DELIBERATION N° 2014-57 DU 12 MARS 2014 DE LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES PORTANT AUTORISATION A LA MISE EN ŒUVRE DU TRAITEMENT AUTOMATISE D'INFORMATIONS NOMINATIVES AYANT POUR FINALITE « *PREVENTION DES FUITES DE DONNEES CONFIDENTIELLES* » PRESENTE PAR UBS (MONACO) S.A.

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, et son Ordonnance Souveraine d'application ;

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 ;

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 le Règlement CRBF n° 97-02 du 21 février 1997, modifié, relatif au contrôle interne des établissements de crédit et des entreprises d'investissement, applicable à Monaco ;

Vu la Recommandation du Conseil de l'Europe n° R(89)2 du 19 janvier 1989 sur la protection des données à caractère personnel utilisées à des fins d'emploi ;

Vu le Code pénal monégasque et le Code monétaire et financier français ;

Vu la demande d'autorisation déposée par la UBS (Monaco) S.A. le 24 décembre 2013 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Prévention des fuites de données confidentielles* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 17 février 2014, conformément à l'article 11-1 de la Loi n° 1.165, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 12 mars 2014 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

UBS (MONACO) S.A. est une société anonyme ayant pour activité « *dans la Principauté et à l'étranger l'exploitation d'une banque (…)* ».

Afin de prévenir tous risques inhérents à l'utilisation, par les employés, des canaux de communications électroniques (messagerie électronique, internet, ports USB …), UBS (Monaco) S.A. souhaite mettre en œuvre un système destiné à prévenir les fuites de données confidentielles.

A ce titre, en application de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, relatif à la mise en œuvre de traitements automatisés d'informations nominatives « *à des fins de surveillance* » ou « *portant sur des soupçons d'activités illicites, des infractions* », UBS (Monaco) S.A. soumet la présente demande d'autorisation concernant le traitement ayant pour finalité « *Prévention des fuites de données confidentielles* ».

I. Sur la finalité et les fonctionnalités du traitement

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

Les personnes concernées sont « *les employés et prestataires de services internes et les destinataires des emails* ».

A l'examen du dossier, la Commission considère que les fonctionnalités du traitement sont :

- la surveillance des canaux de communication (messagerie électronique, navigation internet, connexions internet sécurisées, transferts de fichiers, ports USB, gravure CD/DVD et impressions) ;
- la sélection automatique d'emails envoyés à une adresse email externe à UBS aux fins de lecture par le Service du contrôle permanent et de la conformité ;
- l'analyse automatique des données envoyées vers les canaux de communication externes à UBS (Monaco) S.A. afin de vérifier l'absence ou l'existence d'une fuite de données ;
- la constitution de preuve en cas de litige.

Par ailleurs, elle appelle l'attention du responsable de traitement sur le fait que le traitement dont s'agit ne saurait être utilisé à une autre fin que la prévention des fuites de données confidentielles.

Enfin, elle considère que la finalité est déterminée, explicite et légitime, conformément à l'article 10-1 de la Loi n° 1.165, modifiée.

II. Sur la licéité du traitement

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 L511-33 du Code monétaire et financier français.

Par ailleurs, elle relève que le Règlement CRBF n° 97-02 du 21 février 1997, modifié, relatif au contrôle interne des établissements de crédit et des entreprises d'investissement, applicable à Monaco (à l'exception de ses articles 11-7, 38-1 et 42 – cf. art. 46), dispose à l'article 14 alinéa 1er que « *les entreprises assujetties déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers. Elles veillent au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés* » et au c) du même article qu' « *en toutes circonstances sont préservées l'intégrité et la confidentialité des informations* ».

En conséquence, la Commission considère que le traitement est licite, conformément aux dispositions légales.

III. Sur la justification du traitement

Le responsable de traitement indique que le traitement est justifié par la réalisation d'un intérêt légitime poursuivi par le responsable de traitement, et ne méconnaît ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

A cet égard, il précise « *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* ».

Par ailleurs, la Commission considère que les mesures mises en place par le responsable de traitement doivent être strictement nécessaires au but recherché.

En l'espèce, la Commission relève que la « *Charte d'usage des outils de communication électronique à destination des salariés* » décrit le système de prévention des fuites de données (Data Leakage Prevention – « DLP ») ainsi que suit :

« *Ce système consiste à [exécuter un] logiciel sur les postes de travail ou les ordinateurs portables destiné à surveiller les canaux de communication comprenant la messagerie électronique, les connexions internet standard (http) ou sécurisées (https), les transferts de fichiers, les ports USB, la gravure CD/DVD et les systèmes d'impression. A ce titre, les données envoyées vers les canaux de communication externes à UBS (Monaco) S.A. seront analysées automatiquement afin de vérifier qu'elles ne constituent pas un cas de fuite de données* ».

En ce sens, le responsable de traitement précise que si tel est le cas, « *une alerte est transmise à l'équipe d'intervention DLP sous une forme anonyme où un premier tri sera effectué afin d'éliminer les fausses alertes* » et qu' « *en cas de détection potentielle d'une fuite (…) une investigation plus approfondie sera conduite par le Service du contrôle permanent et de la conformité* » lequel aura alors la possibilité de visualiser l'intégralité des contenus.

Par ailleurs, si la fuite de données est avérée, il indique que des sanctions seront prises conformément au règlement intérieur d'UBS (Monaco) S.A. et à la Convention Collective Monégasque du Travail du Personnel des Banques.

A cet égard, la Commission observe qu'au point 8 d'un document intitulé « *Prévention des fuites de données (Data Leakage Prevention) : Foire Aux Questions* », le responsable de traitement informe que « *la supervision réalisée respecte les législations des différentes juridictions où UBS est implantée. La supervision ne sera pas mise en place en tout lieu où l'accord légal adéquat ne sera pas obtenu* ».

