Délibération n° 2024-171 du 11 septembre 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

« *Contrôles périodiques des informations relatives aux employés « sensibles » d'UBS (Monaco) S.A.* »

présenté par UBS (Monaco) S.A.

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention 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, 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, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive et la corruption ;

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 déposée par la UBS (Monaco) S.A., le 3 juin 2024, concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôles périodiques des informations relatives aux employés « sensibles » d'UBS (Monaco) S.A.* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 1er aout 2024 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 11 septembre 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

UBS (Monaco) S.A. est une société anonyme monégasque, immatriculée au répertoire du Commerce et de l'Industrie sous le numéro 56S00336, qui a pour activité « *dans la Principauté et à l'étranger, l'exploitation d'une banque (…)* ».

Cette société indique que « *conformément aux procédures internes du groupe UBS et afin de se prémunir de tous comportements incompatibles dans le cadre de leurs activités, UBS (Monaco) S.A. procède à des contrôles périodiques portant sur les casiers judiciaires ainsi que sur de potentiels évènements liés aux risques de criminalité financière* ».

Ledit traitement « *portant sur des soupçons d'activités illicites, des infractions, des mesures de sûreté* », il relève donc du régime de l'autorisation préalable visé à 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 « *Contrôles périodiques des informations relatives aux employés « sensibles » d'UBS (Monaco) S.A.* ».

Sont concernés « *un nombre limité d'employés spécifiquement identifiés selon une procédure interne au groupe UBS comme occupant des postes sensibles* ».

Les fonctionnalités du traitement sont les suivantes :

- tenue d'une liste des employés sensibles faisant l'objet d'une revue annuelle ;
- demander par email aux employés de se loguer à une plateforme afin de procéder à la communication des informations requises (casier judiciaire), ou directement par mail ;
- demander aux Autorités les casiers judiciaires ;
- rédiger des rapports ;
- effectuer screening de vérification sur l'application métier de la compliance afin d'identifier de potentiels évènements liés aux risques de criminalité financière ;
- effectuer des vérifications sur l'historique des adresses postales des salariés ;
- Si nécessaire, prendre des mesures à l'encontre du salarié.

Les vérifications sont effectuées tous les trois ans.

En ce qui concerne les demandes de casiers aux Autorités, la Commission renvoie au point II de la présente délibération.

Sous cette réserve, la Commission 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

Le responsable de traitement indique que le traitement est justifié par le respect d'une obligation légale à laquelle il est soumis, par l'exécution d'un contrat avec la personne concernée ainsi que par la réalisation d'un intérêt légitime, sans que ne soient méconnus les droits et libertés fondamentaux de la personne concernée.

La Commission relève qu'il n'y a pas en droit interne de dispositions qui obligeraient un salarié de banque à transmettre obligatoirement son casier judiciaire.

De plus, aucun élément présent au dossier ne permet d'étayer une justification fondée sur l'exécution d'un contrat.

La Commission relève néanmoins que la banque dispose d'un intérêt légitime à procéder aux vérifications objets du présent traitement, eu égard au secteur particulier dont s'agit qui nécessite une gestion des risques et des garanties quant à la prévention de tout acte en lien avec des infractions de corruption ou financières. Les acteurs du secteur bancaire peuvent aussi, en fonction de leur établissement, être soumis à des lois d'applications extraterritoriales, telles que le UK Bribery Act ou la Loi américaine Foreign Corrupt Practices Act de 1977 (FCPA).

Elle relève toutefois que la prévention de la corruption et la lutte contre le blanchiment de capitaux est encadrée à Monaco par la Loi n° 1.362 du 3 aout 2009, et son Ordonnance d'application.

A cet égard, l'article 30 de l'Ordonnance Souveraine n° 2.318 dispose qu'« *En application de l'article 27 de la loi n° 1.362 du 3 août 2009, modifiée, susvisée, les professionnels :*

1°) élaborent une classification des risques de blanchiment des capitaux et de financement du terrorisme présentés par leurs activités, selon le degré d'exposition à ces risques apprécié en fonction notamment de la nature des produits ou des services offerts, des conditions des transactions proposées, des canaux de distribution utilisés ainsi que des caractéristiques des clients ;
2°) déterminent, un profil de la relation d'affaires avec le client, permettant de détecter des anomalies dans cette relation, au regard des risques de blanchiment de capitaux ou de financement du terrorisme ;
3°) définissent les procédures à appliquer pour le contrôle des risques, la mise en œuvre des mesures de vigilance relatives à la clientèle, la conservation des pièces, la détection des transactions inhabituelles ou suspectes et le respect de l'obligation de déclaration au service exerçant la fonction de renseignement financier de l'Autorité, au Conseil de l'Ordre des avocats-défenseurs et avocats, selon les cas ;
4°) mettent en œuvre des procédures de contrôle, périodique et permanent, des risques de blanchiment de capitaux et de financement du terrorisme ;
5°) prennent en compte, dans le recrutement de leur personnel, selon le niveau des responsabilités exercées, les risques au regard de la lutte contre le blanchiment de capitaux et le financement du terrorisme ».

