

Délibération n° 2018-016 du 17 janvier 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

« La détection, l'analyse, des transactions réalisées par des clients qui pourraient être liées au blanchiment de capitaux »

présenté par BNP Paribas Succursale de Monte-Carlo

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° 1.362 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° 15.321 du 08 avril 2002 relative aux procédures de gel des fonds aux fins de lutte contre le terrorisme ;

Vu l'Ordonnance Souveraine n° 1.675 du 10 juin 2008 relative aux procédures de gel des fonds mettant en œuvre des sanctions économiques ;

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° 2.318 du 3 août 2009, modifiée, fixant les conditions d'application de la Loi n° 1.362 du 3 août 2009, 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 la demande d'autorisation présentée le 17 octobre 2017 par BNP Paribas Succursale de Monte Carlo SA, concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *La détection, l'analyse, des transactions réalisées par des clients qui pourraient être liées au blanchiment de capitaux* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation modificative notifiée au responsable de traitement le 14 décembre 2017, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 17 janvier 2018 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

BNP Paribas Succursale de Monte Carlo est enregistrée au RCI sous le numéro 67S01164, ayant pour activité la réalisation d' « *Opérations de banque et de bourse* ».

Effectuant « *à titre habituel des opérations de banque* » au sens du 1^{er}) de l'article 1^{er} de la Loi n° 1.362 du 3 août 2009, elle est soumise aux dispositions de ladite Loi.

A ce titre, elle doit déterminer et vérifier l'identité de la clientèle, des éventuels mandataires et des personnes au profit desquelles les opérations et les transactions sont effectuées, conformément aux articles 3 et 5 de la Loi n° 1.362 du 3 août 2009.

Par ailleurs, elle est tenue d'exercer une vigilance constante à l'égard de la relation d'affaires au sens de l'article 4 de la même Loi.

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 détection, l'analyse, des transactions réalisées par des clients qui pourraient être liées au blanchiment de capitaux* ».

Le responsable de traitement indique qu'il concerne « *les clients (personnes physiques, personnes morales, mandataires, bénéficiaires économiques) et employés* ».

A cet égard, la Commission constate que seuls sont exploités pour les gestionnaires leurs « *nom, prénom et numéro de matricule* ».

Aussi, elle rappelle que seules les personnes expressément visées par la Loi n° 1.362 du 3 août 2009 et ses textes d'application sont susceptibles d'être l'objet des diligences qui s'y rapportent.

Le traitement a pour fonctionnalité « *la détection et l'analyse des transactions réalisées par des clients qui pourraient être liées au blanchiment de capitaux, au financement du terrorisme ou au délit de corruption et qui, à ce titre, seraient susceptibles de donner lieu à une déclaration de soupçon* ».

Le responsable de traitement précise également que « *ce traitement (...) [permet] d'assurer un suivi continu [des clients] par la définition d'une méthodologie pour identifier le profil de risque des clients [et] par l'examen obligatoire des transactions anormales en soi ou anormales par rapport au client* ».

A cet égard, 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.

Aussi, 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

Eu égard à l'objet social du responsable de traitement, et aux obligations qui lui incombent en application de la Loi n° 1.362 du 3 août 2009, la Commission considère que ce traitement est licite et justifié, au sens 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 : *Personne Physique* : Client/Mandataire/Bénéficiaire Economique Effectif : nom, prénom, nationalité, date de naissance, âge; *Gestionnaire* : nom, prénom, numéro de matricule ; *Personne morale* : raison sociale, numéro SIREN ;
- adresses et coordonnées : NPAI, pays de résidence fiscale des personnes physiques et siège social des personnes morales, adresse courrier ;
- formation-diplômes-vie professionnelle : profession du client, du mandataire ou du BEE, secteur d'activité de la personne morale ;
- caractéristiques financières : numéro de compte, solde du compte, type d'opérations, fonctionnement/ utilisation du compte (mouvement fréquence...), date/ heure/ lieu de l'opération, instruments de paiement, origines/ destination des fonds ;
- informations faisant apparaître (...) des appartenances politiques : Statut Personne Politiquement Exposée (PPE) ;
- Infractions, condamnations, mesures de sûreté, soupçon d'activité illicite : alertes émises par le logiciel dans le cadre du traitement ;
- profil de risque : niveau de risque client.

Le responsable de traitement indique que les alertes émises par le logiciel sont générées par le système, le profil de risque est issu du traitement ayant pour finalité « *Evaluer le niveau de sensibilité des clients aux risques de blanchiment de capitaux* », les caractéristiques financières ont pour origine les traitements ayant pour finalités respectives « *Tenue des comptes de la clientèle et le traitement des informations s'y rattachant par les établissements bancaires et assimilés* » et « *Valeurs mobilières et autres instruments financiers* ». Enfin, les autres informations sont issues du traitement ayant pour finalité « *Gestion de l'identification et de la vérification des personnes soumises à la Loi 1.362 du 3 août 2009* ».

