Délibération n° 2024-012 du 17 janvier 2024

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« C*ontrôler, a posteriori, les transactions opérées sur les marchés boursiers aux fins de détection d'éventuels abus de marché* »,

présenté par UBP - Succursale de 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 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, 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, modifiée ;

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'Annexe à l'Ordonnance Souveraine n° 9.830 du 15 mars 2023 modifiant les annexes A et B de l'Accord Monétaire conclu le 29 novembre 2011 entre l'Union Européenne et la Principauté de Monaco ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 15 décembre 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 17 janvier 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Union Bancaire Privée (UBP) est la succursale à Monaco de UBP SA, établissement bancaire suisse (Genève), immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 14S06257, qui a pour activité « *la réalisation de toutes opérations de banque ou connexes telles que définies par la loi bancaire applicable (…)* ».

Cette société est, en raison de son activité, assujettie à la Loi n° 1.338 du 7 septembre 2007 relative aux activités financières, modifiée.

A ce titre, UBP (Succursale de Monaco) exerce une vigilance constante afin de s'assurer que les opérations de la clientèle ne contreviennent pas à la Loi précitée.

Ce traitement étant mis en œuvre à des fins de surveillance et portant sur des soupçons d'activités illicites, des infractions, des mesures de sûreté, il est donc soumis au régime de l'autorisation préalable 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 « *Contrôler, a posteriori, les transactions opérées sur les marchés boursiers aux fins de détection d'éventuels abus de marché* ».

Les personnes concernées sont les clients (personne physique et personne morale).

En outre, la Commission relève à la lecture du dossier que sont également concernés par le présent traitement les employés du responsable de traitement.

Le responsable de traitement indique que le traitement poursuit l'objectif suivant :

« Les contrôles de MARKET ABUSE DETECTION (« MAD ») visent à identifier les abus et tentatives d'abus de marché dans le but d'en tirer un profit personnel, pour le compte d'un employé ou pour le compte de clients de la banque, au travers des contrôles de scenarii suivants :

- *Insider Dealing, Insider Profit/Loss Avoidance : détecte l'exécution d'un ordre, en amont de la publication d'une information susceptible d'impacter le cours d'un titre coté sur les marchés, permettant à l'acheteur/vendeur du titre de tirer profit / d'éviter une baisse ;*
- *Wash Traiding : détecte les transactions en sens opposé résultant en une position neutre et visant à accroitre volontairement et artificiellement la liquidité d'un titre ;*
- *Suspicious Trading Volume : détecte une tentative de manipulation des prix marché (identification des comptes enregistrant un volume de transactions représentant plus de 10% du volume total échangé sur un même titre et au cours d'une même journée).* »

Ainsi, il appert à l'analyse du dossier et des pièces complémentaires que les fonctionnalités du traitement sont les suivantes :

- établissement d'un fichier accessible uniquement au service Compliance *« qui permet de recenser et tenir à jour la liste des clients les plus sensibles en matière d'abus de marché »* ;

- envoi d'un fichier avec l'ensemble des transactions de la journée précédente dans l'outil déployé pour l'identification d'éventuels abus de marché ;
- comparaison des transactions avec les informations des marchés selon les critères d'alertes définis, directement dans l'outil, par le département Compliance ;
- génération d'une alerte en cas de transaction apparaissant comme suspecte ;
- traitement de l'alerte par le département Compliance qui repose sur « *différents points de contrôle et d'attention* ». Il s'agit notamment de la consultation des informations générales relatives au client (profession, secteur d'activité), des informations relatives au profil transactionnel du client (investisseur ou non, appétence au risque) ainsi que des informations relatives au compte concerné par l'alerte et plus particulièrement son mode de gestion.

S'agissant de cette dernière fonctionnalité, le responsable de traitement indique que *« le traitement des alertes nécessite d'être attentif au contexte économique et politique dans lequel intervient la transaction* ». A cet égard, il précise que le collaborateur en charge du traitement de l'alerte peut également s'appuyer *« sur d'autres sources étant donné que les réseaux d'informations publiques (internet) sont aussi consultés si besoin* ».

