Délibération n° 2018-103 du 18 juillet 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 de la messagerie électronique utilisée à des fins de surveillance* »

présenté par EFG BANK (MONACO) SAM

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° 1.338 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 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 EFG BANK (MONACO) SAM le 5 avril 2018 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion de la messagerie électronique utilisée à des fins de surveillance* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 4 juin 2018, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 18 juillet 2018 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

EFG BANK (MONACO) SAM est une société monégasque, immatriculée au Répertoire du Commerce et de l'industrie sous le numéro 90S02647, ayant entre autres pour objet de « *faire dans la Principauté de Monaco et à l'étranger, pour elle-même, pour le compte de tiers ou en participation, toutes opérations de banque, de crédit, de financement, d'escompte, de garantie, de détention, de conservation, de dépôt, d'administration, de gestion, de bourse, de courtage, de change, ainsi que toutes opérations d'acquisition, d'offre et de cession de valeurs mobilières, d'effets de commerce, de métaux précieux et d'autres instruments d'investissement et de placement* ».

Dans le cadre de l'exercice de leurs fonctions, les collaborateurs de cette société disposent d'une messagerie professionnelle faisant l'objet d'une surveillance.

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 de la messagerie électronique utilisée à des fins de surveillance ».*

Les personnes concernées sont le « *personnel de EFG (BANK) MONACO SAM* » et « *Toute personne communiquant par email avec EFG BANK (MONACO) SAM* ».

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

- échange de messages électroniques en interne ou avec l'extérieur ;
- historisation des messages électroniques entrants et sortants ;
- gestion des contacts de la messagerie électronique ;
- gestion des dossiers de la messagerie et des messages archivés ;
- établissement et lecture de fichiers journaux ;
- gestion de l'agenda ;
- contrôle du respect des règles professionnelles liées à l'usage de la messagerie électronique professionnelle ;
- analyse des messages électroniques adressés à l'extérieur afin de s'assurer qu'ils ne contiennent aucune information confidentielle ;
- établissement de preuves en cas de litige avec un client/employé (en cas de contestation d'un ordre, etc…) ou de procédure disciplinaire contre un 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 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.

A cet égard, la Commission observe que « *EFG BANK (MONACO) SAM bénéficie, notamment, de l'agrément de la Commission de Contrôle des Activités Financières au titre de l'article 1er de la loi n° 1.338 du 7 septembre 2007 sur les activités financières* » et qu'elle était par conséquent soumise aux dispositions de l'article 23 de cette loi selon laquelle « *les sociétés agréées sont tenues d'observer les règles prudentielles et de bonne conduite définies par ordonnance souveraine* ».

La Commission relève que cette même société est également soumise aux dispositions des articles 6 à 11 de l'Ordonnance Souveraine n°1.284 du 10 septembre 2007, modifiée, qui prévoient notamment que celle-ci doit :

« *disposer d'une organisation administrative et comptable, ainsi que des mécanismes de sécurité et de contrôle interne et externe adéquats, notamment en ce qui concerne les opérations pour compte propre et les opérations personnelles de leurs salariés* » et être structurée et organisée *« de façon à restreindre au minimum tout risque de conflits d'intérêts* » ;

« *respecter des règles de bonne conduite destinées à garantir la protection des investisseurs et la régularité des opérations* » ;

« *s'abstenir de toute initiative qui aurait pour objet ou pour effet de privilégier »* ses intérêts propres au détriment des intérêts de ses clients ;

« *mettre en place une organisation interne adéquate permettant de justifier en détail l'origine et la transmission des ordres* » et « *pour chaque ordre, pouvoir apporter la preuve de la date de la date de sa réception, ainsi que celle de sa transmission* ».

La Commission constate en outre que EFG BANK (MONACO) SAM est également soumise aux dispositions de la Loi n° 1.362 du 3 août 2009.

