DÉLIBÉRATION N° 2014-12 DU 4 FÉVRIER 2014 DE LA COMMISSION DE CONTRÔLE DES INFORMATIONS NOMINATIVES PORTANT AUTORISATION À LA MISE EN ŒUVRE DU TRAITEMENT AUTOMATISÉ D'INFORMATIONS NOMINATIVES AYANT POUR FINALITÉ « *SUPERVISION DE L'ACTIVITÉ DES ADMINISTRATEURS DES SYSTÈMES INFORMATIQUES* » PRÉSENTÉ PAR LA LLOYDS BANK PLC

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 LLOYDS BANK PLC, le 29 novembre 2013 concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Supervision de l'activité des administrateurs des systèmes informatiques* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 21 janvier 2014, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230 susmentionné ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 4 février 2014 portant examen du traitement automatisé susvisé ;

La Commission de Contrôle des Informations Nominatives,

Préambule

La LLOYDS BANK PLC est une société de droit britannique ayant pour objet « *toutes opérations de banque* ». Elle est représentée en Principauté par sa succursale.

Afin de prévenir toute atteinte à l'intégrité des informations qu'elle détient, et à leur confidentialité, elle souhaite mettre en œuvre un traitement permettant de superviser l'activité des administrateurs des systèmes informatiques.

A ce titre, en application de l'article 11-1 de la loi n° 1.165 du 23 décembre 1993, concernant un traitement automatisé d'informations nominatives mis en œuvre à des fins de surveillance, ladite société soumet la présente demande d'autorisation à la Commission de Contrôle des Informations Nominatives.

I - Sur la finalité et les fonctionnalités du traitement

Le présent traitement a pour finalité « *Supervision de l'activité des administrateurs des systèmes informatiques* ».

Il concerne les administrateurs des systèmes informatiques de la succursale à Monaco.

Ses fonctionnalités sont les suivantes :

- « *Créer et disposer d'un log de sécurité sur les accès au système informatique de Monaco ;*
- *Réaliser un contrôle du log afin de détecter d'éventuels manquements au respect du secret professionnel, tels que sanctionnables au titre de l'article 308 du Code pénal monégasque ;*
- *Procéder à la restauration des données et à une investigation des actions liées aux manquements détectés* ».

A l'analyse du dossier, il apparait qu'est exploitée une finalité supplémentaire qui consiste en la consultation et la réception des rapports de monitoring. La Commission en prend acte.

Elle 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***

La Commission estime que ce traitement est justifié par la réalisation d'un intérêt légitime poursuivi par le responsable de traitement.

A cet égard, elle 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.

Enfin, elle observe que la surveillance de l'activité des administrateurs est limitée à des actions d'ordres uniquement techniques et professionnels, à savoir : échec d'authentification, connexions interactives, redémarrage du serveur, changement de la configuration sécurité du serveur, logs applicatifs spécifiques. Par ailleurs, les logs au niveau des PCs des utilisateurs ne sont pas collectés.

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

Ainsi, la Commission considère que le 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 objets du présent traitement sont :

- identité : User ID permettant une identification des noms et prénoms ;
- données d'identification électronique : logs de connexion des administrateurs des systèmes informatiques (département IT Monaco) ;
- historique de l'activité: date, heure de l'activité.

Concernant cette dernière catégorie d'information, il ressort de l'analyse du dossier que sont également exploitées les informations suivantes : type d'évènement ayant généré le log (échec d'authentification, connexion interactive, …), niveau de criticité de l'évènement, retour sur l'évènement (succès, erreur, échec, …). La Commission en prend acte.

Les informations relatives aux données d'identification électronique et à l'historique de l'activité 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 permet d'attribuer des profils d'accès aux salariés de la Lloyds Bank PLC.

Elle observe que ce traitement a été légalement mis en œuvre le 19 septembre 2002 sous la finalité « *Administration des systèmes* ».

Concernant ce dernier traitement, la Commission invite néanmoins le responsable de traitement à vérifier qu'il est conforme aux nouvelles dispositions introduites la Loi n° 1.165 du 23 décembre 1993, modifiée.

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 et par email.

Seul le mail d'information a été joint au dossier. La Commission constate que les mentions d'informations sont conformes à l'article 14 de la loi n° 1.165 du 23 décembre 1993, modifiée.

Elle considère donc 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. Le délai de réponse est de 30 jours.

Les droits de modification et de mise à jour des données sont exercés selon les mêmes modalités.

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 personnes ayant accès au traitement

Les personnes habilitées à avoir accès au présent traitement sont :

- le personnel du département IT Security Monaco (Manager Credit et IT) en consultation ;
- le personnel du Département IT Security Genève en modification, mise à jour et consultation.

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 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.

VII – Sur la durée de conservation

Le responsable de traitement indique que les informations sont conservées 10 ans.

La Commission constate que cette durée de conservation n'est pas adéquate au regard des fonctionnalités du traitement objet de la présente demande d'autorisation.

Aussi, conformément à l'article 9 de la loi n°1.165, elle fixe la durée de conservation des informations relatives :

- à l'historique de l'activité à 3 ans à compter de leur collecte, conformément aux règles de prescription légales en matière délictuelle visées à l'article 13 du Code de procédure pénale ;
- à l'identité de l'administrateur et aux données d'identification électronique à 3 ans à compter du départ de l'employé.

Après en avoir délibéré,

Rappelle que :

- les accès au traitement et aux données qu'il contient devront être limités à ce qui est nécessaire aux personnes habilitées « *pour les stricts besoins de l'accomplissement de leurs missions* » ;

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

Fixe la durée de conservation des informations nominatives à 3 ans ans à compter de leur collecte en ce qui concerne l'historique de l'activité, et à 3 ans à compter du départ de l'employé en ce qui concerne l'identité de l'administrateur et aux données d'identification électronique ;

Invite le responsable de traitement à vérifier la conformité du traitement ayant pour finalité « *Administration des systèmes* » aux nouvelles dispositions de la loi n° 1.165 du 23 décembre 1993, modifiée.

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 la LLOYDS BANK PLC, du traitement automatisé d'informations nominatives ayant pour finalité « *Supervision de l'activité des administrateurs des systèmes informatiques* ».**

Le Président,

Michel SOSSO