De plus, la Commission constate que si les alertes sont générées à partir de scénarii contrôlés par des algorithmes, il y a nécessairement intervention humaine avant toute conséquence pour la personne concernée. Dès lors, les dispositions de l'article 14-1 de la Loi n° 1.165 sont respectées.

Enfin, s'agissant de la liste des clients sensibles en matière d'abus de marché, la Commission rappelle qu'elle doit s'établir sur des critères objectifs et que sa mise à jour ne doit pas conduire uniquement à l'incrémenter mais doit également permettre de sortir les clients de ladite liste lorsque les raisons de leur insertion initiale ne sont plus justifiées.

La Commission considère que la finalité du traitement est *« déterminée, explicite et légitime »,* conformément à 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 à laquelle il est soumis.

A cet égard, la Commission relève que la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée, comporte en son sein une section VI « *Des délits d'abus de marché* ».

En outre, il résulte des Ordonnances Souveraines successives modifiant les Annexes A et B de l'Accord monétaire conclu le 29 novembre 2011 entre l'Union européenne et la Principauté de Monaco, que le Règlement n° 2016/1033 du Parlement européen et du Conseil du 23 juin 2016 modifiant le règlement (UE) n° 600/2014 concernant les marchés d'instruments financiers, le règlement (UE) n° 596/2014 sur les abus de marché et le règlement (UE) n° 909/2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres est placé en Annexe A concernant la législation applicable à l'activité et au contrôle des établissements de crédit et à la prévention des risques systémiques dans les systèmes de paiement et les systèmes de règlement et de livraison de titres.

Enfin, en application de la Loi n° 1.362 précitée, le responsable de traitement est *« tenu d'identifier toute transaction constitutive d'une infraction sous-jacente au blanchiment de capitaux, dont l'abus de marché fait partie* ». La Commission relève comme évoqué au point II que l'analyse de la transaction peut s'effectuer à l'aune de sources disponibles sur Internet.

A cet égard, elle rappelle que, conformément à l'article 3 alinéa 4 de la Loi précitée, le responsable de traitement doit tenir uniquement compte :

- *« des facteurs inhérents aux clients, aux produits, services, canaux de distribution, du développement de nouveaux produits et de nouvelles pratiques commerciales, y compris les nouveaux mécanismes de distribution et l'utilisation de technologies nouvelles ou en développement en lien avec de nouveaux produits ou les produits préexistants ainsi qu'aux pays ou zones géographiques ;*
- *des documents, recommandations ou déclarations émanant de sources fiables, comme les organismes internationaux spécialisés dans la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive et la corruption ;*
- *de l'évaluation nationale des risques ; et*
- *des lignes directrices établies, selon les cas, par l'Autorité Monégasque de Sécurité Financière ou par le Conseil de l'Ordre des avocats-défenseurs et des avocats ».*

Ainsi, 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 :

- données d'identification électroniques : nom, prénom, adresse email professionnelle, numéro de téléphone professionnel ;
- informations temporelles : log de connexion, log de changement de configuration (dans l'application) ;
- fichiers des transactions et alertes : contexte transactionnel (numéro de compte, informations relatives à l'opération, informations relatives au marché, indicateur d'analyse de risque, valeur, horodatage des opérations,…), type d'alerte (nom de l'alerte, score, couleur,…).

Ces informations proviennent du système à l'exception des informations contenues dans l'alerte qui ont pour origine le fichier de gestion des opérations de marché poussé par le responsable de traitement dans l'outil.

Il est en outre précisé que le compliance officer se connecte aux autres traitements de l'établissement en lien avec le client concerné afin d'analyser le contexte de l'opération et d'effectuer en cas d'alerte avérée une déclaration de soupçons.

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 mention ou clause particulière intégrée dans un document remis à l'intéressé.

Ainsi, a été jointe au dossier la clause 23 des conditions générales relative à la « *Protection des informations nominatives* ». A sa lecture, la Commission considère que le document ne contient pas l'ensemble des dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993, notamment s'agissant de la finalité du traitement dont s'agit.

