir d'emails, ni en envoyer, à l'exception d'un message automatique qui sera adressé à chaque personne ayant envoyé un email à l'adresse concernée. Ce message automatique a vocation à informer l'expéditeur de l'email que son interlocuteur ne travaille plus au sein de l'entité, et qu'il devra désormais envoyer ses emails à telle ou telle adresse. Ceci pourra être pratiqué pendant 3 mois au maximum, selon les fonctions et le degré de responsabilité de l'ancien salarié.

Elle rappelle en outre qu'à l'échéance de cette période l'adresse email nominative de l'ancien salarié sera désactivée (supprimée) et que l'employeur doit permettre au salarié de récupérer les emails privés susceptibles de se trouver dans sa boite email nominative professionnelle.

Le responsable de traitement indique par ailleurs que les informations collectées dans le cadre de la prévention des fuites de données sont conservées 1 an, à l'exception des données d'identification électronique et des habilitations qui sont conservées 15 mois.

En ce qui concerne les informations collectées dans le cadre de l'analyse des menaces, les informations liées à l'identité sont conservées 1 an, les informations temporelles, les logs d'accès et les autres données sont conservés 180 jours et les données d'identification électronique et les habilitations sont conservées 15 mois.

Enfin, en ce qui concerne les informations collectées dans le cadre de la détection des malwares, celles-ci sont conservées 14 jours si aucune alerte n'est détectée ou 30 jours si l'email contient des malwares potentiels pour analyse, puis 18 mois sous format agrégé sans conservation du contenu de l'email.

Le responsable de traitement précise à cet effet que suite à cette analyse, le message est soit :

- automatiquement validé si aucune menace n'est identifiée ;
- directement supprimé en cas de menace manifeste ;
- placé en quarantaine et revu manuellement par les équipes Barclays Ops Cyber.

La Commission en prend acte.

Après en avoir délibéré, la Commission :

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

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 en cas de doute que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Rappelle 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 ;

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

- l'information préalable doit s'effectuer auprès de l'ensemble des personnes concernées, à savoir y compris les tiers ;

- la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande ;

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

- l'AMSF 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 chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé ;

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

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 Barclays Bank PLC (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

Robert CHANAS