Ainsi, elle prend acte de ces éléments et renouvelle les principes par elle posés dans sa délibération de ce jour autorisant la mise en œuvre par UBS (Monaco) S.A. du traitement ayant pour finalité la « *Gestion de la procédure de revue des emails dans le cadre d'un litige ou sur demande d'une autorité compétente* » et rappelle à cet égard « *qu'en toutes hypothèses l'ouverture d'un email personnel du salarié sans son consentement ne saurait être effectuée hors les cas expressément et limitativement prévus par la loi* ».

Au vu de l'ensemble de ces éléments, la Commission considère que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165, modifiée.

IV. Sur les informations traitées

Les informations objets du traitement sont :

- identité : nom, prénom ;
- adresses et coordonnées : adresse professionnelle
- données d'identification électronique : adresse email du destinataire et de l'expéditeur ;
- 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.

Elles ont pour origine le traitement, légalement mis en œuvre, dénommé « *HRI* » ayant pour finalité la « *Gestion des données du personnel* » (pour l'expéditeur), Microsoft Exchange (pour le destinataire) et l'application Endforce Platform (pour les logs de connexion).

La Commission considère que ces informations 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.

V. Sur les droits des personnes concernées

➢ ***Sur l'information des personnes concernées***

L'information préalable des personnes concernées est effectuée au moyen d'un document spécifique, d'une mention ou clause particulière intégrée dans un document remis à l'intéressé et un courrier adressé à l'intéressé.

A cet égard, le responsable traitement a joint au dossier copies du « *disclaimer email* », d'un extrait du contrat de travail et du règlement intérieur et une note d'information à l'intention des salariés.

A l'examen de ces éléments, la Commission constate qu'ils ne sont pas conformes aux dispositions de l'article 14 de la Loi n° 1.165, modifiée, et elle demande que chaque catégorie de personnes concernées soit valablement informée, et au sein d'un même document, de l'intégralité des éléments suivants :

- l'identité du responsable de traitement ;
- la finalité du traitement ;
- l'existence d'un droit d'accès et de rectification des informations les concernant.

- ***Sur l'exercice des droits d'accès, de rectification et d'opposition***

L'exercice du droit d'accès, de modification, de mise jour ou de suppression des données, s'exerce sur place auprès du Service des Ressources Humaines d'UBS Monaco S.A.

La réponse à la demande de droit d'accès est effectuée dans un délai de 30 jours.

A cet égard, la Commission considère que certains destinataires des emails, en raison notamment de leur éloignement de la Principauté de Monaco, ne sont pas en mesure d'exercer de manière effective ces droits.

Par ailleurs, elle demande que le responsable de traitement s'assure que le Service des Ressources Humaines d'UBS Monaco S.A. est valablement habilité pour recevoir les demandes de droit d'accès de l'ensemble des personnes concernées.

Elle demande donc que les personnes concernées soient en mesure d'exercer leurs droits de manière effective et que les modalités d'exercice de ces droits figurent expressément dans la mention insérée en bas des messages électroniques sortants.

VI. Sur les personnes ayant accès au traitement

Les Services legal & compliance et du contrôle permanent et de la conformité (LRU) ont accès aux informations en consultation. La Direction dispose également d'un tel accès lorsque l'alerte est confirmée.

Par ailleurs, le service informatique, sous la supervision du responsable de la sécurité des systèmes d'information (LRSO) ont accès aux informations en modification et mise à jour.

Concernant les services susvisés, la Commission observe qu'ils sont expressément visés par la « *Charte d'usage des outils de communication électronique à destination des salariés* ».

Par ailleurs, elle rappelle qu'en application de l'article 17-1 de la Loi n° 1.165, modifiée, la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et doit pouvoir lui être communiquée à première réquisition.

Enfin, elle considère que ces accès sont justifiés.

VII. Sur les interconnexions avec d'autres traitements

Le responsable de traitement indique des interconnexions avec les traitements ayant respectivement pour finalité la « *Gestion des données du personnel* » et « *Messagerie électronique interne et externe* », légalement mis en oeuvre.

A cet égard, la Commission demande que, conformément aux dispositions des articles 9 et 10-1 de la Loi n° 1.165, modifiée, ces 2 traitements soient valablement modifiés de sorte à ce qu'apparaissent expressément leur interconnexion avec le traitement dont s'agit.

VIII. 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'observations particulières.

La Commission rappelle néanmoins que, conformément à l'article 17 de la Loi n° 1.165, modifiée, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement 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.

IX. Sur la durée de conservation

Le responsable de traitement indique que les informations nominatives sont conservées « *5 jours ou sur la durée d'une investigation* ».

La Commission prend acte de ces durées de conservation et elle rappelle que dans le cadre de l'ouverture d'une procédure judiciaire, toute information nécessaire, notamment à des fins probatoires, pourra être conservée jusqu'au terme de la procédure.

En conséquence, elle considère que cette durée de conservation est conforme aux exigences légales.

Après en avoir délibéré,

Demande :

- la mise en conformité de l'information préalable des personnes concernées ;

- que les personnes concernées soient en mesure d'exercer leurs droits de manière effective et que les modalités d'exercice de ces droits figurent expressément dans la mention insérée en bas des messages électroniques sortants ;

- que les traitements ayant pour finalité « *Gestion des données du personnel* » et « *Messagerie électronique interne et externe* » soient dûment modifiés ;

- que la liste nominative des personnes ayant accès au traitement soit tenue à jour, et puisse être communiquée à la Commission à première réquisition ;

A la condition de la prise en compte de ce qui précède,

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 « *Prévention des fuites de données confidentielles* ».**

Le Président,

Michel SOSSO