DELIBERATION N° 2015-12 DU 28 JANVIER 2015 DE LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES PORTANT AUTORISATION A LA MISE EN ŒUVRE DU TRAITEMENT AUTOMATISE D'INFORMATIONS NOMINATIVES AYANT POUR FINALITE « *SURVEILLANCE DES ACCES LOGIQUES* » PRESENTE PAR LA HSBC PRIVATE BANK (MONACO) SA

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 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, susvisée ;

Vu la demande d'autorisation déposée par la HSBC Private Bank (Monaco) SA, le 17 novembre 2014 concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Surveillance des accès logiques* » ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 28 janvier 2015 portant examen du traitement automatisé susvisé ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 15 janvier 2015, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230, susmentionnée ;

La Commission de Contrôle des Informations Nominatives,

Préambule

La HSBC Private Bank (Monaco) SA, immatriculée au RCI sous le numéro 97 S 03269, est une société ayant notamment pour activité « *la réalisation de toutes opérations de banque ou connexes telles que définies par la « loi bancaire » applicable […]* ».

Afin de prévenir toute perte d'informations et d'identifier les accès à ces dernières, cet établissement souhaite mettre en œuvre un traitement permettant la traçabilité des accès 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 présent traitement a pour finalité « *Surveillance des accès logiques* ».

Les personnes concernées sont les collaborateurs ainsi que « *les clients et personnes extérieures via leur adresse de messagerie lorsqu'ils sont contactés* ».

Ses fonctionnalités sont les suivantes :

- collecter les journaux d'accès dont le rôle est de collecter les historiques des actions effectuées par les personnes concernées sur tous les serveurs et équipements du réseau de la HSBC Private Bank (Monaco) SA (tous les serveurs, les stations de travail, les pc portables, les appareils portables - tablettes, smartphones – se connectant au système d'information, les équipements réseau - firewall, commutateurs, routeurs -, les proxys internet) ;
- permettre de vérifier la véracité d'un évènement en cas de litige ;
- prévenir un accès non-autorisé ;
- prévenir un éventuel vol de données.

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, modifiée.

II. Sur la licéité et la justification du traitement

➢ *Sur la licéité du traitement*

La Commission constate que dans le cadre de son activité, le responsable de traitement est soumis à une obligation particulière de secret professionnel, à savoir le secret bancaire, prévue à l'article 308 du Code pénal.

Elle relève également qu'il est tenu, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, de « *[prévoir] des mesures techniques et d'organisation appropriées pour protéger les informations nominatives contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé* ».

A cet égard, elle observe que ce traitement constitue une mesure appropriée permettant d'assurer la sécurité des informations et du traitement.

Elle considère donc que ce traitement est licite conformément à l'article 10-1 de la loi précitée.

- ***Sur la justification du traitement***

Le traitement est justifié par la réalisation d'un intérêt légitime poursuivi par le responsable de traitement.

A cet égard, la Commission relève que ce traitement permet de veiller au respect du secret professionnel ainsi que de constituer des preuves en cas de violation de cette obligation légale, notamment en cas de vol de données en interne. La surveillance se fait au niveau de rapports et/ou d'alertes.

Enfin, elle prend acte que le traitement n'a pas pour vocation d'être utilisé pour surveiller la qualité, ni la quantité de travail fourni par les collaborateurs.

Elle constate donc que les droits et libertés des personnes sont respectés.

Elle considère par conséquent que ce traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165, modifiée.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité : nom, prénom des personnes loguées ;
- données d'identification électronique : accès des personnes habilitées ;
- historique : enregistrement de la date et heure des logs, trace des actions effectuées (modification, suppression, tentative d'accès, extraction, copie).

La Commission relève que sont également collectés les noms, prénoms, adresse email des clients et personnes extérieures dans le cadre de l'envoi d'un email, ainsi que les logs et accès des administrateurs du système informatique.

Les informations relatives aux données d'identification électronique et à l'historique ont pour origine le système informatique lui-même.

Les informations relatives à l'identité ont pour origine l'Active Directory.

A cet égard, la Commission relève que l'Active Directory précité n'a fait l'objet d'aucune formalité légale de la part du responsable de traitement.

Ainsi, elle conditionne l'alimentation du présent traitement à l'accomplissement, par la HSBC Private Bank (Monaco) SA des formalités relatives à la mise en œuvre dudit Active Directory.

IV. Sur les droits des personnes concernées

- ***Sur l'information préalable des personnes concernées***

L'information préalable des personnes concernées est effectuée par le biais d'un document spécifique, d'une mention ou clause particulière intégrée dans un document remis à l'intéressé ainsi que par une procédure interne accessible en Intranet.

