Délibération n° 2021-016 du 20 janvier 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

« *Dispositif d'alertes professionnelles (Whistleblowing)* »

présenté par CFM Indosuez Wealth,

dénommé Business Keeper Monitoring System (BKMS)

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 ° 1.362 du 3 aout 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

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 1er 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 portant recommandation sur les dispositifs d'alerte professionnelle mis en œuvre sur le lieu de travail ;

Vu la demande d'autorisation déposée par CFM Indosuez Wealth, le 1er octobre 2020, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Dispositif d'alertes professionnelles (Whistleblowing)* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 30 novembre 2020, 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 20 janvier 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

CA Indosuez Wealth (Group), maison mère située à Paris, est établie à Monaco par le biais de sa filiale, le CFM Indosuez Wealth, société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 56S00341, et qui a pour objet social « *en Principauté de Monaco et à l'étranger, pour son compte, pour le compte de tiers ou en participation, toutes opérations bancaires et financières et plus généralement toutes opérations pouvant être exercées par les établissements de crédit de droit monégasque en conformité avec la législation et la réglementation qui leurs sont applicables* ».

Pour des raisons liées à son activité, ce responsable de traitement 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 *« Dispositif d'alertes professionnelles « Whistleblowing » »*. Il est dénommé Business Keeper Monitoring System (BKMS).

Le responsable de traitement indique qu'il concerne les « *salariés, fournisseurs, clients, prestataires* » et de manière générale « *toute personne visée par l'alerte* ».

Les fonctionnalités sont les suivantes :

- *«Permettre aux collaborateurs ainsi qu'aux fournisseurs, prestataires et clients de formuler une alerte en cas de dysfonctionnement ;*
- *Enregistrer et assurer le suivi des alertes jusqu'à leur clôture ;*
- *Etablir des statistiques et des reportings sur les alertes* ».

Le dispositif a pour champ d'application :

- *« Corruption et atteintes à la probité ;*
- *Vol, fraude, fraude fiscale, abus de confiance, abus de faiblesse ;*
- *Abus de bien social, prise illégale d'intérêt, conflits d'intérêts ;*
- *Blanchiment d'argent, violation des sanctions internationales ;*
- *Manipulation de cours, délits d'initié ;*
- *Discrimination, harcèlement moral/sexuel, agression physique/sexuelle ;*
- *Non-respect des droits humains et environnementaux, menace ou préjudice grave pour l'intérêt général ;*
- *Autre délit, autre crime ».*

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, il est indiqué que la maison mère étant sise en France et établissant des comptes consolidés, elle doit appliquer à ses filiales les dispositions de la Loi française n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

Ce texte impose la mise en œuvre d'un « *dispositif d'alerte interne destiné à permettre le recueil des signalements émanant d'employés et relatifs à l'existence de conduites ou de situations contraires au code de conduite de la société* ».

La Commission constate que le champ d'application des alertes est conforme au droit local et aux dispositions de la Loi n° 1.457 du 12 décembre 2017 relative au harcèlement et à la violence au travail et à la Loi n° 1.362.

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

Le responsable de traitement précise toutefois que « *conformément aux préconisation de Tranparency International France figurant dans son « Guide pratique pour la mise en œuvre des mesures anticorruption imposées par la loi aux entreprises », le groupe Crédit Agricole a décidé d'ouvrir le dispositif d'alertes professionnelles aux partenaires commerciaux, aux sous-traitants, aux fournisseurs et aux clients* ».

Par ailleurs, il ressort des pièces jointes au dossier qu'une alerte anonyme peut être traitée. 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. Les lanceurs d'alerte peuvent s'ils le souhaitent créer un compte et suivre les alertes qu'ils ont émises.

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 du lanceur d'alerte et/ou de la personne visée par l'alerte ;
- adresses et coordonnées : lieu de survenance de l'incident, localisation du lanceur d'alerte, localisation de l'entité concernée ;
- vie professionnelle : lien entre le lanceur d'alerte et l'entité concernée ;
- données d'identification électronique : numéro de l'alerte ;
- infractions, condamnations, mesures de sûreté, soupçon d'activité illicite : faits signalés, description de l'évènement et documents justificatifs/complémentaires ;
- informations temporelles : logs de connexion de l'outil, date de réception de l'alerte, date de dernière activité ;
- informations relatives à l'alerte : statut de l'alerte, résultat des investigations, suites données à l'alerte.

Les informations ont pour origine le lanceur d'alerte, exceptées celles relatives aux données d'identification électronique et les informations temporelles qui sont générées par le système, et les informations relatives à l'alerte qui sont produites par l'analyste et/ou le superviseur.

En ce qui concerne les lanceurs d'alerte ayant créé un compte, la Commission relève que des informations d'identifiant/mot de passe sont exploitées.

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 et une rubrique propre à la protection des données accessible en ligne.

Ces documents n'ayant pas été joints au dossier, la Commission rappelle que l'information des personnes concernées doit être effectuée de manière conforme 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 responsable de traitement indique que le droit d'accès s'effectue par voie postale, sur place ou par courrier électronique auprès du « *Data Protection Officer* ».

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.

Par ailleurs, 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 :

- Le lanceur d'alerte pour les informations relatives à l'alerte émise par ce dernier en inscription et/ou consultation ;

- Le Directeur Compliance et le Responsable Regulatory Compliance de CA Indosuez Wealth (Group), profil superviseur et le Directeur Compliance et le Responsable Déontologie et Données clients de CFM Indosuez Wealth, profil analyste : inscription, modification, et consultation ;

- Le Directeur de la Conformité du groupe Crédit Agricole et son délégué : consultation ;

- Le service Dispositif lanceur d'alerte du Groupe Crédit Agricole : consultation, maintenance.

La Commission rappelle qu'une liste nominative des personnes ayant accès au traitement doit tenue à jour et 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 les informations peuvent être communiquées aux autorités habilitées.

La Commission en prend acte.

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

Le responsable de traitement indique des interconnexions avec le traitement ayant pour finalité la « *Gestion du contentieux* », légalement mis en œuvre, car « *les alertes qui font l'objet d'une action judiciaire ou disciplinaire sont transmises au service concerné et sont traitées dans le cadre du traitement « Gestion du contentieux »* ».

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.

En outre, la Commission relève que les comptes créés par les lanceurs d'alerte sont supprimés quand l'alerte est clôturée.

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.

Enfin, les logs de connexion à l'outil sont conservés un an.

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

Après en avoir délibéré, la Commission :

Rappelle que :

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

- l'information des personnes concernées doit être effectuée de manière conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- 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 ;

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 CFM Indosuez Wealth, du traitement automatisé d'informations nominatives ayant pour finalité « *Dispositif d'alertes professionnelles (Whistleblowing)* ».**

Le Président

Guy MAGNAN