Délibération n° 2023-100 du 19 juillet 2023

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 électronique professionnelle à des fins de surveillance et de contrôle* »

présenté par Bank Julius Baer (Monaco) S.A.M.

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 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° 2014-159 du 12 novembre 2014 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* » présenté par la Bank Julius Baer (Monaco) SAM ;

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 Bank Julius Baer (Monaco) S.A.M. le 18 avril 2023 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion et supervision de la messagerie électronique 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 15 juin 2023, 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 19 juillet 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Bank Julius Baer (Monaco) S.A.M. est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 96S03173, ayant entre autres pour objet *« en Principauté de Monaco et à l'étranger, pour son compte ou le compte de tiers, directement ou en participation : La réalisation de toutes opérations de banque ou connexes telles que définies par la "loi bancaire" applicable* ».

Par délibération n° 2014-159 en date du 12 novembre 2014, la Commission avait autorisé la mise en œuvre d'un traitement automatisé des informations nominatives ayant pour finalité « *Système et supervision de la messagerie professionnelle »*. Les modalités d'exploitation de ce traitement ayant évolué, le responsable de traitement souhaite aujourd'hui remplacer le traitement initial par le présent traitement.

La Commission en prend acte.

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 électronique professionnelle à des fins de surveillance et de contrôle ».*

Les personnes concernées sont les employés, les clients, les prospects 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 ;
- 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* » par l'exécution du contrat de travail qui lie le responsable de traitement et le salarié, 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 n° 1.362 du 3 août 2009, ainsi que de l'Arrêté 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 puisqu'il est demandé aux employés d'identifier les mails privés avec une mention dans le sujet telle que « *Personnel* » ou « *Privé* ».

La Commission prend ainsi note que le « *système de « DLP » ne va enregistrer que les mails soumis à une alerte (contenant a minima un rapprochement avec 1 numéro de compte + le nom du titulaire du compte*) » et que *« Dans le cadre d'une discussion personnelle, il n'y a donc aucune alerte et donc aucun enregistrement* » dans le système.

Elle constate également que dans le cas où un mail est identifié comme « *personnel* » (ou assimilé) mais contient des concordances avec des numéros de compte ou des informations sensibles des clients « *ce mail pourra être analysé avec l'accord de l'utilisateur. Si ce dernier ne donne pas son accord, une demande est remontée* » au DPO et au département juridique.

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 condition, 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, dénomination sociale, photo d'identité (uniquement via l'annuaire interne) ;
- données d'identification électronique : adresse de messagerie électronique ;
- adresses et coordonnées : adresse professionnelle, numéros professionnels (fixe, mobile, fax) ;
- formation, diplômes, vie professionnelle : compagnie, fonction, supérieur hiérarchique, et membres de l'équipe (uniquement via l'annuaire interne) ;
- caractéristiques financières : désignation du compte et numéro de compte, destinataire des opérations effectuées ;
- gestion des contacts : nom, prénom, numéro de téléphone professionnel, raison sociale ;
- informations temporelles : date et heure de réception/envoi de messages ;
- messages : contenu de la messagerie et des messages, objet, dossiers de classement et d'archivage, pièces jointes ;
- logs d'accès : identifiants de connexion, logs de connexion des personnels habilités ;
- 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 DLP « *Data Loss Prevention* ».

Le responsable de traitement indique que les informations ont pour origine « *Tout écrivant (dans le cadre des communications échangées)* », à l'exception des logs d'accès et des fichiers journaux qui ont pour origine le système.

La Commission considère toutefois que les informations relatives à l'identité, aux données d'identification électronique, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle ainsi que les caractéristiques financières et la gestion des contacts peuvent avoir pour origine les traitements ayant pour finalité « *Gestion administrative des salariés* » et « *Gestion et supervision des droits et habilitations* » ainsi que tout écrivant dans le cadre des communications échangées.

Les informations temporelles et les messages ont pour origine tout écrivant dans le cadre des communications échangées.

Les logs d'accès et les fichiers journaux ont pour origine les systèmes.

