Délibération n° 2023-134 du 20 septembre 2023

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

« *Prévention des fuites de données* »

présentée par UBS (MONACO) S.A.

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 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 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'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 déclaration ordinaire n° 2006.01116 déposée par UBS (Monaco) S.A. le 16 novembre 2006 concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Messagerie électronique interne et externe* », et dont il a été délivré récépissé le 11 décembre 2006 ;

Vu la déclaration ordinaire n° 2006.01116 déposée par UBS (Monaco) S.A. le 16 avril 2014 concernant la mise en œuvre de la modification traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la messagerie professionnelle d'UBS (Monaco) S.A.* », et dont il a été délivré récépissé le 30 avril 2014 ;

Vu la Délibération n° 2014-57 du 12 mars 2014 de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre par UBS (Monaco) SA du

traitement automatisé d'informations nominatives ayant pour finalité « *Prévention des fuites de données confidentielles* » ;

Vu la Délibération n° 2017-205 du 15 novembre 2017 de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre par UBS (Monaco) SA de la modification du traitement automatisé d'informations nominatives ayant pour finalité *« Prévention des fuites de données »* ;

Vu la demande d'autorisation modificative déposée par UBS (Monaco) S.A., le 6 juin 2023, concernant le traitement automatisé d'informations nominatives ayant pour finalité « *Prévention des fuites de données* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 3 août 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 15 novembre 2017.

La Commission de Contrôle des Informations Nominatives,

Préambule

UBS (Monaco) S.A. est une société anonyme monégasque, enregistrée au RCI sous le numéro 56S00336, ayant pour activité *« 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 des 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, et 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* ».

Afin de prévenir tous risques inhérents à l'utilisation, par les collaborateurs, des canaux de communications électroniques (messagerie électronique, navigation Internet, ports USB, imprimantes…), UBS (Monaco) S.A. a mis en œuvre un traitement automatisé d'informations nominatives ayant pour finalité « *Prévention des fuites de données confidentielles* » autorisé par délibérations n° 2014-57 du 12 mars 2014 et n° 2017-205 du 15 novembre 2017.

Le responsable de traitement souhaite modifier le traitement dont s'agit et soumet cette modification à l'autorisation de la Commission en application de l'article 9 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

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

Il concerne *« tous les collaborateurs d'UBS (Monaco) S.A. (employés, prestataires, intérimaires, etc.) ».*

Le responsable de traitement indique que les fonctionnalités sont les suivantes :

« *Le présent traitement, à travers un logiciel installé sur le poste informatique de la personne concernée, et des logiciels installés sur les passerelles Internet et email externe, permet de réduire le risque de fuites de données sur les canaux de communication (messagerie électronique, internet, ports USB, imprimantes…).*

Ce traitement est destiné à prévenir le risque que des collaborateurs d'UBS (Monaco) S.A., autorisés à accéder à certaines données, puissent divulguer des informations en dehors de l'entreprise, accidentellement ou intentionnellement. Par exemple, si un utilisateur essaie de transmettre une présentation classifiée « Strictement confidentiel » à une adresse email non UBS, une alerte sera créée dans le système de traitement. Par ailleurs, le système prévoit le blocage d'envoi d'emails pour des cas identifiés à risque selon des critères définis par la direction d'UBS (Monaco) S.A.

A chaque envoi d'email vers l'extérieur de la banque et indépendamment de la sensibilité des informations, un message contextuel est proposé à l'utilisateur pour lui demander confirmation du transfert.

Le système de prévention des fuites de données ne se limite pas aux données clients mais s'étend à toutes les informations devant rester internes à UBS en général (comptes-rendus de réunions, documents concernant les règlementations de l'entreprise, les informations sur le personnel, le code source des applications, les documents de conception informatique…).

Ce traitement permet le respect de la confidentialité des données utilisées par UBS, le respect du secret bancaire ainsi que la protection des intérêts des clients ».

