

Délibération n° 2017-027 du 15 mars 2017

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 Corporation Financière Européenne 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 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 Corporation Financière Européenne SAM le 5 décembre 2016 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 3 février 2017, 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 15 mars 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Corporation Financière Européenne (CFE) est une société monégasque, immatriculée au Répertoire du Commerce et de l'industrie sous le numéro 14S06286, ayant pour objet « *la réception et la transmission d'ordres sur les marchés financiers, portant sur des valeurs mobilières ou des instruments financiers à terme, pour le compte de tiers* » ainsi que « *le conseil et l'assistance dans la réception et la transmission d'ordres sur les marchés financiers, portant sur des valeurs mobilières ou des instruments financiers à terme, pour le compte de tiers* ».

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

Les personnes concernées sont le personnel de CFE SAM ainsi que toute personne contactant la société par courrier électronique.

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 des habilitations d'accès à la messagerie ;
- contrôle du respect des règles professionnelles liées à l'usage de la messagerie professionnelle ;
- établissement de preuves en cas de litige avec un client/employé (en cas de contestation d'un ordre, etc..).

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 23 de la Loi n°1.338 du 7 septembre 2007 stipule que « *les sociétés agréées sont tenues d'observer les règles prudentielles et de bonne conduite définies par ordonnance souveraine* ».

Par ailleurs, les articles 6 à 11 de l'Ordonnance Souveraine n°1.284 du 10 septembre 2007 stipulent que ces sociétés doivent :

« *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 structurées et organisées 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 régularités des opérations* » ;

« *s'abstenir de toute initiative qui aurait pour objet ou pour effet de privilégier leurs intérêts propres au détriment des intérêts de leurs 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 sa réception, ainsi que de celle de sa transmission* ».

Enfin, 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 qui « *ne méconnaît 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° 1.338 du 7 septembre 2007 et n° 1.362 du 3 août 2009.

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

- 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 se protéger contre tout acte susceptible d'engager sa responsabilité civile ou pénale, ou de lui porter préjudice ;
- de prévenir la réalisation de faits illicites.

Le responsable de traitement précise également que les droits et libertés des personnes concernées sont respectés puisque l'usage de la messagerie professionnelle à des fins personnelles est toléré et qu'il est interdit d'accéder aux messages dont l'objet contient des mots clés tels que « *privé* », « *[PRV]* » 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

Les informations nominatives traitées sont :

- identité : nom, prénom, identifiant ;
- données d'identification électronique : adresse de messagerie électronique ;
- messages : contenu, objet, dossiers de classement ou d'archivage ;
- informations temporelles : date, heure ;
- gestion des contacts : nom, prénom, raison sociale ;
- 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.

Le responsable de traitement indique que les informations relatives à l'identité ont pour objet le dossier papier des Ressources Humaines.

Les informations relatives aux données d'identification électronique, aux informations temporelles, aux logs d'accès, aux fichiers journaux et aux habilitations ont pour origine le gestionnaire du système.

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

Aussi, la Commission considère 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 du personnel se fait par le biais d'un document spécifique.

Ce document n'ayant pas été joint à la demande, la Commission rappelle à cet égard que celui-ci doit impérativement informer les personnes concernées de la finalité du traitement, ainsi que de leurs droits conformément 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.

Enfin, concernant les tiers extérieurs, elle prend acte des précisions du responsable de traitement selon lesquelles une mention d'information sera insérée au bas de tout message électronique sortant afin d'informer lesdits tiers de la finalité du traitement, ainsi que de leurs droits.

La Commission considère donc que les modalités d'information préalable sont conformes aux dispositions de l'article 14 de la Loi n° 1.165, modifiée.

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

Le droit d'accès s'exerce par voie postale. La réponse à ce droit d'accès s'exerce selon les mêmes modalités.

Le délai de réponse à une demande de droit d'accès est de 30 jours.

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

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

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

Les personnes habilitées à avoir accès au traitement sont :

- les employés : en création et consultation pour l'usage de leur compte de messagerie ;
- le Compliance Officer : en consultation ;
- l'Administrateur Délégué : en consultation ;
- les prestataires dans le cadre exclusif de leurs fonctions liées au fonctionnement et à la maintenance du système.

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

En ce qui concerne les prestataires, la Commission rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service. De plus, lesdits prestataires sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

Elle 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 judiciaires et policières dans le cadre de leurs missions légalement conférées.

La Commission estime que la communication aux autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, elle 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 par ailleurs 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 des informations nominatives traitées.

VI. 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 relève néanmoins que l'architecture technique repose sur des équipements de raccordement (switchs, routeurs, pare-feux) de serveurs et périphériques qui doivent être protégés par un login et un mot de passe réputé fort et que les ports non utilisés doivent être désactivés.

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.

VII. Sur la durée de conservation

Le responsable de traitement indique que les informations relatives à l'identité, aux données d'identification électronique, à la gestion des contacts et aux habilitations sont conservées 3 mois maximum après le départ de l'utilisateur.

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

Enfin, les messages et les informations temporelles sont conservés 5 ans.

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

Après en avoir délibéré, la Commission :

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

Rappelle que :

- l'information 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 ;
- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit lui être communiquée à première réquisition ;
- les autorités judiciaires ne peuvent avoir accès aux informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;
- les équipements de raccordement (switchs, routeurs, pare-feux) de serveurs et périphériques doivent être protégés par un login et un mot de passe réputé fort et que les ports non utilisés doivent être désactivés ;
- la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

Recommande :

- si cela n'est déjà fait, la mise en place d'une charte informatique pour informer les collaborateurs de la société de leurs droits et obligations ;
- 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.

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 Corporation Financière Européenne du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la messagerie électronique utilisée à des fins de surveillance* ».**

Le Président

Guy MAGNAN