Par ailleurs, le responsable de traitement indique que le traitement est justifié par la réalisation d'un intérêt légitime poursuivi puisqu'il va lui permettre :

- d'assurer la sécurité et le bon fonctionnement technique du réseau et de son système informatique ;

- de contrôler le respect des règles internes d'usage des outils de communication électronique ainsi que de son règlement intérieur ;

- de préserver ses intérêts économiques, commerciaux et financiers de la banque ;

- de se protéger contre tout acte susceptible d'engager sa responsabilité civile ou pénale, ou de lui porter préjudice ;

- de prévenir les faits illicites.

Le responsable de traitement précise également que les droits et libertés des personnes concernées sont respectés puisque « *EFG BANK (MONACO) SAM tolère l'usage de la messagerie professionnelle à des fins personnelles et s'interdit d'accéder au contenu des messages dont l'objet contient des mots clés tels que « privé », « [PRV] » ou « personnel » afin de ne pas violer le secret de la correspondance privée* ».

A cet égard, la Commission rappelle, conformément à sa délibération n° 2015-111 du 18 novembre 2015, que « *seule une autorisation du juge peut permettre à l'employeur d'accéder licitement aux messages privés de ses employés lorsque ces derniers n'ont pas autorisé l'employeur à lire leurs messages privés, et cela même si l'employeur a des motifs légitimes de suspecter des actes de concurrence déloyale ou toute autre atteinte portée à ses intérêts ou à la Loi* ».

Elle considère donc que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. 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 ;
- informations temporelles : date et heure de réception/envoi de messages ;
- messages : contenu, objet, dossiers de classement ou d'archivage ;
- gestion des contacts : nom, prénom, raison sociale ;
- logs d'accès : logs de connexion des personnes habilitées à avoir accès au traitement ;
- gestion des alertes : réception des alertes en fonction des niveaux hiérarchiques concernés ;
- fichiers journaux : nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format, pièces jointes, noms de domaine expéditeurs de message ;
- 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 administrative des salariés* » ainsi que le présent traitement.

Les informations relatives aux données d'identification électronique, aux informations temporelles, aux logs d'accès, à la gestion des alertes et aux fichiers journaux ont pour origine le système de messagerie.

Concernant les alertes, la Commission considère toutefois qu'elles ont également pour origine le système de détection des fuites de données confidentielles.

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

Enfin, les informations relatives aux habilitations ont pour origine le gestionnaire du 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 personnes concernées est effectuée par le biais d'une page d'information sur le site web de EFG BANK (MONACO) SAM et d'une procédure interne accessible en intranet.

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

Elle rappelle également que cette information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, et notamment les tiers extérieurs.

A cet égard, la Commission recommande l'insertion d'une mention d'information au bas de tout message électronique sortant afin d'informer lesdits tiers de la finalité du traitement, ainsi que de leurs droits.

- ***Sur l'exercice du droit d'accès, de modification et de mise à jour***

Le droit d'accès s'exerce par voie postale ou par courrier électronique auprès du Service Juridique.

S'agissant de l'exercice du droit d'accès par voie électronique, la Commission considère qu'une procédure 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.

Sous cette condition, la Commission constate ainsi que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

V. Sur les personnes ayant accès au traitement et les destinataires

- ***Sur les personnes ayant accès au traitement***

Le responsable de traitement indique que les personnes ayant accès à la messagerie sont :

- le personnel de EFG BANK (MONACO) SAM: chacun pour ce qui le concerne, en inscription, modification et suppression;
- le Service Informatique de EFG BANK (MONACO) SAM: en tant qu'administrateur du système, en inscription, suppression;
- le RSSI de EFG BANK (MONACO) SAM: en consultation, dans un processus d'autorisation stricte et encadré, dans la mesure où ces accès doivent faire l'objet d'une demande spécifique, validée par la Direction, dans le cadre exclusif des vérifications menées concernant les activités de la banque;
- le Contrôle Interne de EFG BANK (MONACO) SAM: en consultation, dans un processus d'autorisation stricte et encadré, dans la mesure où ces accès doivent faire l'objet d'une demande spécifique, validée par la Direction, dans le cadre exclusif des vérifications menées concernant les activités de la banque;
- le personnel technique du Groupe EFG BANK, situé en dans les locaux de EFG BANK en Suisse et à Monaco, en charge de la maintenance du système d'information: accès dans le cadre exclusif de sa fonction liée au fonctionnement et à la sécurité du système.