Le responsable de traitement indique que la liste des canaux de communication électronique *« est à considérer comme non exhaustive car les canaux de communications approuvés par UBS peuvent évoluer »*. La Commission en prend acte et rappelle que tout traitement d'informations nominatives doit, préalablement à sa mise en œuvre, faire l'objet d'une formalité auprès d'elle. A cet égard, elle recommande de faire apparaître, pour chaque finalité concernée (messagerie professionnelle, navigation Internet), l'existence d'une surveillance par un outil DLP et ainsi de soumettre lesdits traitements aux dispositions de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée. En effet, outre les mesures techniques propres à chaque outil, l'information préalable des salariés doit leur permettre d'identifier les comportements attendus dans l'utilisation de chaque environnement mis à leur disposition. A titre d'exemple, la Commission relève en outre que le DLP mis en œuvre par le responsable de traitement permet de connaître les informations liées aux flux https et donc potentiellement des informations de type messagerie privée si leur utilisation est autorisée. De ce fait l'information ne peut pas être générique à la mise en place d'un outil DLP et doit donc être adaptée à chaque outil.

Sous cette réserve, 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. <u>Sur la licéité et la justification du traitement</u>

Le responsable de traitement indique que le traitement est justifié par la réalisation d'un intérêt légitime, sans que soient méconnus ni l'intérêt ni les libertés et droits fondamentaux des personnes concernées.

A cet égard, il indique que « *ce traitement est justifié au regard de la confidentialité des données bancaires et des données en général. Il s'agit de protéger l'intérêt de la banque ainsi que celui des employés et des clients. Cela permet le fonctionnement de la banque de manière sécurisée* ».

En outre, il ajoute que :

- « *l'intérêt et les droits fondamentaux des personnes concernées sont respectés. En effet, les personnes concernées sont informées de l'existence du traitement et de toutes les autres obligations prévues à l'article 14 de la Loi n° 1.165. Les clients sont informés par des clauses présentes dans les conditions générales ;*
- *le présent traitement est indiqué dans le règlement intérieur et dans la procédure « Usage des outils de communications électroniques », annexe locale à la politique du Groupe UBS ;*
- *des mesures spécifiques sont prévues pour permettre l'identification et le traitement des emails personnels pour garantir le principe du secret de la correspondance* ».

Par ailleurs, la Commission observe qu'il incombe aux professionnels visés de respecter le secret professionnel auquel ils sont liés 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.

De surcroît, 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, dispose à l'article 270-3 *« les entreprises assujetties établissent par écrit une politique de sécurité du système d'information qui détermine les principes mis en œuvre pour protéger la confidentialité, l'intégrité et la disponibilité de leurs informations et des données de leurs clients, de leurs actifs et services informatiques. (…) En application de leur politique de sécurité du système d'information, les entreprises assujetties formalisent et mettent en œuvre des mesures de sécurité physique et logique adaptées à la sensibilité des locaux, des actifs et services informatiques, ainsi que des données ».*

A titre liminaire, la Commission considère que le traitement, dont la finalité est limitée à la prévention des fuites de données confidentielles, ne saurait conduire à une surveillance permanente et inopportune des salariés, et ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993.

Le responsable de traitement indique que l'ensemble des flux de données sortant de la Banque sont filtrés par rapport à des critères d'alerte intégrés dans l'outil DLP. En cas de potentielle fuite, une alerte sera générée. Celle-ci sera d'abord traitée par une équipe chargée du triage des alertes, afin d'éliminer les fausses positives. Si l'équipe considère qu'il s'agit d'un véritable incident, elle procède à une escalade auprès d'autres divisions de la Banque. A ce titre, le responsable de traitement explique que « *les équipes locales en charge de la gestion du risque business seront en charge, si nécessaire, de toute intensification des recherches afin de vérifier que les envois de données détectées ne constituent pas un cas de fuite de données* ».

Il est précisé que les équipes du responsable de traitement analysent d'abord les informations contenues dans l'alerte et ce n'est que dans l'hypothèse ou des investigations plus approfondies sont nécessaires que les emails et/ou fichiers ayant déclenchés les alertes seront étudiés.

