Délibération n° 2023-091 du 21 juin 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

« *Lutte contre la fraude interne* »,

présenté par Banque Populaire Méditerranée Succursale de 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 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, 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 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° 1.284 du 10 septembre 2007 fixant les modalités d'application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, susvisée ;

Vu l'Ordonnance Souveraine n° 3.559 du 5 décembre 2011 rendant exécutoire l'Accord monétaire entre l'Union européenne et la Principauté de Monaco ;

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 demande d'autorisation déposée par la société Banque Populaire Méditerranée Succursale de Monaco, le 23 février 2023, concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Lutte contre la fraude interne* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 21 avril 2023, conformément à l'article 11-1 de la Loi n° 1.165, susmentionnée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 21 juin 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Banque Populaire Méditerranée (BPMED) est une société française établie à Monaco par sa succursale enregistrée au RCI sous le numéro 00S03751, ayant une activité d'*« agence bancaire ».*

Afin de lutter contre la fraude interne, cet établissement souhaite mettre en place un traitement permettant la détection et la gestion des incidents de fraude émanant des collaborateurs.

Le responsable de traitement indique que le traitement, objet de la présente demande, porte sur des soupçons d'activités illicites, des infractions, des mesures de sûreté et qu'il est 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, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Lutte contre la fraude interne* ».

Les personnes concernées sont les collaborateurs, les clients et les prospects.

Les fonctionnalités du traitement sont les suivantes :

- détection des fraudes internes par la mise en place de requêtes informatiques et la saisie manuelle d'alertes dont la source est non informatisée (réclamations, déclarations de soupçons, etc…) ;
- qualification des alertes ;
- constitution et suivi de l'avancement des dossiers ;
- mise à disposition de statistiques agrégées concernant les alertes et les cas avérés.

Le responsable de traitement précise que les requêtes informatiques sont générées à partir des données présentes dans le système d'information (tels que des données clients, des événements (changement d'adresse, de numéro de téléphone sécurisé, d'éléments d'identité, etc) et des données relatives à l'identité du collaborateur ayant traité l'opération) après comparaison avec différents scénarios identifiés par la banque.

Par ailleurs, le responsable de traitement indique que certaines alertes peuvent également être manuellement insérées *« par un investigateur s'il soupçonne ou observe un comportement / une activité suspect(e) »* ou suite à des remontées des différents Services supports et d'agences.

La Commission constate que le traitement permet également la constitution de preuve en cas de litige.

Le responsable de traitement précise que le Service Fraude n'opère pas une surveillance des courriels et qu'il n'a pas recours à un outil Data Leak Protection (DLP).

La Commission rappelle que le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165.

Le responsable de traitement indique par ailleurs que le collaborateur concerné est informé qu'une enquête a été diligentée sur des faits le concernant au moment d'un entretien contradictoire d'investigation. Un compte rendu est réalisé après l'entretien et est intégré au rapport. Les faits peuvent, dans certains cas, être présentés au Comité Ethique qui veille à la juste proportionnalité de la sanction imposée au collaborateur au regard des circonstances. Préalablement à la fixation de la sanction, un entretien entre le collaborateur et les Ressources Humaines a lieu avant un nouveau passage devant le Comité Ethique pour entériner la sanction.

Elle considère 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

Le présent traitement est justifié par l'existence d'une obligation légale à laquelle est soumis le responsable de traitement.

La Commission relève qu'aux termes de l'Arrêté 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, notamment en son article 94, le responsable de traitement est tenu de se doter d'un *« système d'analyse et de mesure des risques en les adaptant à la nature et au volume de leurs opérations afin d'appréhender »* le risque opérationnel dont fait partie le risque de fraude interne conformément à l'article 10 du même texte.

La Commission considère que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité : données d'identité des clients et collaborateurs : état civil, données RH ;
- adresses et coordonnées : données de contact des clients et collaborateurs : adresses légales et juridiques, NPAI, coordonnées téléphoniques et électroniques ;
- caractéristiques financières : données relatives au domaine bancaire des clients et collaborateurs : volume et typologie d'opérations (virement, prélèvement, espèces, carte bancaire), provenance et destination des fonds, montant des avoirs gérés, opérations à risque élevé, opérations espèces… ;
- données d'identification électronique : numéro d'identification client et collaborateur (matricule) ;
- informations temporelles : données d'activité et de suivi individuel des collaborateurs ;
- alertes : rapports, faux positifs.

A l'étude du dossier, la Commission relève que dans le cadre de la préparation des entretiens contradictoires d'investigation des documents Word comprenant notamment la liste des questions peuvent être créés et placés dans l'outil.

Le responsable de traitement indique que ces informations proviennent du système d'information de la banque.

La Commission considère que les informations traitées 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 préalable des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est assurée au moyen :

- d'un document spécifique ;
- d'une mention ou clause particulière intégrée dans un document remis à l'intéressé ;
- d'une rubrique propre à la protection des données accessible en ligne ;
- d'une *« notice d'information sur le traitement des données à caractère personnel »*.

