

Délibération n° 2020-017 du 15 janvier 2020

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

« *Mise en place d'un dispositif d'alertes professionnelles* »

présenté par Société Générale Private Banking SAM,

dénommé Whistleblowing

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 ;

Vu la Loi n° 1.457 du 12 décembre 2017 relative au harcèlement et à la violence au travail ;

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° 1.284 du 10 septembre 2007 portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, susvisée ;

Vu l'Arrêté français du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution ;

Vu la Recommandation CM/Rec(2015)5 du Conseil de l'Europe du 1^{er} avril 2015 sur le traitement des données à caractère personnel dans le cadre de l'emploi ;

Vu la Délibération n° 2011-73 du 26 septembre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les dispositifs d'alerte professionnelle mis en œuvre sur le lieu de travail ;

Vu la demande d'autorisation déposée par la Société Générale Private Banking SAM, le 30 septembre 2019, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Mise en place d'un dispositif d'alertes professionnelles* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 28 novembre 2019, 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 janvier 2020 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Société Générale Private Banking (Monaco) SAM est une société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 96S03214 ayant pour activité « *dans les conditions déterminées par la législation et la réglementation applicables aux établissements de crédit, d'effectuer avec toutes personnes physiques ou morales, tant en Principauté de Monaco qu'à l'étranger : toutes opérations de banque à savoir : recevoir du public des fonds, notamment sous forme de dépôts, consentir des crédits sous des formes quelconques, prendre tous engagements par signature tels qu'aval, cautionnement ou garantie, mettre à disposition et gérer tous moyens de paiements, effectuer toutes opérations de crédit-bail et toutes opérations de location assorties d'une option d'achat (...)* ».

Pour des raisons liées à son activité, elle souhaite mettre en place un dispositif d'alertes professionnelles.

Aussi, le traitement objet de la présente demande porte sur des soupçons d'activités illicites, des infractions, des mesures de sûreté. Il est également mis en œuvre à des fins de surveillance. Il est donc soumis au régime de l'autorisation de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité la « *Mise en place d'un dispositif d'alertes professionnelles* ». Il est dénommé « *Whistleblowing* ».

Le responsable de traitement indique qu'il concerne les « *collaborateurs (saliés, intérimaires, stagiaires, tiers collaborateurs extérieurs permanents, tiers collaborateurs extérieurs temporaires, personnes visées par l'alerte n'étant pas des collaborateurs* ».

Les fonctionnalités sont les suivantes :

« *Le dispositif d'alerte en vigueur au sein de l'Entité a pour objet de permettre à tout collaborateur de faire part d'un manquement avéré (ou de soupçons d'un tel manquement) au titre des articles 36 et 37 de l'Arrêté du 03 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement*

et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution dans les domaines d'application suivants :

- *conflit d'intérêts*
- *vol de matériel*
- *pratique anti-concurrentielle*
- *violation des sanctions internationales et autres mesures de gel des avoirs*
- *intégrité des marchés : opérations d'initiés, manipulation de cours, diffusion de fausses informations*
- *fraude comptable*
- *RH : discrimination, santé et sécurité des salariés*
- *droits humains et libertés fondamentales*
- *respect de la confidentialité de l'information*
- *protection des données personnelles*
- *contournement ou tentative de contournement des contrôles*
- *falsification de documents*
- *un autre crime ou délit*
- *une autre violation grave et manifeste d'un engagement international régulièrement approuvé ou ratifié par la France ou par Monaco*
- *une autre violation grave et manifeste de la loi ou de la réglementation.*

Les fonctionnalités du traitement sont les suivantes :

- *Permettre à l'ensemble du personnel ainsi qu'aux collaborateurs extérieurs permanents et temporaires de formuler une alerte ;*
- *Recevoir et traiter ces alertes par les personnels désignés par la banque ;*
- *Etablir des comptes rendus relatifs à l'alerte et son suivi ;*
- *Archiver et détruire les données ».*

La Commission constate que le périmètre des alertes professionnelles souhaité par le responsable de traitement va au-delà de celui qu'elle autorise, et recouvre des domaines dont les contours sont difficilement appréhendables.

Aussi la Commission limite le champ des alertes professionnelles aux domaines suivants :

- *actes de corruption (articles 113-2 et suivants du Code Pénal monégasque) ;*
- *actes de fraudes (articles 331 et suivants du Code Pénal monégasque) ;*
- *actes relatifs au harcèlement et à la violence au travail (Loi n° 1.457 du 12 décembre 2017) ;*
- *actes relatifs au non-respect de règles d'éthiques professionnelles – protection des clients, régularité des opérations et conflits d'intérêts (Ordonnance Souveraine n° 1.284 du 10 septembre 2007) ;*
- *actes relatifs au non-respect des règles en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption (Loi n° 1.362 du 3 août 2009 et Ordonnance Souveraine n° 2.318 du 3 août 2009, modifiées) ;*
- *actes relatifs au non-respect des règles en matière de sanctions et d'embargos ;*
- *actes relatifs au non-respect des règles en matière d'intégrité de marché (Loi n° 1.338 du 7 septembre 2007 sur les activités financières) ;*
- *actes relatifs au non-respect des règles relatives à la protection des données nominatives (Loi n° 1.165 du 23 décembre 1993, modifiée).*