A l'analyse des documents annexés à la présente demande d'autorisation, la Commission relève tout d'abord que ces derniers sont uniquement à l'attention des employés.

De même, ces documents ne comportent pas l'intégralité des mentions exigées par l'article 14 de la Loi n°1.165 dont s'agit.

Ainsi, elle demande à ce que des modalités d'informations soient également effectuées à l'attention de la clientèle et que les documents soient complétés de manière à répondre aux exigences de la Loi.

Sous cette condition, la Commission considère que les modalités d'information préalable des personnes concernées sont conformes aux exigences légales.

- ***Sur l'exercice du droit d'accès, de modification et de mise à jour***

Le droit d'accès est exercé par courrier électronique, voie postale et sur place.

Le délai de réponse est de 30 jours.

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***

Les informations traitées sont susceptibles d'être transmises en cas de contentieux à la Direction de la Sûreté Publique, ainsi qu'aux huissiers ou tout autre auxiliaire de justice monégasque.

La Commission estime que la communication à la Direction de la Sûreté Publique peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, elle rappelle qu'en cas de transmission, les Services de Police ne pourront avoir accès aux informations traitées, que dans le strict cadre de leurs missions légalement conférées.

De même, elle considère que les huissiers ou les auxiliaires de justice (avocat…) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires d'informations nominatives traitées.

Ainsi, la Commission considère que de telles transmissions sont conformes aux exigences légales.

- ***Sur les personnes ayant accès***

Les personnes habilitées à avoir accès au présent traitement sont :

- le personnel des services IT, IFR et Infra Team (consultation des rapports/alertes) ;
- les employés de différents services de la banque (consultation des rapports/alertes).

La Commission prend également acte du fait que « *les logs transitent par HSBC Private Bank (Suisse) SA où se situe la sortie/entrée internet, mais personne n'a accès à la console de log de la banque HSBC Private Bank (Monaco) SA* ».

Ainsi, considérant les attributions de ces services, et eu égard à la finalité du traitement, la Commission considère que ces accès sont justifiés.

Elle rappelle enfin que conformément à l'article 17-1 de la Loi n° 1.165, modifiée, 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 demande donc à ce que cette liste, tenue à jour, puisse lui être communiquée à première réquisition.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement ne fait l'objet d'aucune interconnexion avec d'autres traitements. Toutefois, il appert de l'examen de la demande d'autorisation que ledit traitement fait l'objet d'une interconnexion avec l'intégralité des traitements objets de la surveillance des accès logiques.

Ainsi, en l'absence de précisions de la part du responsable de traitement, elle conditionne l'alimentation de ce traitement ayant pour finalité « *Surveillance des accès logiques* » à la réalisation des formalités légales pour les autres traitements avec lesquels il est interconnecté.

De plus, elle demande à la HSBC Private Bank (Monaco) SA de lui communiquer dans les plus brefs délais la liste desdits traitements interconnectés avec celui-ci.

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 de la part de la Commission.

Elle 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.

VIII. Sur la durée de conservation

Le responsable de traitement indique que les informations sont conservées 1 an.

La Commission considère que cette durée de conservation est conforme aux exigences légales

Après en avoir délibéré, la Commission :

Rappelle que la liste nominative des personnes ayant accès au traitement, doit être tenue à jour, et pouvoir être communiquée à première réquisition ;

Demande que :

- les formalités relatives à la mise en œuvre du traitement ayant pour finalité « *la gestion de l'Active Directory* » soient effectuées ;

- des modalités d'informations soient également effectuées à l'attention de la clientèle et que les documents soient complétés de manière à répondre aux exigences de l'article 14 de la loi dont s'agit ;

- la liste des traitements interconnectés avec celui-ci lui soit communiquée.

Conditionne :

- l'alimentation du présent traitement à l'accomplissement, par la HSBC Private Bank (Monaco) SA, des formalités relatives à la mise en œuvre du traitement ayant pour finalité « *la gestion de l'Active Directory* » duquel proviennent certaines informations traitées présentement ;

- l'alimentation de ce traitement ayant pour finalité « *Surveillance des accès logiques* » à la réalisation des formalités légales pour les autres traitements (qu'il appartient au responsable de traitement de déterminer) avec lesquels il est interconnecté et desquels proviennent certaines informations traitées présentement.

Sous réserve de la prise en compte des demandes et conditions qui précèdent,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre, par la HSBC Private Bank (Monaco) SA, du traitement automatisé d'informations nominatives ayant pour finalité « *Surveillance des accès logiques* ».**

Le Président,

Guy MAGNAN