La Commission constate que tous les traitements ci-dessus sont légalement mis en œuvre.

Elle estime que la classification PPE ne constitue pas en tant que telle une appartenance politique.

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 mention ou clause particulière intégrée dans un document remis à l'intéressé et d'une procédure interne accessible en intranet.

A l'examen de l'extrait de la convention de compte jointe au dossier, la Commission relève, qu'elle ne mentionne pas l'ensemble des dispositions de l'article 14 de la Loi n°1.165 du 23 décembre 1993.

Par ailleurs elle constate, s'agissant des clients et des employés, que « *l'entité tient également à [leur] disposition la liste des traitements automatisés portant sur leurs informations nominatives* ».

Aussi, la Commission estime qu'informer la personne concernée de la tenue à disposition d'une liste de traitements, qui nécessite de sa part une démarche active, n'est pas équivalent au fait de l'avertir, en ce que son abstention ne doit pas la priver d'être dûment informée.

En conséquence, la Commission demande que soit assurée l'information de l'ensemble des personnes concernées et qu'elle soit 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 les personnes concernées ne disposent que d'un droit d'accès indirect auprès de la CCIN.

A cet égard, la Commission estime que seules les informations relevant de la catégorie « *infractions, condamnations, mesures de sûreté, soupçons d'activités illicites* » font l'objet d'un droit d'accès indirect, en ce que l'article 43 de la Loi n° 1.362 du 3 août 2009 sanctionne pénalement les dirigeants ou les préposés des organismes financiers qui ont :

- « *informé sciemment le propriétaire des sommes, l'auteur de l'une des opérations, ou un tiers de l'existence de la déclaration ou de la transmission de renseignements prévus au Chapitre VI ;*
- *divulgué à quiconque des informations sur les suites données à la déclaration* ».

En conséquence, la Commission demande que les personnes concernées soient valablement informées, par le responsable de traitement, de leur faculté d'exercer leur droit d'accès direct, conformément à l'article 15 de la Loi n° 1.165 du 23 décembre 1993, et que seules les informations susceptibles de relever de l'article 43 de la Loi n° 1.362 du 3 août 2009 fassent l'objet d'un droit d'accès indirect.

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

➤ **Sur les accès au traitement**

Le responsable de traitement indique qu'ont accès au traitement :

- « *Utilisateurs succursale de Monaco : le personnel habilité de la force de vente, du Service de production et d'Appui commercial (SPAC), du Service Crédits, du Pôle conformité (ex Pôle Contrôle et Surveillance des Risques) et de la Direction a accès aux informations en inscription, modification, mise à jour et consultation ;*
- *Utilisateurs BNP Paribas SA : les collaborateurs du Back office peuvent avoir accès en inscription, modification, mise à jour et consultation ;*
- *Administrateurs : les équipes IT groupe sont en charge de l'installation et de la maintenance des programmes et leurs droits ne permettent pas d'accéder aux informations, objets du traitement ;*
- *Le service IT local, en tant que support fonctionnel de premier niveau, dispose d'un accès en consultation uniquement ;*
- *Les personnes habilitées du contrôle permanent et du contrôle périodique ont accès aux informations en consultation uniquement dans le cadre des missions qui leurs sont conférées ;*
- *Prestataire : en cas de recours à des prestataires externes, les interventions sont systématiquement encadrées par du personnel interne ».*

Par ailleurs, il précise qu'« *une liste des personnes habilitées à avoir accès aux informations est tenue à jour* ».

La Commission en prend acte et précise que cette liste doit lui être communiquée à première réquisition.

Aussi, elle souligne qu'en cas de recours à des prestataires, leurs accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993. De plus ils sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement.

Elle considère que ces accès sont justifiés.

➤ **Sur les communications d'informations**

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées à Monaco aux Autorités administratives (SICCFIN) et judiciaires légalement habilitées.

Aussi, la Commission rappelle qu'elles sont susceptibles d'être communiquées aux Autorités compétentes dans le cadre des missions qui leurs sont légalement conférées.

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

Le responsable de traitement indique une interconnexion avec les traitements ayant pour finalité respective la « *Gestion administrative des salariés* », la « *Gestion de l'identification et de la vérification des personnes soumises à la Loi 1.362 du 3 août 2009* », la « *Gestion des déclarations de soupçon* », « *Evaluer le niveau de sensibilité des clients aux risques de blanchiment de capitaux* », la « *Tenue des comptes de la clientèle et les*

traitements des informations s'y rattachant par les établissements bancaires et assimilés », « Valeurs mobilières et autres instruments financiers » tous légalement mis en œuvre.

A l'examen du dossier, la Commission constate que *« des revues régulières sur le bien-fondé des accès autorisés et sur leur traçabilité sont réalisées »*.

A cet égard, elle rappelle que l'Arrêté Ministériel n° 2016-501 du 5 août 2016 relatif aux modalités de déclaration simplifiée des traitements automatisés d'informations nominatives relatifs à la gestion administrative des salariés permet *« la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des applications informatiques et des réseaux »* mais exclut *« tout traitement opérant une surveillance de l'activité des salariés »*.