Sous cette réserve, la Commission constate 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

La Commission rappelle qu'aux termes de sa délibération n° 2011-73 du 26 septembre 2011 relative aux dispositifs d'alerte professionnelle mis en œuvre sur le lieu de travail, le champ du dispositif d'alerte professionnelle doit être clairement défini afin que la pertinence de l'alerte puisse être étudiée de manière objective.

Elle relève qu'en l'espèce tel est le cas et considère donc que le traitement est licite, conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

Le responsable de traitement indique que le traitement est justifié par le respect d'une obligation légale et la réalisation d'un intérêt légitime, sans que ne soient méconnus ni les intérêts, ni les droits et libertés fondamentaux des personnes concernées.

Concernant la justification fondée sur le respect d'une obligation légale, les textes concernés sont :

- la Loi n° 1.462 du 28 juin 2018 renforçant le dispositif de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;
- la Loi n° 1.457 du 12 décembre 2017 relative au harcèlement et à la violence au travail ;
- les articles 331 et suivants du Code Pénal monégasque ;
- la Loi n° 1.338 du 7 septembre 2007 sur les activités financières ;
- l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 ;
- la Loi n°1.165 di 23 décembre 1993, modifiée.

La Commission relève que ces textes n'imposent pas en eux-mêmes la mise en œuvre à Monaco du dispositif dont s'agit, qui permet de laisser aux collaborateurs la faculté de signaler par un canal dédié la non-conformité aux Lois précédemment citées.

Toutefois, la Commission considère que la justification est conforme au point « *II. Légitimité et finalités du traitement relatif à un dispositif d'alerte professionnelle* ».

Par ailleurs, il ressort des pièces jointes au dossier qu'une alerte anonyme peut être traitée. Il est précisé qu'en tout état de cause « *les informations obtenues doivent être formulées de manière objective et factuelle en ligne avec le champ d'application* ». La Commission rappelle qu'il convient de prendre des mesures de précautions sur le traitement d'une alerte anonyme, qui doit être une modalité de signalement exceptionnelle, et être conformes au point IV « *traitement de l'identité de l'émetteur* » de la délibération n° 2011-73 du 26 septembre 2011 portant recommandation sur les dispositifs d'alerte professionnelle mis en œuvre sur le lieu de travail.

Au vu de ce qui précède, la Commission considère que le traitement est justifié, conformément à l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité : nom, prénom, fonction de l'émetteur de l'alerte, des personnes faisant l'objet de l'alerte et des personnes intervenant dans le recueil ou le traitement de l'alerte, BU/SU de l'émetteur de l'alerte s'il s'agit d'un salarié ;
- adresses et coordonnées : émetteur de l'alerte : localisation géographique et coordonnées, personnes faisant l'objet de l'alerte et personnes intervenant dans le recueil ou le traitement de l'alerte : coordonnées ;

- infractions, condamnations, mesures de sûreté, soupçon d'activité illicite : l'objet des faits signalés, la description précise des faits faisant l'objet du signalement, les documents de nature à étayer le signalement ;
- attestation de bonne foi : confirmation que l'émetteur de l'alerte a bien eu personnellement connaissance des faits signalés et qu'il agit en bonne foi et de manière désintéressée.

Les informations ont pour origine l'émetteur de l'alerte, les personnes intervenant dans le recueil ou le traitement de l'alerte et les services conformité Groupe et local.

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 des personnes concernées est assurée au moyen d'une procédure interne accessible en Intranet.

A cet égard, il a été joint un document intitulé « *procédure* : dispositif d'alerte à Monaco ».

A la lecture dudit document, la Commission constate que l'information des personnes concernées est conforme à 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 responsable de traitement indique que le droit d'accès s'effectue par voie postale ou par courrier électronique auprès du Délégué à la Protection des Données (Service Compliance).

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit s'exercer dans le mois suivant la réception de la demande.

En outre, la Commission relève que les tiers peuvent exercer leur droit d'accès par le biais d'une adresse mail dédiée.

Enfin, s'agissant de l'exercice du droit d'accès par voie électronique, la Commission considère qu'une procédure 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. 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° 2015-116 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

V. Sur les communications d'informations et les personnes ayant accès au traitement

➤ **Sur les accès :**

Le responsable de traitement indique qu'ont accès aux informations :

Concernant les « *utilisateurs SGPB Monaco* » :

- Le déclarant de l'alerte, les personnes habilitées du service Conformité, la DRH et les référents désignés par la DRH (exclusivement pour les alertes liées au harcèlement au travail) en inscription, modification, mise à jour et consultation ;

Concernant les « *utilisateurs SGPB Groupe* » :

- Le responsable de la Conformité groupe, son adjoint, ainsi que 2 référents centraux de la Conformité Groupe en inscription, modification, mise à jour et consultation ;
- Le responsable anticorruption du Groupe en consultation ;
- Les membres habilités de l'Inspection générale en consultation en cas d'investigation.