Enfin, la Commission considère que la gestion des alertes a pour origine le système DLP.

Elle constate 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***

L'information préalable des personnes concernées s'effectue par le biais d'un document spécifique, d'une mention ou clause particulière intégrée dans un document remis à l'intéressé et d'une procédure interne accessible en Intranet.

A cet égard, la Commission rappelle que 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.

Elle rappelle également que cette information préalable doit s'effectuer auprès de l'ensemble des personnes concernées, à savoir y compris les tiers.

Aussi, 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 auprès du Directeur Juridique et Data Protection Office.

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 :

- les utilisateurs de la messagerie : tous droits sur leur propre messagerie ;
- les agents habilités (délégation) par le titulaire du compte de messagerie (boite aux lettres) : selon l'habilitation accordée ;
- les administrateurs système du Service Informatique du Groupe : tous droits dans le strict cadre de l'accomplissement de leur mission technique et de maintenance du système ;
- l'équipe en charge des alertes et contrôle à Monaco (équipes locales IT et Risk Management) : sollicitation, consultation et modification en cas d'alertes ;
- l'équipe du « *SOC* » Suisse : tous droits, limités aux journaux (analyse des logs et flux) dans le cadre de la prévention numérique ;
- l'équipe en charge des alertes de la filiale du Groupe sise à Singapour, dans le cadre des échanges entre ses salariés et ceux de Bank Julius Baer Monaco. Une remontée d'informations est possible dans le système de monitoring Data Loss Prevention de Singapour : sollicitation, consultation et modification en cas d'alertes ;
- GIA « *Global Internal Audit* » : consultation uniquement dans le cadre d'une présomption sérieuse de violation des règles de conduite.

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

La Commission précise toutefois que les accès par l'équipe en charge des alertes de la filiale du Groupe sise à Singapour seront analysés dans la demande d'autorisation de transfert concomitamment soumise.

Elle rappelle 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 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 dument habilitées.

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.

La Commission 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 de trois interconnexions avec les traitements ayant respectivement pour finalité « *Gestion administrative des*

salariés », « *Tenue des comptes de la clientèle et le traitement des informations s'y rattachant par les établissements bancaires et assimilés* » et « *Gestion et supervision des droits et habilitations* ».

La Commission constate que ces 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, aux adresses et coordonnées, à la formation, aux diplômes, à la vie professionnelle ainsi que les caractéristiques financières et la gestion des contacts sont conservées 1 mois après le départ de l'employé.

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

Les messages et les informations temporelles sont conservés 7 ans maximum.

A cet égard, la Commission reconnait que les messages électroniques des collaborateurs peuvent être conservés durant plusieurs années notamment en ce qui concerne les établissements bancaires et assimilés à des fins de traçabilité des opérations financières, ou en cas de soupçons d'activités illicites.

Elle considère ainsi que les messages récents peuvent être stockés dans la messagerie interne du collaborateur pendant une période n'excédant pas 3 ans maximum (archives courantes) puis être automatiquement déplacés afin d'être conservés en archives intermédiaires le temps nécessaire avant d'être placés en archives définitives avec un accès possible sur demande.

Enfin, le responsable de traitement indique que les alertes sont conservées 5 ans à compter de la réception de l'alerte.

La Commission en prend acte mais demande toutefois que les données relatives à un évènement ne mettant pas en lumière un incident (faux positifs par exemple) soient immédiatement supprimées après analyse.

Après en avoir délibéré, la Commission :

Précise que les accès aux alertes par l'équipe en charge des alertes de la filiale du Groupe sise à Singapour seront analysés dans la demande d'autorisation de transfert concomitamment soumise.

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 :

- 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 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.

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 que, s'agissant des alertes générées, les données relatives à un évènement ne mettant pas en lumière un incident (faux positifs par exemple) soient immédiatement supprimées après analyse.

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 Bank Julius Baer (Monaco) S.A.M. du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie électronique professionnelle à des fins de surveillance et de contrôle* ».**

Le Président

Guy MAGNAN