La Commission n'ayant pas été destinataire desdits documents, elle n'est pas en mesure de se prononcer sur la qualité de l'information dispensée.

A cet égard elle rappelle que l'ensemble des personnes concernées doit être informé conformément aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

- ***Sur l'exercice du droit d'accès des personnes concernées***

Le responsable de traitement indique que le droit d'accès est exercé de manière indirecte.

Toutefois, par complément d'information, le responsable de traitement a précisé que le droit d'accès s'exerce de manière directe auprès de la Direction des Risques et de la Conformité.

A cet égard, la Commission rappelle que dans l'hypothèse où le droit d'accès s'exerce par voie postale, la réponse doit intervenir dans le mois suivant la réception de la demande.

En outre, dans l'hypothèse où le droit d'accès s'exerce par voie électronique, la Commission rappelle qu'une procédure doit être mise en place afin que le responsable de traitement puisse s'assurer, en cas de doute sur l'identité de la personne à l'origine du courriel, qu'il s'agit effectivement de la personne concernée par les informations.

Elle rappelle par ailleurs concernant le traitement dont s'agit que le droit d'accès ne peut conduire les personnes concernées à accéder directement à l'ensemble des documents du traitement, notamment ceux couverts par le secret professionnel des avocats.

Sous ces conditions, 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 du 23 décembre 1993, modifiée.

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

- ***Sur les accès au traitement***

Le responsable de traitement indique qu'ont accès aux informations objet du présent traitement les collaborateurs et hiérarchiques de la Direction Risques et Conformité en charge du contrôle en inscription, modification, consultation, maintenance, tous les droits.

Par ailleurs, le responsable de traitement précise que pour leurs missions de maintenance, le Service Informatique ainsi que le Responsable de la Sécurité des Systèmes d'Information n'ont pas accès aux informations objet du présent traitement.

La Commission en prend acte.

Elle considère que ces accès sont conformes aux exigences légales et sont justifiés au regard de la finalité du traitement.

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

La Commission estime que les informations sont susceptibles d'être communiquées aux Autorités Administratives et Judiciaires légalement habilitées et rappelle que celles-ci ne peuvent avoir communication des informations objet du présent traitement que dans le strict cadre de leurs missions légalement conférées.

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

Le responsable de traitement indique que le présent traitement ne fait l'objet d'aucune interconnexion et d'aucun rapprochement.

A l'étude du dossier, la Commission relève néanmoins que le présent traitement peut être interconnecté et rapproché avec les traitements, légalement mis en œuvre suivants, ayant pour finalités :

- *« Gestion et supervision de la messagerie professionnelle »* ;
- *« Gestion des services de téléphonie professionnelle et enregistrement des conversations téléphoniques »* ;
- *« Gestion administrative des salariés »* ;
- *« Gestion de la relation clients et prospects »* ;
- *« Gestion des habilitations informatiques et accès aux applications* ».

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 par ailleurs que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

Elle 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 l'ensemble des informations objet du présent traitement sont conservées selon le statut de l'alerte :

- alertes non classées « *à investiguer* » : 3 mois maximum ;
- alertes « *à investiguer* » : 6 mois maximum ;
- alertes classées « *sans suite* » : 30 jours à compter de la date de qualification ;
- alertes pour lesquelles un dossier d'investigation a été ouvert : le temps de l'enquête jusqu'à ce que la fraude soit ou non avérée ;
- dossier clos avéré fraude : 5 ans à compter de la date de la qualification ;
- dossier clos avéré manquement : 5 ans à compter de la date de la qualification.

Le responsable de traitement indique par ailleurs, que les *« données d'activité et de suivi individuel des collaborateurs »* sont conservées pendant *« 5 ans de la date de la fraude ».* Par complément d'information, le responsable de traitement précise toutefois que ces logs de connexion sont conservés « *selon une durée de 3 mois minimum (en base active) à 1 an maximum (archivage intermédiaire)* ».

La Commission considère que ces durées de conservation sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Rappelle que :

- le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993 ;

- l'information de l'ensemble des personnes concernées doit être préalable et conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- une procédure relative au droit d'accès par voie électronique doit être mise en place afin que le responsable de traitement puisse s'assurer, en cas de doute sur l'identité de la personne à l'origine du courriel, qu'il s'agisse effectivement de la personne concernée par les informations ;

- le droit d'accès ne peut conduire les personnes concernées à accéder directement à l'ensemble des documents du traitement, notamment ceux couverts par le secret professionnel des avocats ;

- 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.

Sous le bénéfice de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre, par la Banque Populaire Méditerranée Succursale Monaco, du traitement automatisé d'informations nominatives ayant pour finalité *« Lutte contre le fraude interne ».***

Le Président

Guy MAGNAN