Il est également indiqué qu'une liste nominative des personnes ayant accès au traitement est tenue à jour. A cet égard, la Commission rappelle que cette liste doit lui être communiquée à première réquisition

Elle considère enfin que ces accès sont justifiés.

➤ **Sur les communications d'informations :**

Le responsable de traitement indique que « *conformément à la Loi, les autorités de tutelle sont susceptibles, dans le cadre de leur mission, d'avoir accès aux informations objet du traitement* ».

La Commission en prend acte.

VI. Sur les rapprochements et interconnexions avec d'autres traitements

Le responsable de traitement indique des interconnexions avec les traitements ayant pour finalité respective la « *Gestion et traçabilité des habilitations informatiques* » aux fins de gestion des habilitations des personnels concernés, « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle* », canal de signalement d'alertes, tous deux 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.

Cependant 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 Commission rappelle enfin 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 aux personnes concernées sont :

- détruites immédiatement pour les informations considérées dès leur réception comme n'entrant pas dans le champ du dispositif ;
- détruites dans un délai de deux mois à compter de la clôture des opérations de vérification lorsque l'alerte n'est pas suivie d'une procédure disciplinaire ou judiciaire ;
- conservées jusqu'au terme de la procédure lorsqu'une procédure disciplinaire ou judiciaire est engagée à l'encontre de la personne mise en cause ou de l'auteur de l'alerte abusive.

A cet égard, la Commission rappelle que, suivant le point X de sa délibération n° 2011-73 du 26 septembre 2011 elle considère que :

- doivent être détruites sans délai les informations relatives à une alerte, considérée dès son recueil comme n'entrant pas dans le champ du dispositif d'alerte professionnelle dont s'agit ;
- les informations relatives à une alerte qui n'est pas suivie d'une procédure disciplinaire ou judiciaire doivent être détruites dans un délai de deux mois à compter de la clôture des opérations de vérification ;
- les informations d'une alerte qui a donné lieu à une procédure judiciaire ou disciplinaire peuvent être conservées jusqu'au terme de la procédure.

En conséquence, la Commission considère que ces durées de conservation sont conformes aux exigences légales.

Elle relève cependant que certaines annexes comportent des durées de conservation pouvant être plus longues que celles indiquées précédemment. Aussi, la Commission demande que le responsable de traitement s'assure que les durées de conservation mentionnée à la présente rubrique VIII sont respectées.

Après en avoir délibéré, la Commission :

Limite le champ des alertes professionnelles aux domaines suivants :

- actes de corruption (articles 113-2 et suivants du Code Pénal monégasque) ;
- actes de fraudes (articles 331 et suivants du Code Pénal monégasque) ;
- actes relatifs au harcèlement et à la violence au travail (Loi n° 1.457 du 12 décembre 2017) ;
- actes relatifs au non-respect de règles d'éthiques professionnelles – protection des clients, régularité des opérations et conflits d'intérêts (Ordonnance Souveraine n° 1.284 du 10 septembre 2007) ;
- actes relatifs au non-respect des règles en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption (Loi n° 1.362 du 3 août 2009 et Ordonnance Souveraine n° 2.318 du 3 août 2009, modifiées) ;
- actes relatifs au non-respect des règles en matière de sanctions et d'embargos ;
- actes relatifs au non-respect des règles en matière d'intégrité de marché (Loi n° 1.338 du 7 septembre 2007 sur les activités financières) ;

- actes relatifs au non-respect des règles relatives à la protection des données nominatives (Loi n° 1.165 du 23 décembre 1993, modifiée).

Considère qu'une procédure 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 :

- la liste nominative des personnes ayant accès au traitement doit lui être communiquée à première réquisition ;
- 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 ;
- l'alerte signalée de manière anonyme doit être une modalité exceptionnelle et être accompagnées de mesures de précaution, conformément au point IV « *traitement de l'identité de l'émetteur* » de la délibération n° 2011-73 du 26 septembre 2011 portant recommandation sur les dispositifs d'alerte professionnelle mis en œuvre sur le lieu de travail.

Demande que le responsable de traitement s'assure que les durées de conservation mentionnées à la rubrique VIII de la présente délibération sont respectées, certaines annexes mentionnant des durées de conservation potentiellement plus longues.

A la condition de la prise en compte des éléments qui précèdent,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre, par Société Générale Private Banking SAM., du traitement automatisé d'informations nominatives ayant pour finalité « *Mise en place d'un dispositif d'alertes professionnelles* ».**

Le Président

Guy MAGNAN