Le responsable de traitement poursuit en expliquant que, « *dans le cas où une fuite de données est avérée, selon l'évaluation et la décision de la direction d'UBS (Monaco) S.A.,*

une sanction sera prise à l'encontre du collaborateur concerné conformément au Règlement Intérieur d'UBS (Monaco) S.A. et à la Convention Monégasque du Travail du Personnel des Banques ». La Commission en prend acte.

Par ailleurs, le responsable de traitement indique que les règles de détection des fuites de données sont validées par la Banque et peuvent évoluer par rapport à son appétence au risque.

En outre, le responsable de traitement a joint des extraits de la Policy du Groupe intitulée « *Usage des outils de communications électroniques* ». A la lecture du point 2.1.2 de celui-ci, la Commission constate que dans le cas où une communication personnelle a fait l'objet d'une alerte, et sous réserve de l'utilisation frauduleuse du caractère personnel pour masquer une fuite de données, le responsable de traitement se réserve le droit de demander au salarié qu'il ouvre ladite communication en présence d'un ou plusieurs membres de la direction. Enfin, il est précisé que si une communication n'est pas identifiée comme personnelle mais qui à la lecture a un contenu personnel *« la lecture doit être stoppée dès que la personne effectuant l'investigation se rend compte de son caractère personnel ».* La Commission en prend acte.

Aussi la Commission considère que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité/situation de famille : nom et prénom de la personne concernée et de son supérieur hiérarchique, nom des clients pour nourrir le système de blocage DLP (vue cryptée) ;
- adresses et coordonnées : adresse professionnelle, téléphone professionnel (issu de la signature de l'email) ;
- données d'identification électronique : adresse email du destinataire et de l'expéditeur GPN/Tnumber ;
- informations temporelles : date et heure de l'alerte, date et heure des actions effectuées par les équipes ;
- données filtrées : contenu du message, du ou des fichiers transmis ou de la saisie d'informations ;
- logs de connexion du système : connexions au système et aux données accédées par l'équipe DLP dans le cadre de l'utilisation de la plateforme technique ;
- rapports : contenu des données traitées, commentaires de l'équipe BRO pour suivi de la Direction.

Les informations relatives aux adresses et coordonnées, à certaines données identité/situation de famille et à certaines données d'identification électroniques sont issues du traitement ayant pour finalité « *Gestion des données du personnel* ». Les autres données relevant de la catégorie identité/situation de famille sont issues du traitement ayant pour finalité « *Tenue des comptes de la clientèle et le traitement des informations s'y rattachant* » et les autres données d'identification électronique proviennent du traitement ayant pour finalité « *Gestion de la messagerie professionnelle d'UBS* ». Enfin, les informations temporelles, les données filtrées, les logs de connexion et les rapports ont pour origine le système lui-même, les contenus analysés et les équipes en charge de l'exploitation de l'outil.

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 des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est assurée au moyen d'un document spécifique, d'une mention ou clause particulière intégrée dans un document remis à l'intéressé ainsi que d'une information disponible sur le site Internet d'UBS (Monaco) S.A.

A cet égard, le responsable de traitement a joint un document intitulé *« Projet d'amendement du Règlement Intérieur – 2023 ».*

A l'examen du document, la Commission observe qu'il informe les personnes sur l'existence d'un outil DLP en indiquant les canaux de communication électronique qui sont surveillés.

Toutefois, la Commission constate que ce document n'informe pas conformément à l'article 14 de la Loi n° 1.165, notamment s'agissant des destinataires et des droits dont disposent les personnes concernées ainsi que de leurs modalités d'exercice.

Par ailleurs, le responsable de traitement a également joint au dossier plusieurs extraits de la « *Charte d'usage des outils de communication électronique ».*

A l'analyse desdits documents, la Commission relève qu'ils fournissent une information plus détaillée sur le fonctionnement de l'outil DLP ainsi que sur les comportements attendus des personnes concernées dans le cadre de l'utilisation de la messagerie professionnelle et de la navigation Internet, sans préciser les comportements attendus dans l'utilisation des imprimantes, des ports USB ainsi que de la gravure des CD/DVD.

