

**DELIBERATION N° 2014-159 DU 12 NOVEMBRE 2014 DE LA COMMISSION DE CONTROLE
DES INFORMATIONS NOMINATIVES AUTORISATION A LA MISE EN ŒUVRE DU TRAITEMENT
AUTOMATISE D'INFORMATIONS NOMINATIVES AYANT POUR FINALITE « *GESTION ET
SUPERVISION DE LA MESSAGERIE PROFESSIONNELLE* » PRESENTE PAR
LA BANK JULIUS BAER (MONACO) SAM**

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention n° 108 du Conseil de l'Europe 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 d'administration d'instruments financiers ;

Vu la Loi n° 1.338 du 7 septembre 2007 sur les activités financières et son Ordonnance d'application ;

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° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, susvisée ;

Vu 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 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

Vu l'Ordonnance Souveraine n° 4.104 du 26 décembre 2012 modifiant 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 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° 2012-119 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 professionnelle* » utilisés à des fins de contrôle de l'activité des employés ;

Vu la demande d'autorisation reçue le 2 octobre 2014 concernant la mise en œuvre par la Bank Julius Baer (Monaco) SAM d'un traitement automatisé ayant pour finalité « *Gestion de la messagerie professionnelle* » ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 12 novembre 2014 portant examen du traitement automatisé susvisé ;

La Commission de Contrôle des Informations Nominatives,

Préambule

La Bank Julius Baer (Monaco) SAM, immatriculée au RCI sous le numéro 96 S 03173, a notamment pour objet « *la réalisation de toutes opérations de banque ou connexes telles que définies par la « loi bancaire » applicable [...]* ».

Dans le cadre de l'exercice de leurs fonctions, les collaborateurs de cet établissement bancaire disposent d'une messagerie professionnelle.

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, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Gestion de la messagerie professionnelle* ».

Les personnes concernées sont « *les employés, clients et tout utilisateur de la messagerie électronique (expéditeurs et destinataires des messages)*. »

Enfin, les fonctionnalités du traitement sont les suivantes :

- « *échange de messages électroniques en interne ou avec l'extérieur ;*
- *établissement d'un historique 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 des fichiers journaux ;*
- *gestion des habilitations d'accès à la messagerie ;*
- *mise en place d'une procédure de contrôle graduée ;*
- *en cas de litige, contrôle par certains départements uniquement ;*
- *établissement de preuves en cas de litige avec un client/employé (en cas de contestation d'un ordre, etc..).* »

Considérant les fonctionnalités du traitement, la Commission rappelle que tout traitement d'informations nominatives doit avoir une finalité « *déterminée, explicite et légitime* » aux termes de l'article 10-1 de la loi n° 1.165, susmentionnée.

A cet égard, la finalité du présent traitement doit être plus explicite et mettre en évidence l'objectif recherché par le responsable de traitement, soit celui superviser la messagerie professionnelle mise à disposition des collaborateurs de la banque.

Par conséquent, elle considère que la finalité du traitement en objet doit être modifiée par « *Gestion et supervision de la messagerie professionnelle* ».

II. Sur la licéité et la justification du traitement

➤ *Sur la licéité du traitement*

Aux termes de l'article 11-1 de la loi n° 1.165, modifiée, les traitements « *mis en œuvre à des fins de surveillance* » ou « *portant sur des soupçons d'activités illicites, des infractions* », doivent pour être licites, être « *nécessaires à la poursuite d'un objectif légitime essentiel et [respecter] les droits et libertés mentionnés à l'article premier des personnes concernées (...)* ».

Dans sa délibération n° 2012-119 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle* » utilisés à des fins de contrôle de l'activité des employés, la Commission rappelle que conformément au principe de proportionnalité, le responsable de traitement est tenu de mettre en place une procédure de contrôle graduée, adaptée aux divers niveaux de risques auxquels il est confronté.

A cet égard, le responsable de traitement a annexé à la présente demande d'autorisation un exemplaire du « *Code of Conduct for Email and Internet Use* » relatif à l'utilisation des outils internet et de messagerie.

Il appert de l'analyse de ce document que la Bank Julius Baer (Monaco) SAM détaille effectivement les conditions d'utilisation de ce système, ainsi que la procédure de contrôle graduée, allant de la surveillance globale non nominative de l'usage de la messagerie au contrôle nominatif du contenu des messages électroniques, décomposée comme suit :

- phase 1 : le contrôle non nominatif global des fichiers journaux de la messagerie (ex. nombre de messages envoyés, format des pièces jointes, volumes, etc.) ;
- phase 2 : le contrôle des fichiers journaux des messageries d'un ou plusieurs employés déterminés ;
- phase 3 : le contrôle du contenu des communications électroniques (archivées ou non) d'un ou plusieurs employés déterminés ou déterminables, sélectionnés aléatoirement (échantillonnage) ou par filtrage automatique ;
- phase 4 : le contrôle du contenu des communications électroniques (archivées ou non) d'un ou plusieurs employés déterminé(s).