La Commission relève que l'application d'analyses en lien avec la lutte contre le blanchiment de capitaux n'est expressément prévue que lors de la procédure d'embauche et constate qu'en ce qui concerne l'organisation interne, la soumission des personnels des établissements bancaires aux vérifications n'est pas expressément prévue en Principauté.

Elle relève toutefois que des procédures doivent être mises en place eu égard aux risques de blanchiment et de corruption mais estime, conformément au 5° de l'article 30 susvisé ; que ces vérifications doivent en tout état de cause s'opérer eu égard au niveau de responsabilité exercé et au risque pesant sur la relation d'affaires, relativement au blanchiment et au risque de corruption.

A cet égard, la Commission relève que les opérations de vérifications concernent des personnels identifiés comme étant « *sensibles* », recensés sur une liste faisant l'objet d'une revue annuelle.

Les postes sensibles sont ceux :

- « *qui confèrent au collaborateur une autorité renforcée due à son rang ou à un accès privilégié aux systèmes, réseaux (…) ; ou*
- *dont on considère qu'ils exigent un niveau maximal d'intégrité personnelle* ».

Par ailleurs, elle relève que le présent traitement opère une différence de traitement entre les salariés résidents français (entendu comme salariés résidents en France) et les autres.

Il est en effet indiqué, « *concernant les employés non-résidents français »,* le prestataire qui effectue les vérifications pour le compte de la banque « *effectue les demandes auprès du service gouvernemental afin d'obtenir le casier judiciaire. Il procède par la suite à la vérification de celui-ci* ».

A contrario, concernant les salariés résidents en France, la banque ne peut qu'analyser les casiers transmis par les salariés.

La Commission demande à ce que le régime appliqué aux salariés résidents en France soit appliqué à l'ensemble des employés, en l'absence de justification particulière.

Elle estime que les personnes concernées doivent être informées des éventuelles conséquences si le salarié choisit de ne pas communiquer son casier judiciaire.

En effet, cette situation n'est envisagée que sous le prisme d'un risque « *d'escalade* » alors qu'il est indiqué au sein d'une annexe que « *toutes les données sont collectées et utilisées uniquement dans le but de réaliser la prestation (vérification des antécédents d'un candidat) et avec le consentement de la personne concern*ée ».

Ne sont indiquées au dossier que les seules conséquences qu'un salarié encourt en cas d'écart majeur entre les éléments qu'il fournit et les constatations opérées par la banque, à savoir :

- demander des explications à l'employé concerné ;
- contacter les services locaux Ressources Humaines et Compliance & Operational Risk Control pour information et demande de préconisation ;
- prendre les mesures adéquates telles qu'un changement de poste ou une restriction d'accès.

La Commission rappelle en outre qu'il doit y avoir une certaine corrélation entre la nature de la condamnation de l'employé et son métier au sein de la banque, toute condamnation ne devant pas entrainer par principe des conséquences à son égard.

Enfin, elle relève des pièces communiquées qu'une fois notifiée de la demande de communication de documents, la personne concernée dispose de dix jours ouvrés pour y répondre et les joindre, sous peine « *d'escalade* ». La Commission s'interroge sur un tel délai qui n'apparait pas compatible avec le temps nécessaire pour un salarié d'obtenir un extrait de casier judiciaire.

La Commission considère de ce fait qu'il ne peut y avoir de conséquence négative à l'encontre des salariés en cas de dépassement de délai pour des raisons administratives.

III. Sur les informations traitées

Le responsable de traitement indique que les informations exploitées aux fins du présent traitement sont :

- identité : nom, prénom, date de naissance, sexe, lieu de naissance, nationalité ;
- adresses et coordonnées : adresse postale, historique des adresses, email professionnel, numéro de téléphone ;

- formation, diplôme, vie professionnelle : rang interne UBS de l'employé, numéro d'identification de l'employé, langues parlées ;
- infractions, condamnations, mesures de sûreté, soupçon d'activités illicites : extrait de casier judiciaire de moins de trois mois.

La Commission constate que sont également collectés les éléments relevés par la banque en utilisant l'application de screening de la fonction Compliance, ainsi que les rapports rédigés par le prestataire en charge des opérations de vérification.

De plus, il résulte de l'analyse d'informations complémentaires que le responsable de traitement semble pouvoir demander des informations relatives à la solvabilité des personnes concernées « *sous réserve des lois en vigueur* ». Cette catégorie d'information n'est pas inscrite au sein du dossier soumis par le responsable de traitement. La Commission précise en tout état de cause que la collecte de telles données est disproportionnée eu égard à la finalité du traitement.

Sous cette réserve, 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 du 23 décembre 1993.

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 effectuée par le biais d'une mention ou clause particulière intégrée dans un document remis à l'intéressé, ainsi que par un document spécifique.

