Délibération n° 2018-114 du 18 juillet 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

« *Notification de toute tentative de fraude ou fraude liée aux opérations de paiement par virement* »

présenté par UBS (Monaco) SA

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 et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, 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, modifiée, fixant les conditions d'application de la Loi n° 1.362 du 3 août 2009, susvisée ;

Vu l'Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprise 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 présentée le 18 avril 2018 par la Banque UBS (Monaco) SA, concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Notification de toute tentative de fraude ou fraude avérée liée aux opérations de paiement par virement* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation modificative notifiée au responsable de traitement le 15 juin 2018, 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 18 juillet 2018 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

UBS (Monaco) SA est une société anonyme monégasque enregistrée au RCI sous le numéro 56S0336, ayant pour objet « (…) *dans la Principauté de Monaco et à l'étranger, l'exploitation d'une banque, à cette fin elle peut effectuer toutes opérations bancaires, financières, commerciales, mobilières et immobilières et fournir tous services s'y rapportant, et, notamment les services d'investissement. Son activité s'étend principalement aux affaires habituelles de banques commerciales. La société peut fonder des représentations et des filiales en Principauté de Monaco et à l'étranger, des succursales, prendre des participations dans d'autres entreprises existantes ou à créer, été effectuer toutes opérations susceptibles de faciliter la réalisation et le développement de l'objet social dans le cadre et le respect de la législation en vigueur* ».

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 opérationnels dont font partie les risques de fraude ».*

A ce titre, « l*e fait de centraliser les incidents liés à la fraude permettra de renforcer l'analyse du risque et de mettre en place des contrôles plus appropriés* » et ce, « *afin de prévenir la réitération de cas de fraudes préjudiciables pour la clientèle et le groupe UBS* ».

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 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 « *Notification de toute tentative de fraude ou fraude avérée liée aux opérations de paiement par virement* ».

Le responsable de traitement précise qu'il concerne les clients, les collaborateurs, les bénéficiaires de la fraude/ tentative de fraude.

La Commission relève que sont également concernées : la personne qui commet la fraude ou la tentative de fraude et le client victime.

Les fonctionnalités sont :

- « *Traiter les informations relatives à une tentative de fraude ou à une fraude avérée dans le circuit de validation d'un ordre de paiement par virement ;*
- *Bloquer les tentatives d'opérations par virement dont les caractéristiques sont similaires et qui se présenteraient par la suite sur un ou plusieurs comptes d'un ou plusieurs clients ;*
- *Renforcement de la politique de lutte contre la fraude en ajoutant un niveau de contrôle ».*

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

Le responsable de traitement indique que le traitement est justifié par la réalisation d'un intérêt légitime (…) sans que ne soient méconnus l'intérêt et les droits et libertés fondamentaux des personnes concernées, notamment en ce qu'il vise à prévenir la réitération de cas de fraudes préjudiciables pour la clientèle et le Groupe UBS.

La Commission constate que le responsable de traitement se fonde sur l'article 94 de l'Arrêté du 3 novembre 2014, à cet égard elle considère que le traitement est également justifié par le respect d'une obligation légale.

Le responsable de traitement précise qu'il est nécessaire de mettre en place un « *système d'analyse et de mesures de risques opérationnels dont font partie les risques de fraude* » et ajoute que « *le fait de centraliser les incidents liés à la fraude permettra de renforcer l'analyse du risque et la mise en place de contrôles plus appropriés* ».

Il ajoute que l'alerte « *détectant une fraude ou une tentative de fraude se matérialise par une vérification humaine, le conseiller à la clientèle transmet l'information dès lors qu'il a un doute sur la provenance d'un email ou d'un appel téléphonique* ». Le collaborateur rappelle « *immédiatement la personne (call back) afin de s'assurer de la véracité de l'appel/email (…)* » et ajoute que « *L'outil CORISC recense les IBAN frauduleux. Ces derniers sont conservés pour une période de cinq ans afin pourvoir bloquer les éventuelles futures opérations relatives à ces IBAN* ».

