Délibération n° 2017-065 du 19 avril 2017

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

« *Gestion et traçabilité des habilitations informatiques* »

présenté 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 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° 1.338 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, modifiée, susvisée ;

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, 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 Recommandation CM/Rec(2015)5 du Conseil de l'Europe du 1er avril 2015 sur le traitement des données à caractère personnel dans le cadre de l'emploi ;

Vu la demande d'autorisation déposée par UBS SA (Suisse) représentée à Monaco par UBS (Monaco) S.A., le 7 février 2017, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Gestion et traçabilité des habilitations informatiques* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 5 avril 2017, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 19 avril 2017.

La Commission de Contrôle des Informations Nominatives,

Préambule

UBS SA est une société suisse disposant à Monaco d'une filiale, UBS (Monaco) S.A., afin d'accomplir ses formalités légales.

Lors de sa séance plénière du mois de février 2016, la Commission a estimé que seuls les responsables de traitements qui n'étaient pas établis à Monaco devaient choisir un représentant établi à Monaco.

En l'espèce, UBS SA est établie à Monaco par le biais de sa filiale à 99,9% UBS (Monaco) S.A. enregistrée au RCI sous le numéro 56S00336, ayant pour activité « *dans la Principauté et à l'étranger, l'exploitation d'une banque (…)* ».

Dans le cadre de son organisation interne, et afin d'assurer la sécurité informatique de son réseau, la banque souhaite mettre en œuvre un traitement ayant pour finalité « *Gestion et traçabilité des habilitations informatiques »*.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance. Il relève donc du régime de l'autorisation préalable visé à l'article 11-1 de la Loi n° 1.165, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement soumis a pour finalité « *Gestion et traçabilité des habilitations informatiques* ».

Il concerne les salariés et les prestataires externes bénéficiant d'un code d'identification.

Les fonctionnalités sont les suivantes :

« *La gestion des habilitations suppose :*

- *la description de la sécurité et des accès aux applications et répertoires partagés utilisés au sein d'UBS Monaco et du groupe UBS ;*
- la définition des différents types d'accès ;
- la définition et la description des rôles permettant l'accès à un ensemble d'applications/répertoires ;
- *la gestion des autorisations d'accès aux applications (demande, approbation, annulation) ;*
- *l'inventaire et la revue des droits d'accès des employés pour permettre l'évolution de droits, mobilités internes et départs ;*

La traçabilité des habilitations suppose :

- *la collecte automatique des évènements systèmes liés à la sécurité du système d'information ;*
- *l'identification des évènements considérés à risque pour mettre en place une réponse adaptée en termes de sécurité des systèmes informatiques et des installations de la banque ;*
- *la protection des intérêts de la banque notamment pour lutter contre les pratiques contraires ;*
- *permettre d'utiliser les évènements comme preuve à fournir aux autorités judiciaires et administratives légalement habilitées en cas de litige potentiel ;*
- *surveiller les accès non autorisés sur les systèmes (ex : un utilisateur essayant de se connecter sur un système sans avoir l'autorisation), les accès non appropriés sur les systèmes (ex : un utilisateur effectuant une action qui n'est pas en conformité avec les procédures UBS), une attaque Distributed Denial of Service (DDoS), la détection d'une vulnérabilité zero-day, une infection d'un système par malware ou un virus (…) ».*

La Commission considère que la finalité du traitement est 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 le respect d'une obligation légale et 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 le présent traitement permet :

- « *de s'assurer que les salariés ont accès uniquement aux applications dont ils ont besoin pour effecteur leur travail en fonction de leurs attributions et rôles respectifs ;*
- *de gérer le type d'accès qui est donné au salarié afin que celui-ci n'ait que l'accès dont il a besoin selon les principes de moindre privilège ;*
- *une supervision de la sécurité des systèmes d'information efficace et réactive (…) pour garantir l'intégrité et la confidentialité des informations critiques d'UBS (Monaco) S.A. (…) ».*

Par ailleurs, la Commission relève qu'en effet l'article 11 du Titre II - Le système de contrôle des opérations et des procédures internes - de l'Arrêté susvisé prévoit des obligations « *de vérifier les conditions d'évaluation, d'enregistrement, de conservation et de disponibilité de [l'information comptable et financière] notamment en garantissant l'existence de la piste d'audit au sens de l'article 85* » et de « *vérifier la qualité des systèmes d'information et de communication* », et que les articles 6, 7 et 11 de l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 contiennent des dispositions comparables.

