Délibération n° 2022-156 du 16 novembre 2022

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 la Banque J. Safra Sarasin (Monaco) SA

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 déclaration ordinaire déposée par la Banque J. Safra Sarasin (Monaco) le 20 mars 2017 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion de la messagerie électronique professionnelle* », et dont il a été délivré récépissé le 18 avril 2017 ;

Vu la demande d'autorisation déposée par la Banque J. Safra Sarasin (Monaco) SA le 16 septembre 2022 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 le rapport de la Commission de Contrôle des Informations Nominatives en date du 16 novembre 2022 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Banque J. Safra Sarasin (Monaco) SA est enregistrée au RCI sous le numéro 89S02557, ayant pour activité la réalisation de *« toutes opérations de banque pour elle-même, pour le compte de tiers ou en participation et notamment sans que cette énumération soit limitative, des opérations financières, de crédit, d'escompte, de bourse ou de change de gestion de patrimoine, ainsi que toutes opérations annexes ou connexes et celles généralement quelconques nécessaires à la réalisation de l'objet social »*.

Le 20 mars 2017 cette société a déclaré à la Commission un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la messagerie électronique professionnelle* ». La Commission a émis un récépissé de mise en œuvre de ce traitement le 18 avril 2017.

La Banque J. Safra Sarasin (Monaco) SA souhaite modifier ce traitement afin de mettre en place une procédure de contrôle du contenu des messages sortants.

Le traitement objet de la présente demande étant désormais 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 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 en externe ;
- 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 ;
- l'établissement de preuves en cas de litige avec un client/employé ;
- la mise en place d'une procédure de contrôle graduée ;
- le contrôle au moyen d'un logiciel d'analyse du contenu des messages sortants.

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 :

- 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 conformément à la règlementation monégasque* ».

La Commission relève ainsi que l'utilisation des courriers électroniques à usage privé (personnel) est autorisée à condition d'être limitée à son strict minimum.

Elle note qu'« *Il est recommandé aux salariés de mentionner « Privé » ou « Private » ou « Personnel » ou « Personnal » dans l'objet des mails envoyés à chaque fois que l'envoi n'est pas à caractère professionnel* ».

A cet égard, la Commission rappelle, conformément à sa délibération n° 2015-111 du 18 novembre 2015, que l'employeur ne peut accéder aux contenus des messages privés de ses employés envoyés ou reçus à partir de la messagerie professionnelle, sans que ledit employé soit présent et avec son accord et 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

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 ;
- habilitations : identité des personnes habilitées à avoir accès à la messagerie, type de droits conférés, historisation des habilitations ;
- gestion des alertes : réception des alertes automatiques DLP.

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

Par ailleurs, les logs d'accès, les fichiers journaux, les habilitations et les alertes ont pour origine 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 s'effectue par le biais d'une mention ou clause particulière intégrée dans un document remis à l'intéressé et par une procédure interne accessible en Intranet.

A cet égard, la Commission rappelle que ces documents doivent comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Elle prend acte par ailleurs qu'une mention d'information a été insérée au bas de tout message électronique sortant afin d'informer les 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 auprès du Service Conformité pour les clients et les tiers, et du Président de la Direction Générale pour les salariés.

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 : tous droits sur leur propre messagerie ;
- les supérieurs hiérarchiques des personnes concernées par le traitement : consultation ;
- les agents habilités par le propriétaire de la messagerie lui-même : consultation ;
- les administrateurs système du Service Informatique du Groupe (Suisse) : tout accès dans le cadre de l'accomplissement de leurs missions techniques et de maintenance système ;
- le RLS (Responsable local de sécurité) et le LSO (Local Private Officer) : sollicitation, consultation et modification en cas d'alertes.

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 les messageries du personnel « *sont individuelles et ne peuvent pas être consultées par un autre employé sans l'accord de l'utilisateur* » et que « *Même lors d'une absence prévue d'un salarié, sa boite mail ne peut pas être consultée, sauf si celui-ci donne son accord à son responsable. En aucun cas, les emails reçus sur sa boite ne peuvent être redirigés vers l'adresse d'un autre collègue* ».

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 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* ».

La Commission relève par ailleurs que ce traitement fait l'objet d'une interconnexion avec le traitement ayant pour finalité « *Gestion des téléphonies fixes et mobiles sur le lieu de travail* ».

La Commission constate que ces deux traitements ont été 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 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 relatives à l'identité, aux données d'identification électronique et à la gestion des contacts sont conservées 1 mois maximum après le départ de l'employé.

Les informations temporelles, les logs d'accès, les fichiers journaux, les habilitations et les alertes sont conservés 1 an maximum.

Enfin, les messages, sont archivés jusqu'à ce que la conservation de ces informations ne soit plus nécessaire.

La Commission tient toutefois 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.

Après en avoir délibéré, la Commission :

Constate que la liste nominative des personnes ayant accès au traitement est tenue à jour.

Rappelle que :

- l'information préalable doit 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 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 ;

- 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.

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 Banque J. Safra Sarasin (Monaco) SA 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