Délibération n° 2018-166 du 17 octobre 2018

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 BNP Paribas Wealth Management Monaco

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 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 BNP Paribas Wealth Management Monaco, le 4 juillet 2018, 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 3 septembre 2018, 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 17 octobre 2018 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

BNP Paribas Wealth Management Monaco est immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 91S02724, et a pour activité « *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 (…) ».*

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 (salariés, intérimaires, stagiaires et prestataires de services permanents ou temporaires)* ».

A cet égard, la Commission considère qu'il concerne également les personnes visées par l'alerte et qui ne seraient 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 :*
- actes de corruption (articles 113-2 et suivants du Code Pénal monégasque) ;
- actes de fraudes (articles 331et 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 aout 2009 et Ordonnance Souveraine n° 2.318 du 3 aout 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).

- *permette aux collaborateurs de formuler une alerte ;*
- *enregistrer les alertes communiquées téléphoniquement ;*
- *établir des comptes rendus relatifs à l'alerte et son suivi ;*
- *archiver et détruire les données* ».

Aussi, elle 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.

La Commission relève que ces justifications sont conformes au point « *II. Légitimité et finalités du traitement à un dispositif d'alerte professionnelle* » de sa délibération n° 2011-73 portant recommandation sur les dispositifs d'alerte professionnelle mis en œuvre sur le lieu de travail.

Par ailleurs, le responsable de traitement indique que l'émetteur de l'alerte est identifié mais que, « *par exception et uniquement via média téléphonique, il est possible de proposer aux émetteurs d'alertes d'effectuer un signalement anonyme de manière exceptionnelle si les conditions suivantes sont cumulativement réunies : la gravité des faits mentionnés devra être établie ; les éléments factuels devront être suffisamment détaillés* ». Ces mesures de précautions sur le traitement d'une alerte anonyme, qui doit être une modalité de signalement exceptionnelle, sont 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 et fonction (de l'émetteur de l'alerte, de la personne concernée par le signalement et des personnes intervenant dans le recueil ou le traitement de l'alerte)
- adresses et coordonnées : numéros de téléphone, adresses électroniques, lieu de travail ;
- données d'identification électronique : identifiant, mot de passe ;
- infractions, condamnations, mesures de sûreté, soupçon d'activité illicite : faits signalés, éléments recueillis lors de l'instruction, compte rendu des opérations de vérification, suites données l'alerte ;
- données de connexion : date, heure et transactions effectuées.

Les informations relatives aux données d'identification électroniques et aux données de connexions proviennent de la gestion des habilitations issues de la « *Gestion administrative de salariés* ».

Les autres informations ont pour origine l'émetteur de l'alerte, les personnes intervenant dans le recueil ou le traitement de l'alerte et le service 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 les procédures du responsable de traitements sur la CCIN et sur le droit d'alerte éthique.

A la lecture dudit document, la Commission rappelle que l'information des personnes concernées doit être 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'exerce par voie postale auprès du Chief Operating Officer.

La réponse se fera dans le mois suivant la réception de la demande.

La Commission constate ainsi que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 la Loi n° 1.165 du 23 décembre 1993.

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 BNP Paribas WM Monaco :

- Le déclarant de l'alerte, le Responsable de la Conformité et son adjoint en inscription, modification, mise à jour et consultation.

La Commission précise que le déclarant de l'alerte ne pourra avoir accès qu'aux informations de l'alerte émise par ses soins.

Concernant BNP Paribas S.A. :

- Le responsable de l'alerte éthique de la Conformité et le responsable de la Conformité groupe en inscription, modification, mise à jour et consultation ;
- Les membres habilités de l'Inspection générale en consultation en cas d'investigation ;
- Le service de Contrôle Interne en consultation en cas d'utilisation du média téléphonique pour l'alerte éthique.

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 ainsi que ces accès sont justifiés.

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

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

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 administrative des salariés* » aux fins de gestion des habilitations des personnels concernés, et la « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle* » et « *Enregistrements de conversations téléphoniques mises en œuvre sur le lieu de travail* » comme médias pour le signalement d'alertes.

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.

Enfin, les données d'identification électroniques sont conservées le temps de la relation contractuelle de la procédure, tandis que les données de connexion sont conservées 1 an à compter de leur collecte.

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

Après en avoir délibéré, la Commission :

Considère que le présent traitement concerne également les personnes visées par l'alerte et qui ne seraient pas des collaborateurs.

Précise que le déclarant de l'alerte ne pourra avoir accès qu'aux informations de l'alerte émise par ses soins.

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.

Demande que l'information des personnes concernées soit conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

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 BNP Paribas Wealth Management Monaco, du traitement automatisé d'informations nominatives ayant pour finalité « *Mise en place d'un dispositif d'alertes professionnelles* ».**

Le Président

Guy MAGNAN