En outre en l'absence de précision quant aux libertés et droits fondamentaux des personnes concernées et notamment des salariés de la banque, la Commission demande que le responsable de traitement s'assure que les personnes concernées bénéficient d'une information préalable claire quant à l'existence du traitement dont s'agit, aux droits dont elles disposent relativement au traitement et à leurs modalités d'exercice.

Aussi, elle 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 : nom, prénom du salarié concerné, du responsable hiérarchique, [de la personne qui valide], du salarié qui effectue la demande ;
- adresses et coordonnées : coordonnées professionnelles (adresse, numéro de téléphone) ;
- formation-diplôme-vie professionnelle : fonction, service, responsable hiérarchique ;
- données d'identification électronique : numéro d'identification interne (GPN ou T number) ;
- logs d'accès : logs, évènement système, horodatage ;
- autorisation : type d'autorisation donnée, statut de l'autorisation (active, expiring, …) durée de l'autorisation, justification de la demande d'accès à une application.

A l'exception des logs d'accès qui sont générés par le système et des autorisations qui ont pour origine le salarié qui effectue la demande, les informations proviennent du traitement ayant pour finalité « *Gestion des données du personnel* », légalement mis en œuvre.

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 assurée au moyen d'une mention ou clause particulière intégrée dans un document remis à l'intéressé, par une procédure interne accessible en Intranet et une mention particulière intégrée dans un document d'ordre général.

Toutefois, les documents susvisés n'étant pas joints à la présente demande, la Commission n'est pas en mesure de s'assurer que l'information préalable des salariés est conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 et que les prestataires en bénéficient également de manière effective.

Aussi elle rappelle que l'information de l'ensemble des personnes concernées doit être assurée conformément à 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 :***

Les droits d'accès, de modification, de mise à jour et de suppression s'exercent par voie postale ou sur place auprès du Service des Ressources Humaines d'UBS (Monaco) S.A.

Le délai de réponse est de 30 jours.

La Commission considère donc 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 que :

- pour la gestion des habilitations

- les groupes BBS Opérations et BBS Autorisation Solution (basés à UBS AG (Suisse)) ont accès aux informations en inscription, modification, mise à jour et consultation dans le strict cadre de de la gestion des autorisations dans BBS. Ces groupes n'interviennent pas dans la gestion des habilitations effectuée dans les applications, une fois que les actions autorisées dans BBS ont été approuvées ;
- le groupe BBS Reporting (basé à UBS AG (Suisse)) a accès aux informations en consultation, dans le cadre de la fourniture de rapports à l'occasion de contrôles périodiques ;
- le Chef de projet et Role Owner est basé à Monaco, et a accès aux informations en inscription, modification, mise à jour et consultation, dans le cadre de la mise en place ou de la maintenance du processus d'autorisation BBS ;
- les salariés du groupe UBS ont accès aux informations en inscription, modification, mise à jour et consultation, mais seulement dans le strict cadre des informations les concernant, aux fins d'obtenir les habilitations informatiques conformément à leur fonction au sein du groupe UBS ;
- les approbateurs des applications monégasques sont basés à Monaco et ont accès aux informations en inscription, modification, mise à jour et consultation dans le cadre de la validation des habilitations informatiques des employés ;
- pour les applications monégasques dont la gestion des habilitations reste manuelle, la mise en place des droits effectifs est effectuée par le service Informatique, basé à Monaco, une fois toutes les autorisations obtenues dans BBS.

- pour la traçabilité

- les administrateurs des systèmes informatiques (basés tant à UBS UK, Suisse et Monaco) n'ont pas vocation à modifier les données mais ont accès aux informations en consultation et ont la possibilité d'y avoir accès en modification, au regard des droits nécessaires à la bonne supervision des systèmes informatiques ;
- le personnel en charge de la supervision des alertes (basé à UBS Suisse) n'a pas vocation à modifier les données mais a accès aux informations en consultation. Ce service a la possibilité d'y avoir accès en modification. Ses droits concernent le triage des alertes ;
- le département de la sécurité des systèmes d'information (basé à Monaco) a accès aux informations en consultation. Ses droits concernent la revue des alertes considérées à risque et nécessitant une analyse approfondie.