La Commission rappelle donc que l'information doit être préalable et 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 auprès du Service Conformité ou sur place.

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit s'effectuer dans le mois suivant la réception de la demande.

Sous cette réserve, 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 :

- le personnel habilité des Services Compliance : en consultation et traitement ;
- le personnel du Contrôle Permanent et Audit interne et externe : en consultation ;
- les administrateurs IT groupe habilités : en inscription, modification, mise à jour et consultation.

La Commission constate qu'il est fait recours à des prestataires. Elle rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993 les droits d'accès de ces derniers doivent être limités à ce qui est strictement nécessaire à l'exécution de leurs contrats de prestation de service. De plus, lesdits prestataires sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

Sous cette réserve, la Commission considère que ces accès sont justifiés au regard de la finalité du traitement.

Enfin, la Commission rappelle par ailleurs qu'en application de l'article 17-1 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 précise qu'elle doit lui être communiquée à première réquisition.

- **Sur les destinataires**

Le responsable de traitement indique que certaines informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires légalement habilitées.

A cet égard, la Commission rappelle que celles-ci ne peuvent avoir communication des informations objet du présent traitement que dans le strict cadre de leurs missions légalement conférées.

La Commission considère que de telles transmissions sont conformes aux exigences légales.

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

Le responsable de traitement indique que le présent traitement est interconnecté avec le traitement légalement mis en œuvre ayant pour finalité *« Gestion de l'identification et de la vérification des personnes soumises à la Loi n° 1.362 modifiée du 03 août 2009* ».

Le responsable de traitement indique également que le traitement fait l'objet d'un rapprochement avec le traitement légalement mis en œuvre suivant *« Tenue des comptes de la clientèle et les traitements des informations s'y rattachant par les établissements bancaires et assimilés »*.

La Commission considère que cette interconnexion et ce rapprochement sont conformes aux exigences légales.

Il appert en outre à l'étude du dossier que le présent traitement est rapproché avec les traitements suivants, légalement mis en œuvre :

- « *Valeurs mobilières et autres instruments financiers* » ;
- *« Gestion des déclarations de soupçons » ;*
- « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle* ».

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 que les ports non utilisés doivent être désactivés et que 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.

Par ailleurs, il convient de rappeler que les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.

Enfin, elle rappelle 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

Les données d'identification électronique sont conservées pendant *« toute la durée d'utilisation du système par l'employé et supprimées dans un délai de 3 mois après le départ du collaborateur ».*

Les logs de connexion sont effacés au bout de 1 an.

Enfin, le responsable de traitement indique que les autres données sont conservées *« 5 ans après la date d'exécution ».* La Commission prend toutefois acte que ledit délai ne sera applicable qu'au 6 janvier 2030, le responsable de traitement étant contraint de conserver sans suppression les informations jusqu'à cette date.

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

Après en avoir délibéré, la Commission :

Rappelle que :

- la liste des clients sensibles doit s'établir sur des critères objectifs et que sa mise à jour ne doit pas conduire uniquement à l'incrémenter mais doit également permettre de sortir les clients de ladite liste lorsque les raisons de leur insertion initiale ne sont plus justifiées ;

- pour l'identification et l'évaluation des risques de blanchiment de capitaux, de financement du terrorisme et de corruption, le responsable de traitement doit uniquement tenir compte des sources fiables, conformément à l'article 3 de la Loi n° 1.362 du 3 août 2009, modifiée ;

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

- la réponse au droit d'accès doit s'effectuer dans le mois suivant la réception de la demande ;

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

- les Autorités administratives et judiciaires légalement habilitées ne peuvent avoir communication des informations 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 ;

- les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.

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 UBP – Succursale de Monaco, du traitement automatisé d'informations nominatives ayant pour finalité *« Contrôler, a posteriori, les transactions opérées sur les marchés boursiers aux fins de détection d'éventuels abus de marché ».***

Le Président

Guy MAGNAN