DELIBERATION N° 2015-40 DU 15 AVRIL 2015 DE LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES PORTANT AUTORISATION A LA MISE EN ŒUVRE DU TRAITEMENT AUTOMATISE D'INFORMATIONS NOMINATIVES AYANT POUR FINALITÉ « *GESTION DES HABILITATIONS INFORMATIQUES ET TRAÇABILITE DES ACCES* » PRESENTE PAR CREDIT FONCIER DE MONACO (C.F.M.)

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 la Loi n° 1.338 du 7 septembre 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 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'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 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 la demande d'autorisation reçue le 13 mars 2015 concernant la mise en œuvre par Crédit Foncier de Monaco (C.F.M.) d'un traitement automatisé ayant pour finalité « *Gestion des habilitations & des accès aux applications* » ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 15 avril 2015 portant examen du traitement automatisé susvisé ;

La Commission de Contrôle des Informations Nominatives,

Préambule

Le Crédit Foncier de Monaco (C.F.M. Monaco), immatriculé au RCI sous le numéro 56 S 00341, est une banque dont l'activité principale est : « *toutes opérations bancaires et financières et plus généralement toutes opérations pouvant être exercées par les établissements de crédit de droit monégasque en conformité avec la législation et la réglementation qui leurs sont applicables* ».

Dans le cadre de son organisation interne, et afin d'assurer la sécurité informatique de son réseau, le Crédit Foncier de Monaco (C.F.M.) souhaite mettre en œuvre un traitement ayant pour finalité « *Gestion des habilitations & des accès aux applications* ».

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 responsable de traitement dispose que le traitement a pour finalité « *Gestion des habilitations & des accès aux applications* ».

Le responsable de traitement indique que les personnes concernées sont « *l'ensemble des collaborateurs du CFM Monaco* ».

A l'examen des fonctionnalités du traitement, la Commission considère que les personnes concernées sont les salariés et les prestataires du CFM Monaco.

Les fonctionnalités du traitement sont :

« *Dans le cadre de la gestion des habilitations :*

- *octroyer / délivrer aux collaborateurs du CFM Monaco (salariés et prestataires), les moyens techniques et fonctionnels permettant de s'authentifier au système d'information et d'exercer la fonction et les missions pour lesquelles ils ont été recrutés, dans le respect du principe de moindre privilège et du besoin d'en connaître ;*
- *gérer les évolutions de droits, les mobilités internes et les départs ;*
- *mettre à jour les comptes systèmes dans le cadre de changement d'informations administratives (ex : changement de patronyme, le type et l'échéance du contrat, l'adresse professionnelle) ;*
- *permettre la réalisation de l'ensemble des tâches d'activation/ désactivation/ suppression de comptes, de mise à jour des listes de diffusion de messagerie électronique, des listes de contrôle d'accès, des groupes de privilèges auxquels le collaborateur appartient, de l'enregistrement ou non des communications téléphoniques ;*
- *procéder à des revues de contrôles périodiques afin de s'assurer de la conformité des droits délivrés par rapport aux demandes et aux règles édictées en matière d'accès à l'information.*

Dans le cadre de la supervision des accès aux applications :

- *collecter des évènements systèmes permettant de tracer les accès des utilisateurs aux applications et données ;*
- *établir du reporting sur les données sensibles visant à prévenir le risque de fraude et s'assurer de la cohérence des accès* ».

A la lecture des fonctionnalités du traitement, la Commission observe que la notion de traçabilité, qui traduit un caractère de surveillance du traitement dont s'agit, ne figure pas expressément dans sa finalité.

Ainsi, elle considère qu'il convient de reformuler la finalité proposée par le responsable de traitement, conformément à l'article 10-1 de la Loi n° 1.165, lequel dispose que les informations nominatives doivent être collectées pour une finalité déterminée, explicite et légitime.

En conséquence, elle modifie la finalité du traitement comme suit : « *Gestion des habilitations informatiques et traçabilité des accès* ».

II. Sur la licéité et la justification du traitement

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

En ce sens, il précise, d'une part, que le traitement dont s'agit permet de « *limiter l'accès à l'information de manière à en assurer la disponibilité, l'intégrité, la confidentialité et la sécurité* », et d'autre part, de « *protéger les intérêts de la banque et de ses clients en évitant les risques de fraude, notamment la perte ou la fuite de données (confidentielles, stratégiques, …)* ».

Par ailleurs, la Commission constate 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 est partiellement applicable à Monaco.

A cet égard, elle observe que l'article 275 dudit Arrêté dispose que « *les dispositions des articles 43 à 73, 246 et du h de l'article 259 ne sont pas applicables aux établissements de crédit y compris les succursales, aux établissements de paiement et aux établissements de monnaie électronique dont le siège social ou la succursale est situé dans la Principauté de Monaco* ».