La Commission observe que cette procédure est conforme à sa délibération n° 2012-119, précitée.

Elle prend acte des précisions du responsable de traitement selon lesquelles « *la messagerie est réservée à un usage professionnel* » et indiquant que la banque ne peut avoir accès au contenu de la messagerie privée installée sur le téléphone professionnel du collaborateur.

Enfin, elle observe l'existence d'une procédure d'habilitation d'accès à la messagerie professionnelle en cas d'absence temporaire ou définitive d'un salarié de Bank Julius Baer (Monaco) SAM.

La Commission considère que le traitement est licite, conformément à l'article 10-1 de la loi n° 1.165, modifiée.

➤ **Sur la justification**

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 ce traitement permet au responsable de traitement de respecter les obligations découlant des lois n° 1.338 du 7 septembre 2007 sur les activités financières, n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers, et de 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.

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

- 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, du règlement intérieur (code de conduite, d'utilisation de la messagerie électronique et d'internet signé par les employés) ;
- la protection contre tout acte susceptible d'engager la responsabilité civile ou pénale de la Bank Julius Baer (Monaco) SAM, ou de lui porter préjudice ;
- la prévention de la fraude.

La Commission relève que les éléments susmentionnés sont de nature à répondre aux obligations légales précédemment énumérées.

Au vu de ce qui précède, elle considère que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la loi n° 1.165, modifiée.

III. Sur les informations nominatives traitées

Les informations nominatives traitées sont les suivantes :

- identité : nom, prénom, nationalité, dénomination sociale, désignation du compte et numéro de compte, identité des personnes habilitées à avoir accès à la messagerie, destinataire des opérations effectuées ;
- situation de famille : situation de famille ;
- adresses et coordonnées : entité d'appartenance du personnel concerné de la banque, adresse, coordonnées (téléphone, mail, fax) ;
- formation-diplômes/vie professionnelle : profession, formation, diplômes, fonction professionnelle/grade (*ranking*) ;
- caractéristiques financières : portefeuille, numéro de compte, coordonnées bancaires RIB IBAN BIC (y compris celles du destinataire des opérations effectuées) ;
- consommation de biens et services : achat/vente sur les marchés boursiers, achat de biens chez les fournisseurs ou autres ;
- données d'identification électronique : contact et adresse mail, logs de connexion des personnes habilitées à avoir accès au traitement et traçabilité, type de droits conférés ;
- messages : contenu, objet, dossiers de classement et d'archivage, date et heure ;
- fichiers journaux : nombre de messages entrants et sortants, de messages nettoyés, de spams, volume, format, pièces jointes, nom de domaine, expéditeurs de messages, historisation des habilitations.

A l'analyse des éléments susmentionnés, la Commission considère que les « *contacts et adresse mail* » renseignées comme étant des données d'identification électronique sont des éléments relatifs aux « *adresses et coordonnées* ».

Ainsi, les informations relatives à l'identité, à la situation de famille, aux adresses et coordonnées, à la formation-diplômes/vie professionnelle, aux caractéristiques financières, aux messages et à la consommation de biens et services ont pour origine le collaborateur, le client ou le destinataire de l'email dans le cadre de l'échange de correspondances.

Par ailleurs, les informations relatives aux données d'identification électronique et aux fichiers journaux sont générées par le système informatique.

La Commission considère que ces informations 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, modifiée.

IV. Sur les droits des personnes concernées

➤ *Sur l'information des personnes concernées*

Le responsable de traitement indique que l'information préalable des collaborateurs est effectuée par le biais d'un document spécifique (« *le Code of Conduct for Email and Internet Use* »), d'une procédure interne accessible en Intranet et d'une mention dans le disclaimer pour tous les emails sortants.

Après étude de ces documents annexés à la présente demande d'autorisation, la Commission relève qu'ils ne font pas référence à l'article 14 de la loi n° 1.165, modifiée, notamment en ne mentionnant pas l'existence d'un droit d'accès.

La Commission demande donc à ce que ces derniers soient impérativement complétés conformément aux exigences légales susmentionnées.

Sous cette condition, elle considère 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 des personnes concernées*

Les droits d'accès, de modification, de mise à jour et de suppression s'exercent par courrier électronique, par voie postale et sur place auprès du Service Informatique (IT) à Monaco.

Le délai de réponse est de 30 jours.

La Commission considère 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, modifiée.

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

➤ *Sur les destinataires*

Les destinataires des informations sont la Direction de la Sûreté Publique et le SICCFIN.

La Commission considère que la communication à la Direction de la Sûreté Publique peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, elle rappelle qu'en cas de transmission, les services de police ne pourront avoir accès aux informations nominatives traitées que dans le strict cadre de leurs missions légalement conférées.