La Commission souligne qu'en cas de recours à des prestataires, leurs accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, conformément à l'article 17 de la Loi n° 1.165. De plus ils sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement.

Elle rappelle enfin 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 que cette liste doit lui être communiquée à première réquisition.

Elle considère que ces accès sont justifiés.

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

Le responsable de traitement déclare que des informations peuvent être communiquées à la Direction de la Sûreté Publique à Monaco, aux Tribunaux et Cours à Monaco et à l'ACPR en France (pour la traçabilité uniquement), au personnel administrateur des systèmes informatiques et au personnel en charge de la supervision des alertes au Royaume-Uni et en Suisse.

La Commission considère que ces communications d'informations sont justifiées.

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

Le responsable de traitement indique que le présent traitement est interconnecté avec 21 traitements et qu'il fait l'objet de rapprochements avec 12 traitements légalement mis en œuvre et dont la liste a été jointe au dossier.

La Commission considère que le présent traitement pourra également être interconnecté à tous traitements futurs d'UBS (Monaco) S.A. à des fins de sécurité.

Aussi, elle constate qu'un traitement ayant pour finalité « *Gestion des habilitations* » a été légalement mis en œuvre en la forme ordinaire.

A cet égard, la Commission rappelle qu'il appartient, le cas échéant, au responsable de traitement de radier le traitement ayant pour finalité « *Gestion des habilitations* », conformément à l'article 10 de la Loi n° 1.165 du 23 décembre 1993.

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 :

- pour la durée d'emploi du salarié ou 1 an après une décision devenue définitive ou l'écoulement du délai de prescription s'agissant des informations relevant des catégories « *identité* » et « *autorisations* » ;

- pour la durée d'emploi du salarié pour les informations issues des catégories « *adresses et coordonnées* » et « *formation-diplôme-vie professionnelle* » ;
- jusqu'à 12 mois après le départ du salarié ou changement de service pour les « *données d'identification électroniques* » ;
- 12 mois à compter de la collecte des données ou 1 an après une décision devenue définitive ou l'écoulement du délai de prescription pour les logs d'accès.

La Commission considère que certaines de ces durées de conservation sont imprécises ou disproportionnées au regard de la finalité du traitement.

Aussi, elle fixe les durées de conservation ainsi que suit :

- 3 mois maximum après le départ de l'employé s'agissant des données relevant des catégories « *identité* » et « *adresses et coordonnées* » ;
- la durée de la relation contractuelle avec l'employé ou de son affectation à un service (étant entendu que les habilitations devront être supprimées immédiatement après la fin du contrat de travail ou dès le changement de service), s'agissant des « *données d'identification électroniques* » ;
- 1 an maximum à compter de leur collecte, s'agissant des « *logs d'accès* » ;
- la durée de l'autorisation conférée, s'agissant des « *autorisations* ».

Après en avoir délibéré, la Commission :

Considère que le présent traitement pourra également être interconnecté à tous traitements futurs d'UBS (Monaco) S.A. à des fins de sécurité ;

Rappelle que :

- l'information de l'ensemble des personnes concernées doit être assurée conformément à l'article 14 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 doit lui être communiquée à première réquisition ;

- il appartient, le cas échéant, au responsable de traitement de radier le traitement ayant pour finalité « *Gestion des habilitations* » ;

- 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.

Demande que le responsable de traitement s'assure que les personnes concernées bénéficient d'une information préalable claire quant à l'existence du traitement dont s'agit, aux droits dont elles disposent relativement au traitement et à leurs modalités d'exercice ;

Fixe la durée de conservation des informations ainsi que suit :

- 3 mois maximum après le départ de l'employé s'agissant des données relevant des catégories « *identité* » et « *adresses et coordonnées* » ;

- la durée de la relation contractuelle avec l'employé ou de son affectation à un service (étant entendu que les habilitations devront être supprimées immédiatement après la fin du contrat de travail ou dès le changement de service), s'agissant des « *données d'identification électroniques* » ;

- 1 an maximum à compter de leur collecte, s'agissant des « *logs d'accès* » ;

- la durée de l'autorisation conférée, s'agissant des « *autorisations* ».

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 « *Gestion et traçabilité des habilitations informatiques* ».**

Le Président

Guy MAGNAN