En outre, la Commission relève que le responsable de traitement dresse une liste des destinataires, des informations issues du présent traitement, au point *« 2.3 Accès à la donnée* » de la Charte.

Toutefois, à l'examen de ces documents, la Commission constate l'absence de mention relative aux droits des personnes concernées et à leurs modalités d'exercice.

Au regard de ce qui précède, la Commission demande que soit assurée l'information de l'ensemble des personnes concernées et qu'elle soit adaptée à chaque outil mis à la disposition des salariés, complète, préalable et conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

- ***Sur l'exercice du droit d'accès***

Le droit d'accès s'exerce par voie postale, sur place ou par courrier électronique auprès du Service des Ressources Humaines d'UBS (Monaco) S.A.

S'agissant de l'exercice du droit d'accès, 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 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.

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

- ***Sur les accès au traitement***

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

- le Service DLP Triage, basé en Suisse en consultation ;
- le Support local Monaco : le Responsable de la Sécurité des Systèmes d'Information (RSSI) et le Service Business Risk Organization en consultation en support de l'équipe DLP Triage ;
- le Service Operational Risk Control (ORC) en consultation (contrôles de 2ème niveau) ;
- le Service Informatique en maintenance (les données d'alertes sont cryptées et non accessibles par le Service Informatique) ;
- le Service SOC d'UBS Business Solutions, basé en Suisse pour la supervision des événements de sécurité du système ;
- le Service des Ressources Humaines en consultation si nécessaire ;
- la Direction d'UBS (Monaco) S.A. en consultation si nécessaire ;
- le collaborateur et son supérieur hiérarchique dans le cadre de l'évaluation d'une potentielle fuite de données.

La Commission considère que ces accès sont conformes aux exigences légales et sont justifiés au regard de la finalité du traitement.

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

La Commission estime que les informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires légalement habilitées et rappelle que celles-ci ne peuvent avoir communication des informations objet du présent traitement que dans le strict cadre de leurs missions légalement conférées.

VI. Sur les interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement est interconnecté avec les traitements, légalement mis en œuvre, ayant pour finalité respective :

- « *Gestion et traçabilité des habilitations informatiques* » ;
- « *Gestion des données du personnel* » ;
- « *Gestion de la messagerie professionnelle d'UBS (Monaco) S.A.* » ;
- « *Tenue des comptes de la clientèle et le traitement des informations s'y rattachant* ».

La Commission relève que le traitement relatif à la *« Gestion de la messagerie professionnelle d'UBS (Monaco) S.A. »,* a fait l'objet d'une déclaration ordinaire sans mention d'une quelconque finalité de surveillance. Afin que la finalité de ce traitement soit « *déterminée, explicite et légitime* », et comme indiqué au point I de la présente délibération, la Commission demande que ladite déclaration soit modifiée dans les meilleurs délais et soit soumise au régime de demande d'autorisation.

Sous cette réserve, la Commission considère que ces interconnexions 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.

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 informations nominatives collectées sont conservées 1 an ou sur la durée d'une investigation.

Aussi, la Commission considère que cette durée de conservation est conforme aux exigences légales.

Après en avoir délibéré, la Commission :

Rappelle que :

- le présent traitement ne doit pas conduire à une surveillance permanente et inopportune des salariés ;

- le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993 ;

- tout traitement d'informations nominatives doit, préalablement à sa mise en œuvre, faire l'objet d'une formalité auprès de la Commission ;

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

- 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 ;

- les Autorités administratives et judiciaires ne peuvent avoir accès aux informations objet du présent traitement que dans le strict cadre des missions légalement conférées.

Demande que :

- la déclaration ordinaire n° 2006.01116 soit modifiée dans les meilleurs délais et soit soumise au régime de demande d'autorisation ;

- soit assurée l'information de l'ensemble des personnes concernées et qu'elle soit adaptée à chaque outil mis à la disposition des salariés, complète, préalable et conforme 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) S.A. de la modification du traitement automatisé d'informations nominatives ayant pour finalité « *Prévention des fuites de données* ».**

Le Président

Guy MAGNAN