Délibération n° 2021-084 du 19 mai 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

« *Prévention des fuites de données confidentielles* »

présenté par BNP PARIBAS WEALTH MANAGEMENT MONACO

Vu la Constitution du 17 décembre 1962 ;

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 le Code pénal monégasque ;

Vu le Code monétaire et financier français ;

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° 1.284 du 10 septembre 2007 portant application de 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° 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 délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'autorisation déposée par BNP PARIBAS WEALTH MANAGEMENT MONACO le 2 février 2021 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Prévention des fuites de données confidentielles* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 31 mars 2021, conformément à l'article 11-1 de la Loi n° 1.165, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 19 mai 2021 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 (…)* ».

Afin de prévenir tous risques inhérents à l'utilisation, par les employés, du canal de communication des transferts de fichiers vers les sites internet externes, BNP PARIBAS WEALTH MANAGEMENT MONACO souhaite mettre en œuvre un outil DLP (Data Leak Prevention) destiné à prévenir les fuites de données confidentielles.

A ce titre, en application de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, relatif à la mise en œuvre de traitements automatisés d'informations nominatives « *à des fins de surveillance* » ou « *portant sur des soupçons d'activités illicites, des infractions* », BNP PARIBAS WEALTH MANAGEMENT MONACO soumet la présente demande d'autorisation concernant le traitement ayant pour finalité « *Prévention des fuites de données confidentielles* ».

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Prévention des fuites de données confidentielles* ».

Les personnes concernées sont « *les employés* ».

Les fonctionnalités du traitement sont :

- la surveillance et l'analyse automatique du canal de communication des transferts de fichiers sortant vers les sites internet externes afin de vérifier l'absence ou l'existence d'une fuite de données ;
- la constitution de preuve en cas de litige.

A cet égard, la Commission appelle l'attention du responsable de traitement sur le fait que le traitement dont s'agit ne saurait être utilisé à une autre fin que la prévention des fuites de données confidentielles.

Sous cette réserve, 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 responsable de traitement indique que le traitement est justifié par le respect d'une obligation légale.

A cet égard, la Commission observe qu'il incombe à la banque de respecter le secret professionnel auquel elle est liée aux termes de l'article 308 du Code pénal, et le secret bancaire, qui est régi à Monaco par l'article L. 511-33 du Code monétaire et financier français.

Par ailleurs, elle relève que 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, applicable à Monaco (dans les limites de l'article 275), dispose à l'article 88 que « *les entreprises assujetties déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers. Elles veillent au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés* » et au c) de l'article 89 que « *l'intégrité et la confidentialité des informations sont en toutes circonstances préservées* ».

La Commission considère ainsi 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 objets du traitement sont :

- identité : numéro de matricule ;
- sites internet et données filtrées : URL des sites internet sur lesquels des *« uploads »* de fichiers ont été constatés, volume des « *uploads* » contenu du ou des fichiers uploadés, le nom du fichier, la date et l'heure de l' « *upload* », l'adresse IP du poste de travail à partir duquel l' « *upload* » a été effectué ;
- logs de connexions aux systèmes DLP (Data Leak Prevention) : identifiants de connexion et logs de connexion des personnels habilités à avoir accès au traitement ;
- alertes : réception des alertes automatiques DLP (Data Leak Prevention).

Les informations relatives à l'identité ont pour origine le traitement ayant pour finalité la « *Gestion administrative des salariés* », légalement mis en œuvre. Les autres informations sont générées par le système.

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 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, le responsable de traitement a joint un document intitulé *« Procédure « Informations Nominatives » »*.

A l'étude du document, la Commission observe que le document joint n'informe pas les personnes concernées conformément à l'article 14 de la Loi n° 1.165, modifiée, s'agissant notamment des catégories de destinataires des informations et de la finalité du traitement.

Par ailleurs, le responsable de traitement indique qu'il tient « *à la disposition de ses employés la listes des traitements automatisés portant sur leurs informations nominatives, reprenant pour chaque traitement les informations citées à l'article 14 de la loi 1.165 relative à la protection des 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.

Au vu de ce qui précède, la Commission demande que soit assurée l'information de l'ensemble des personnes concernées et que cette information soit effectuée conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

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

Le responsable de traitement indique que le droit d'accès s'exerce par voie postale ou sur place auprès du Chief Operating Officer.

La Commission considère 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, modifiée.

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

- ***Sur les personnes ayant accès au traitement***

Le responsable de traitement indique qu'ont accès au traitement dans le strict cadre de l'accomplissement de leurs missions de contrôle, techniques et de maintenance système :

- le service sécurité de la maison mère en Suisse (traitement des alertes niveau 1) : inscription, modification et consultation ;
- le coordinateur sécurité de Monaco et son suppléant (traitement des alertes niveau 2) : inscription, modification et consultation ;
- le Chief Executive Officer (CEO) et le Chief Operating Officer (COO) : consultation.

A cet égard, la Commission prend acte des précisions du responsable de traitement selon lesquelles le responsable de traitement est une filiale de BNP PARIBAS SUISSE SA, située en Suisse.

Elle prend également acte des précisions du responsable de traitement selon lesquelles « *une liste nominative des personnes ayant accès au traitement est tenue à jour* », et rappelle que cette liste doit lui être communiquée à première réquisition.

La Commission considère que ces accès sont justifiés.

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

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées aux autorités administratives et judicaires légalement habilitées.

La Commission considère que le Service d'Information et de Contrôle des Circuits Financiers (SICCFIN) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires d'informations nominatives traitées.

Par ailleurs, elle estime que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, la Commission rappelle qu'en cas de transmission, ces Autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

Sous ces réserves, elle considère que ces communications d'informations sont justifiées.

VI. Sur les interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion avec le traitement ayant pour finalité *« Gestion administrative des salariés »* et de deux rapprochements avec les traitements ayant respectivement pour finalités *« Gestion de l'identification et de la vérification des personnes soumises à la loi 1.362 du 3 août 2009 »* et « *Tenue des comptes de la clientèle* », tous légalement mis en œuvre.

La Commission estime que cette interconnexion est conforme aux exigences légales.

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'observations particulières.

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.

La Commission rappelle enfin que, conformément à l'article 17 de la Loi n° 1.165, modifiée, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement 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 sont conservées 1 an, à l'exception des informations relatives à l'identité de l'employé qui sont conservées 1 mois après départ de l'employé.

Par ailleurs, la Commission rappelle que dans le cadre de l'ouverture d'une procédure judiciaire, toute information nécessaire, notamment à des fins probatoires, pourra être conservée jusqu'au terme de la procédure.

Après en avoir délibéré, la Commission :

Rappelle que :

- la liste nominative des personnes ayant accès au traitement doit lui être communiqué à première réquisition ;

- le SICCFIN et la CCAF peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires des informations du traitement ;

- les Autorités judiciaires ne peuvent avoir accès aux informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- 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.

Demande que soit assurée l'information de l'ensemble des personnes concernées et que cette information soit effectuée conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

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 « *Prévention des fuites de données confidentielles* ».**

Le Président

Guy MAGNAN