Eu égard à l'objet social du responsable de traitement, et aux obligations qui lui incombent en application de l'Arrêté du 3 novembre 2014, 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 :
  collaborateur : travaillant sur le cas : nom, prénom,
  bénéficiaire : nom, prénom, nom de l'établissement bancaire,
  collaborateur complice de la tentative de fraude/fraude : nom, prénom,
  fraudeur si récupéré, communiqué : nom, prénom et toute éventuelle information communiquée par lui,
  client victime : nom, prénom si communiqué ;

- adresses et coordonnées : coordonnées téléphoniques ou électroniques à partir desquelles l'ordre a été donné, pays du bénéficiaire;

- caractéristiques financières : montant de la fraude ou tentative de fraude;

- données d'identification électronique :
  IBAN du compte bénéficiaire,
  GPN/Tnumber du collaborateur qui travaille sur le cas ;

- infractions, condamnations, mesures de sûreté, soupçons d'activités illicites : existence d'un cas de fraude ou tentative fraude, méthode de détection de la fraude ou de la tentative de fraude.

Les informations proviennent de précédents cas de fraudes ou tentatives de fraudes.

Aussi, 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 effectuée par une rubrique propre à la protection des données accessible en ligne.

La Commission n'ayant pas été destinataire du document, 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 informée conformément aux dispositions de 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 le droit d'accès est exercé sur place. La réponse se fera dans le mois suivant la réception de la demande.

La Commission constate ainsi 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.

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 :

- Service ORC d'UBS (Monaco) SA : notification par email des données concernées ;

- Service C&ORC Financial Crime Anti-fraud d'UBS SA (Suisse) : droits d'inscription, modification, mise à jour ;
- Conseiller clientèle : consultation ;
- Responsable du conseiller clientèle d'UBS (Monaco SA): consultation.

La Commission considère que le Service C&ORC Financial Crime Anti-fraud d'UBS SA (Suisse) a également accès en consultation.

Elle souligne que conformément à l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993, le responsable de traitement est tenu de « *déterminer nominativement la liste des personnes qui ont seul accès, pour les stricts besoins de l'accomplissement de leurs mission, aux locaux et aux installations utilisées pour les traitements, de même qu'aux informations traitées* ». Elle rappelle que cette liste doit être tenue à jour et précise qu'elle doit lui être communiquée à première réquisition.

Elle considère que ces accès sont justifiés.

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

Le responsable de traitement indique que les informations sont transmises aux Auditeurs internes et externes (commissaires aux comptes, cabinets d'audit) en déplacement sur le site de Monaco.

Il précise par ailleurs que les données sont transmises par messagerie interne sécurisée pour notification de tentative de fraude ou fraude au Service C&ORC Financial Crime Anti-Fraud d'UBS S.A. en Suisse pour saisie manuelle dans l'application CORISC chargée de détecter et filtrer automatiquement les opérations présentant un risque de non-conformité.

La Commission considère que ces communications sont conformes aux exigences légales.

VI. Sur les interconnexions avec d'autres traitements

Le responsable de traitement indique des interconnexions avec les traitements légalement mis en œuvre « *gestion et traçabilité des habilitations informatiques* », « *supervision des transactions des clients d'UBS* », « *gestion de la messagerie professionnelle d'UBS Monaco SA* » et « *la gestion des précontentieux et contentieux* ».

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.

Par ailleurs, la Commission rappelle que la copie ou l'extraction d'informations issues de ce traitement doit être chiffré sur son support de réception.

Enfin, elle rappelle par ailleurs 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 5 ans après l'opération.

Aussi, elle considère que la durée de conservation des informations est conforme à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

Après en avoir délibéré, la Commission :

Considère que le Service C&ORC Financial Crime Anti-fraud d'UBS SA (Suisse) a également accès aux données en consultation.

Rappelle que :

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

- la copie ou l'extraction d'informations issues de ce traitement doit être chiffré sur son support de réception ;

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

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) SA du traitement automatisé d'informations nominatives ayant pour finalité « *Notification de toute tentative de fraude ou fraude liée aux opérations de paiement par virement* ».**

Le Président

Guy MAGNAN