Elle constate également que le SICCFIN peut être rendu destinataire des informations dans le cadre des dispositions de 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.

La Commission considère que de telles transmissions sont conformes aux exigences légales.

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

Les personnes ayant accès au traitement sont :

- le service IT Monaco (inscription, modification, mise à jour) ;
- les employés de la banque (collaborateurs Monaco) dans le cadre du classement et de l'archivage de leurs correspondances uniquement (inscription, modification, mise à jour) ;
- le service Legal & Compliance Monaco, les membres de la Direction Monaco et Julius Baer Zurich, le contrôle interne et audit Monaco et Julius Baer Zurich, les collaborateurs sur demande justifiée et en présence d'un membre du management conformément à la procédure établie, (droit de consultation) ;
- le service IT Monaco et Julius Baer Zurich (maintenance) ;
- le service IT Help Desk Julius Baer Zurich, Genève et Lugano (restauration d'emails).

La Commission prend acte de l'indication du responsable de traitement selon laquelle « *en cas de suppression par erreur, une restauration est possible. Il convient alors de contacter l'IT Help Desk. Un numéro de téléphone unique est prévu, mais trois services différents sont disponibles en fonction de la langue sélectionnée (Genève pour le français, Lugano pour l'italien et Zurich pour l'anglais)* ».

Elle relève également que la Bank Julius Baer (Monaco) SAM a recours à un prestataire de service, la Bank Julius Baer & Co LTD, située en Suisse.

Ainsi, 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 le prestataire, la Commission rappelle que conformément aux dispositions de l'article 17 de la loi n° 1.165, modifiée, ses droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, celui-ci est 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, modifiée, la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et doit pouvoir lui être communiquée à première réquisition.

VI. Sur les interconnexions et rapprochements

Ledit traitement fait l'objet d'un rapprochement avec les traitements suivants :

- gestion des opérations de bourse : l'enregistrement des communications électroniques permettra de confirmer l'ordre communiqué en cas de litige avec le client (relatif à un ordre de bourse), légalement mis en œuvre ;
- gestion des ordres de change: l'enregistrement des communications électroniques permettra de confirmer l'ordre communiqué en cas de litige avec le client (relatif à un ordre de change), légalement mis en œuvre ;
- gestion des opérations de caisse : l'enregistrement des communications électroniques permettra de confirmer l'ordre communiqué en cas de litige avec le client (relatif à une opération de caisse) ;
- gestion des ordres de paiement SEPA : l'enregistrement des communications électroniques permettra de confirmer l'ordre communiqué en cas de litige avec le client (relatif à un ordre de paiement) ;
- gestion des transferts : l'enregistrement des communications électroniques permettra de confirmer l'ordre communiqué en cas de litige avec le client (relatif à un ordre de transfert).

A cet égard, la Commission relève que les formalités légales relatives à l'exploitation des traitements ayant pour finalité « *Gestion des opérations de caisse* », « *Gestion des ordres de paiement SEPA* » et « *Gestion des transferts* » n'ont pas été effectuées par la Bank Julius Baer (Monaco) SAM.

Par ailleurs, elle observe que le présent traitement fait également l'objet d'un rapprochement avec un traitement ayant pour finalité « *Gestion de l'Active Directory* ».

A cet égard, la Commission relève que les formalités légales relatives à l'exploitation de ce traitement n'ont pas été effectuées par l'établissement bancaire dont s'agit.

Par conséquent, elle demande que les rapprochements ou interconnexions dont s'agit ne puissent avoir lieu entre les traitements qu'une fois que ces derniers auront 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'observations particulières.

La Commission rappelle néanmoins que, conformément à l'article 17 de la loi n° 1.165, modifiée, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement 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 objets de ce traitement sont conservées pour une durée de 10 ans à compter de l'envoi/réception de l'email. Ces derniers n'étant disponibles dans la boîte email du collaborateur que 360 jours maximum à compter de leur envoi ou réception.

La Commission considère que cette durée de conservation est conforme aux exigences légales.

Après en avoir délibéré, la Commission

Modifie la finalité du traitement par « *Gestion et supervision de la messagerie professionnelle* ».

Rappelle que conformément à l'article 17-1 de la loi n° 1.165, modifiée, la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et doit pouvoir être communiquée à la Commission à première réquisition ;

Demande :

- de mettre en conformité avec l'article 14 de la loi dont s'agit les documents et le disclaimer destinés à l'information des personnes concernées ;
- que les rapprochements ou interconnexions n'aient lieu qu'entre les traitements légalement mis en œuvre ;

A la condition de la prise en compte de la demande qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par la Bank Julius Baer (Monaco) SAM, du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie professionnelle* ».**

Le Président,

Guy MAGNAN