Aussi, la Commission demande que le responsable de traitement s'assure que la gestion des accès et des habilitations est effectuée conformément aux dispositions légales et réglementaires.

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 les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

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 alertes émises par le logiciel sont conservées *« si l'alerte donne lieu à une déclaration de soupçon : 10 ans après la déclaration demeurée sans suite de la part du SICCFIN ou 6 mois au maximum après l'information par le SICCFIN de l'existence d'une décision judiciaire devenue définitive, si l'alerte ne donne pas lieu à une déclaration de soupçon : 5 ans à compter de la génération de l'alerte »*.

Le reste des informations est conservé *« 10 ans à compter de la fin de la relation »*.

A cet égard, la Commission observe que l'article 10 de la Loi n° 1.362, précitée, dispose que :

« Les organismes et les personnes visés aux articles premier et 2 sont tenus de :

- *conserver pendant cinq ans au moins, après avoir mis fin aux relations avec leurs clients habituels ou occasionnels désignés à l'article 3, une copie de tous les documents probants ayant successivement servi à l'identification et à la vérification de l'identité, ainsi que de tous les documents recueillis ayant permis l'identification prescrite à l'article 5 ;*

- *conserver pendant une période d'au moins cinq ans à partir de l'exécution des opérations, une copie des enregistrements, des livres de comptes, de la correspondance commerciale et des documents relatifs aux opérations effectuées de façon à pouvoir les reconstituer précisément ;*
- *enregistrer les opérations effectuées de manière à pouvoir répondre aux demandes de renseignements visées à l'article 27, dans le délai prescrit ;*
- *être en mesure de répondre de manière rapide et complète à toute demande d'information du Service d'Information et de Contrôle sur les Circuits Financiers tendant à déterminer s'ils entretiennent ou ont entretenu au cours des cinq années précédentes une relation d'affaires avec une personne physique ou morale donnée et la nature de cette relation.*

Le Service d'Information et de Contrôle sur les Circuits Financiers peut demander la prorogation des délais de conservation dans le cadre d'une investigation en cours ».

Par ailleurs, elle rappelle que, dans sa délibération n° 2012-147 du 22 octobre 2012 portant recommandation sur les délais de conservation des informations nominatives se rapportant à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, elle préconise une durée de conservation des informations de :

- *« 5 ans après la déclaration de soupçon demeurée sans suite de la part du SICCFIN », en l'absence de transmission du rapport du SICCFIN au Procureur ;*
- *« 6 mois après avoir été informés par le SICCFIN de l'existence d'une décision judiciaire devenue définitive », en cas de transmission du rapport du SICCFIN au Procureur.*

En conséquence, elle fixe la durée de conservation des « alertes émises par le logiciel » si l'alerte donne lieu à une déclaration de soupçon à 5 ans après la déclaration demeurée sans suite de la part du SICCFIN et à 6 mois au maximum après l'information par le SICCFIN de l'existence d'une décision judiciaire devenue définitive.

Par ailleurs, elle demande que les alertes ne donnant pas lieu à une déclaration de soupçon soient conservées 1 an au maximum.

Enfin, elle fixe la durée de conservation des autres informations à « 5 ans après la fin de la relation d'affaires ».

Après en avoir délibéré, la Commission :

Rappelle que :

- seules les personnes expressément visées par la Loi n° 1.362 du 3 août 2009 et ses textes d'applications sont susceptibles d'être l'objet des diligences qui s'y rapportent ;
- le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993 ;
- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et 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 les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

Demande que :

- le responsable de traitement s'assure que la gestion des accès et des habilitations est effectuée conformément aux dispositions légales et réglementaires ;
- l'information de l'ensemble des personnes concernées soit assurée conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;
- les personnes concernées soient valablement informées, par le responsable de traitement, de leur faculté d'exercer leur droit d'accès direct, conformément à l'article 15 de la Loi n°1.165 du 23 décembre 1993, et que seules les informations susceptibles de relever de l'article 43 de la Loi n° 1.362 du 3 août 2009 fassent l'objet d'un droit d'accès indirect.

Fixe la durée de conservation des « *alertes émises par le logiciel* » si l'alerte donne lieu à une déclaration de soupçon à 5 ans après la déclaration demeurée sans suite de la part du SICCFIN et à 6 mois au maximum après l'information par le SICCFIN de l'existence d'une décision judiciaire devenue définitive. Par ailleurs, elle demande que les alertes ne donnant pas lieu à une déclaration de soupçon soient conservées 1 an au maximum. Enfin, elle fixe la durée de conservation des autres informations à « *5 ans après la fin de la relation d'affaires* ».

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 succursale de Monte Carlo du traitement automatisé d'informations nominatives ayant pour finalité « *La détection, l'analyse, des transactions réalisées par des clients qui pourraient être liées au blanchiment de capitaux* ».**

Le Président

Guy MAGNAN