Le responsable de traitement précise par ailleurs que « *Les informations de détection de données confidentielles sont accessibles via :*

- *Une notification sur le poste de travail de l'utilisateur concerné*

- *Des alertes envoyées par email*
  - *Au RSSI de EFG Bank (Monaco)*
  - *Au service conformité de EFG Bank (Monaco)*
  - *Au gestionnaire de EFG Bank (Monaco) en charge du client concerné*

- *Des rapports hebdomadaires envoyés par email, contenant uniquement des statistiques sans aucune donnée nominative*
  - *Au RSSI de EFG Bank (Monaco)*
  - *Au service conformité de EFG Bank (Monaco)*

- *Dans une console, accessible sur un serveur sécurisé*
  - *Au RSSI de EFG Bank (Monaco)*
  - *Au service conformité de EFG Bank (Monaco)* ».

Enfin, la Commission constate que « *Les équipes informatiques et techniques de EFG Bank (Monaco) ont accès à la fonctionnalité de détection des fuites de données confidentielles en tant qu'administrateur de ce système uniquement dans le cadre exclusif de sa fonction liée au fonctionnement et à la sécurité du système. Les équipes informatiques de EFG Bank Genève peuvent accéder à ce système, dans le cadre exclusif de leurs fonctions liées au fonctionnement et à la sécurité du système, uniquement sous la supervision d'un membre des équipes informatiques de EFG Bank (Monaco)* ».

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

La Commission rappelle toutefois qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993 la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

- ***Sur les destinataires***

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

La Commission considère que le Service d'Information et de Contrôle des Circuits Financiers (SICCFIN) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires d'informations nominatives traitées.

Par ailleurs, elle estime que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, la Commission rappelle qu'en cas de transmission, ces Autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

Elle considère donc que de telles transmissions sont conformes aux exigences légales.

VI. Sur les rapprochements et interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion avec le traitement ayant pour finalité « *Gestion administrative des salariés* » ; traitement légalement mis en œuvre.

Il appert par ailleurs, à l'étude du dossier, une interconnexion avec un traitement ayant pour finalité « *Gestion des services de téléphonie fixe et mobile sur le lieu de travail* » ; traitement 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 les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

Elle rappelle également 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 enfin 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

Les informations relatives à l'identité, aux données d'identification électronique, à la gestion des contacts et aux habilitations sont conservées 3 mois après le départ de l'employé.

Les logs d'accès et les fichiers journaux sont conservés 1 an.

Les informations relatives à une alerte sont conservées 1 an à compter du traitement de ladite alerte.

Enfin, les informations relatives aux messages et aux informations temporelles de ces messages sont conservées 5 ans.

A cet égard, la Commission demande, conformément à sa délibération n° 2015 -111 du 18 novembre 2015, qu'une politique d'archivage soit mise en place jusqu'à ce que la conservation desdits messages ne soit plus nécessaire.

Après en avoir délibéré, la Commission :

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 :

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

- l'information des personnes concernées doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, et notamment les tiers extérieurs ;

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

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

- les Autorités judiciaires ne peuvent être destinataires des informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort ;

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

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

Demande qu'une politique d'archivage soit mise en place jusqu'à ce que la conservation des 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 EFG BANK (MONACO) SAM du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la messagerie électronique utilisée à des fins de surveillance* ».**

Le Président

Guy MAGNAN