Délibération n° 2021-074 du 21 avril 2021

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle* »

présenté par Edmond de Rothschild Assurances et Conseils

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° 1.362 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° 2.318 du 3 août 2009, modifiée, 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, modifiée ;

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 Edmond de Rothschild Assurances et Conseils le 10 février 2021 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 et de contrôle »* ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 8 avril 2021, 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 21 avril 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Société Edmond de Rothschild Assurances et Conseils (Monaco) (EDRAC), immatriculée au RCI sous le n° 05S04415, a notamment pour activité « *[…] le courtage de contrats d'assurance vie (à l'exclusion d'autres formes d'assurance), tous conseils et services relatifs à la structuration de patrimoine de toutes personnes physiques ou morales, à l'organisation et à l'administration de sociétés ou de toute autre activité analogue et d'une manière générale, l'ingénierie financière […]* ».

Ladite société est une filiale de la banque Edmond de Rothschild (Monaco) qui a mis à sa disposition un ensemble de ressources humaines, logistiques et informatiques, dont une messagerie professionnelle faisant l'objet d'une supervision, dans le cadre d'une convention de service entre les deux entités.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance. Il relève donc du régime de l'autorisation préalable visé à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Ce traitement a pour finalité « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle ».*

Les personnes concernées sont les employés, les clients et les tiers.

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

- l'échange de messages électroniques en interne ou avec l'extérieur ;
- l'établissement d'un historique 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 sortants ;
- l'établissement de preuves en cas de litige avec un client/employé.

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 impose aux organismes assujettis d'exercer une vigilance constante à l'égard de la relation d'affaires notamment 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 de la Loi 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 :

- 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 société ;
- 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 « *le contrôle de l'utilisation des messageries électroniques professionnelles est réalisé dans le respect de la correspondance privée* » et que seront considérés comme privés les messages « *comportant, à l'émission ou à la réception, une des mentions suivantes dans l'objet : Personnel ou Privé* ».

Enfin, la Commission relève que les personnels chargés de la supervision des moyens de communication électronique, et du contrôle de l'utilisation des messageries électroniques, « *sont tenus par un devoir de confidentialité* » et que dans ce cadre, « *ils ne doivent divulguer aucune information, et encore moins celles couvertes par le secret de la correspondance privée ou qui relèvent de la vie privée des employés* ».

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

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

III. Sur les informations nominatives traitées

Les informations nominatives traitées sont :

- identité : nom, prénom, identifiant ;
- données d'identification électronique : adresse de messagerie électronique ;
- messages : contenu de la messagerie et des messages, objet, dossiers de classement et d'archivage, pièces jointes ;
- gestion des contacts : nom, prénom, raison sociale ;
- informations temporelles : date et heure de réception/envoi de messages ;
- logs d'accès : identifiants de connexion, 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, (…) ;
- gestion des alertes : réception des alertes automatiques DLP ;
- habilitations : identité des personnes habilitées à avoir accès au système de messagerie DLP, type de droits conférés, historisation des habilitations.

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

Les informations relatives aux données d'identification électronique, aux messages, à la gestion des contacts et aux informations temporelles ont pour origine le compte de messagerie.

Enfin, les logs d'accès, les fichiers journaux, les alertes et les habilitations sont générés par le 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 se fait par le biais d'une mention ou clause intégrée dans un document remis à l'intéressé, d'une procédure interne accessible en Intranet et d'une mention d'information en bas de tout message électronique sortant.

A l'analyse de ces documents, la Commission considère que les modalités d'information préalable des personnes sont conformes aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

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

Le droit d'accès s'exerce par voie postale auprès du Service Conformité de la banque Edmond de Rothschild (Monaco) pour les clients et les tiers, et auprès du Chief Operating Officer de la banque Edmond de Rothschild (Monaco) pour les collaborateurs.

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*

Les personnes habilitées à avoir accès au traitement sont :

- les utilisateurs de la messagerie et les délégataires habilités par les utilisateurs eux-mêmes : en inscription, modification et consultation ;
- les administrateurs système du Service Informatique local de la banque Edmond de Rothschild (Monaco) : en inscription, modification et consultation dans le strict cadre de l'accomplissement de leurs missions de contrôle, techniques et de maintenance système ;
- le Responsable de la sécurité des systèmes d'information (RSSI) de la banque Edmond de Rothschild (Monaco) et les personnes habilitées de son service : en inscription, modification et consultation dans le strict cadre de l'accomplissement de leurs missions de contrôle, techniques et de maintenance système ;
- les membres du service support de la Direction des systèmes d'information (traitement des outils de filtrage) de la banque Edmond de Rothschild (Monaco): en inscription, modification et consultation dans le strict cadre de l'accomplissement de leurs missions de contrôle, techniques et de maintenance système.

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

La Commission prend acte des précisions du responsable de traitement selon lesquelles « *Afin d'assurer la continuité des affaires d'Edmond de Rothschild Assurances et Conseils, la messagerie professionnelle d'un employé absent (congés ou maladie) pourra être consultée par un suppléant, à qui l'employé aura donné préalablement les droits d'accès en lecture seule à sa messagerie. Le consentement des collaborateurs concernés se déduit des droits qu'ils accordent eux-mêmes à d'autres collaborateurs dont ils ont connaissance de l'identité. Par ailleurs, ces collaborateurs sont tenus par un devoir de confidentialité, et ne doivent divulguer aucune information couverte par le secret de la correspondance privée ou qui relèvent de la vie privée des employés* ».

La Commission constate par ailleurs qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993 la liste nominative des personnes ayant accès au traitement est tenue à jour, et rappelle 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* » qui a été légalement mis en œuvre.

Il appert par ailleurs une interconnexion avec un traitement lié à la « *base de données clients* ».

La Commission rappelle à cet égard que toute interconnexion ne peut avoir lieu qu'entre des traitements légalement mis en œuvre et demande que celui-ci lui soit soumis dans les plus brefs délais s'il n'a pas déjà fait l'objet des formalités légales auprès d'elle.

VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation particulière.

La Commission rappelle néanmoins que les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

Elle rappelle que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception, conformément à la délibération n° 2015-111 du 18 novembre 2015.

La Commission rappelle également que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

VIII. Sur la durée de conservation

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

Les messages, les informations temporelles, les fichiers journaux et les habilitations sont archivés jusqu'à ce que la conservation de ces informations ne soit plus nécessaire.

Enfin, les logs d'accès et les alertes sont conservés 1 an maximum.

Après en avoir délibéré, la Commission :

Rappelle que :

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

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

- les Autorités judiciaires ne peuvent avoir accès aux informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- toute interconnexion ne peut avoir lieu qu'entre des traitements légalement mis en œuvre ;

- 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.

Demande que le traitement relatif à la *« base de données clients »* lui soit soumis dans les plus brefs délais s'il n'a pas déjà fait l'objet des formalités légales auprès d'elle.

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 Edmond de Rothschild Assurances et Conseils du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle* ».**

Le Président

Guy MAGNAN