Ainsi, a été joint au dossier la « *notice d'information d'UBS à l'attention des salariés - Monaco* ». Il est indiqué au point 3.1 *« finalités de traitement »* point e) *« la conformité et le management du risque et/ou la prévention de la fraude, détection & enquêtes »* que la banque peut :

- « *entreprendre des vérifications sur vos antécédents dans le cadre du processus de recrutement des employés telles que la vérification de tout conflit d'intérêt existant ou potentiel ou tout autre obstacle susceptible de restreindre les activités ou les engagements d'un salariés au sein d'UBS ;*
- *entreprendre des vérifications périodiques si nécessaires* ».

La Commission relève à sa lecture que le document ne contient pas l'ensemble des mentions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993. Les éléments ne permettent pas pour les personnes concernées d'en déduire une finalité déterminée, explicite et légitime, du caractère obligatoire ou facultatif des réponses ; et des conséquences à leur égard d'un défaut de réponse.

La Commission demande donc que l'information préalable 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 droit d'accès s'exerce par courrier électronique auprès du Service des Ressources Humaines d'UBS (Monaco) S.A..

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

Elle rappelle en outre, que dans le cadre de l'exercice du droit d'accès par voie électronique 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.

A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières, comme rappelé dans sa délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous ces conditions, 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, modifiée.

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

- ***Sur les destinataires***

La Commission relève que le responsable de traitement indique ne pas communiquer d'informations à des destinataires au sens de la Loi n° 1.165 du 23 décembre 1993, modifiée.

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

Les personnes ayant accès au traitement sont :

- le prestataire au Royaume-Uni en inscription, consultation et maintenance ;
- le service Compliance & Operational Risk Control Monaco en consultation ;
- le Service Regional Vetting RH UBS en Pologne, en inscription, consultation ;
- le service RH UBS (Monaco) en consultation.

Ainsi, considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

La Commission rappelle 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.

Elle relève toutefois qu'il appert au sein du dossier la mention d'un sous-prestataire qui serait sis en Inde, mais dont les éventuels accès n'ont pas été reportés ni explicités dans les rubriques dédiées. Aussi, elle exclut tout accès éventuel d'un sous-prestataire indien en l'absence d'explication et de demande d'autorisation de transfert y associée.

VI. Sur les interconnexions

Le présent traitement fait l'objet d'interconnexions avec les traitements légalement mis en œuvre suivants :

- « *Gestion administrative des salariés* », pour « *lier les employés d'UBS (Monaco) S.A. et la gestion des habilitations informatiques* » ;
- « *Gestion et traçabilité des habilitations informatiques* », pour permettre les accès sécurisés au Système d'information d'UBS.

La Commission relève également que des informations sont échangées par le biais de la messagerie professionnelle, et que les personnels font l'objet d'un screening par le biais du logiciel utilisé par la Compliance et déjà soumis à formalité légale auprès de la CCIN. Elle en prend acte et considère que ces interconnexions et ce rapprochement sont conformes 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'observation particulière.

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.

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

La Commission rappelle également 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 sont conservées :

- 150 jours en ce qui concerne les screenings ;
- 12 mois chez le prestataire et au sein du Service Regional Vetting RH UBS avant d'être détruites pour les autres informations.

La Commission relève toutefois qu'en l'absence de texte permettant la conservation des casiers judiciaires, ces derniers doivent être supprimés dès la vérification opérée. Le responsable de traitement peut garder une traçabilité de l'opération en indiquant si la vérification a été opérée *via* un choix oui/non.

Sous cette réserve, la Commission considère que cette durée est conforme aux exigences légales.

Après en avoir délibéré, la Commission :

Demande que:

- les salariés soient informés des conséquences encourues en cas de non transmission des casiers judiciaires ;

- l'information préalable des personnes concernées soit conforme à l'article 14 de la Loi n° 1.165 ;

- en l'absence de justification particulière, le régime appliqué aux salariés résidents en France, à qui il appartient de communiquer les casiers judiciaires, soit appliqué à l'ensemble des employés, et que le responsable de traitement ne se procure pas les casiers judiciaires auprès des Autorités concernées ;

- ne soient pas collectées d'informations en lien avec la solvabilité des salariés ;

- les casiers judiciaires soient supprimés dès analyse de leur contenu et des conséquences y associées.

Rappelle que :

- toute condamnation d'un salarié ne doit pas entrainer par principe des conséquences à son égard ;

- 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 ;

- 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 ;

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

Exclut tout accès à un sous-prestataire éventuel situé en Inde.

Relève que le délai de 10 jours ouvrés pour transmettre les documents demandés sous peine *« d'escalade »* n'apparait pas cohérent avec les délais d'obtention dédits documents par les personnes concernées et qu'en conséquence il ne peut y avoir de conséquence négative à leur encontre en cas de transmission tardive pour des raisons administratives.

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 UBS (Monaco) S.A. du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôles périodiques des informations relatives aux employés « sensibles » d'UBS (Monaco) S.A.* ».**

Le Président,

Robert CHANAS