Aussi, elle relève que l'article 11 du Titre II - Le système de contrôle des opérations et des procédures internes - de ce même Arrêté 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* ».

Subsidiairement, elle observe que 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 prévoit, notamment à ses articles 6, 7 et 11 des dispositions comparables.

Enfin, elle rappelle que le traitement dont s'agit participe à la sécurisation du système informatique de la banque, conformément aux exigences des articles 17 et 17-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

La Commission considère par conséquent que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165, modifiée.

III. Sur les informations traitées

Les informations nominatives traitées sont les suivantes :

- identité : nom, prénom, numéro matricule, date d'entrée, nature et durée du contrat, affectation et localisation, numéro de badge, sensibilité du collaborateur, identifiants système de connexion ;
- données d'identification électronique : comptes utilisateurs, adresse email professionnelle ;
- biens techniques et fonctionnels : énumération des outils, applications et profil associé, éventuels commentaires apportant des précisions sur les demandes ;
- journalisation : logs, évènements et accounting système, comptes utilisateurs, horodatage.

Le responsable de traitement indique que les informations relatives à l'identité ont pour origine les Services de « *la Gestion du personnel [et de] la Direction Informatique* ». Celles se rapportant aux biens techniques et fonctionnels sont issues du Service « *Management* ». Enfin, les autres informations proviennent du système lui-même.

Par ailleurs, concernant la notion de « *sensibilité du collaborateur* », le responsable de traitement précise que cette information « *concerne la sensibilité du collaborateur sur les marchés financiers* » et qu'elle « *n'a d'intérêt que pour gérer (créer, mettre à jour) des listes de diffusion au sein de la messagerie électronique (…) afin de pouvoir cibler les seuls collaborateurs concernés* ».

Aussi, la Commission considère que ces informations sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement.

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 effectuée par le biais d'une rubrique propre à la protection des données accessible en ligne et une procédure interne accessible en intranet.

A cet effet, il a joint une retranscription du message accessible en intranet.

A la lecture de celui-ci, la Commission constate qu'il n'indique pas l'identité des destinataires ou des catégories de destinataires, conformément à l'article 14 de la Loi n° 1.165, modifiée.

Subsidiairement, et après avoir estimé que les personnes concernées sont les salariés et les prestataires de la banque, la Commission invite le responsable de traitement à s'assurer

que l'information préalable des prestataires est conforme aux dispositions de l'article 14 de la Loi n° 1.165, modifiée.

Elle demande donc que l'information préalable soit délivrée à l'ensemble des personnes concernées et conformément à l'article 14 de la Loi n° 1.165, modifiée.

- ***Sur l'exercice du droit d'accès des personnes concernées***

Les droits d'accès, de modification, de mise à jour et de suppression s'exercent par courrier électronique ou sur place auprès de la Direction des Ressources Humaines.

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, modifiée.

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

- ***Sur les destinataires***

Le responsable de traitement indique que le « *Contrôle Interne (Inspection Générale et Contrôle Permanent)* » de la banque et la Direction de la Sûreté Publique peuvent être destinataires des informations.

A cet égard, il précise qu'il s'agit de communications et non d'accès en ce que même si l'Inspection Générale et le Contrôle Permanent ont potentiellement le droit d'accéder à les toutes informations au sein du CFM Monaco, elles ne leur sont délivrées « *que sur requête en réponse à un besoin justifié* » suivant le principe du « *need to know* ».

Par ailleurs, la Commission observe 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.

La Commission considère que ces communications sont conformes aux exigences légales.

- ***Sur les personnes ayant accès au traitement***

Le responsable de traitement indique que les personnes ayant accès au traitement sont :

- la fonction Gestion du Personnel (limité à 2 personnes) sur la totalité du périmètre : en inscription ;
- la fonction RSSI de la Direction de la Sécurité de l'Information & de la Continuité d'Activité (SECU – « *Sécurité de l'Information & de la Continuité d'Activité* ») sur la totalité du périmètre : en modification ;
- la Direction Informatique (GHF – « *Gestion des Habilitations Fonctionnelles* » : limité à 3 personnes, GBM – « *Gestion des Biens Matériels* » : limité à 5 personnes, HDT – « *HelpDesk Technique* » : limité à 3 personnes), la Direction des Services et des Moyens Généraux (limité à 3 personnes), les Responsables d'unité (hiérarchiques) ou leur délégataire sur le seul périmètre de collaborateurs directs : en mise à jour ;

- les Correspondants Informatiques de Proximité (CIP) sur leur seul périmètre de collaborateurs directs et le responsable Déontologie de la Direction de la Compliance : en consultation.

La Commission rappelle enfin 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.

Par ailleurs, considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, elle estime que ces accès sont justifiés.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que « *l'ensemble des traitements automatisés et exploités par le CFM Monaco sont interconnectés avec ce traitement qui est le point de convergence et de contrôle des habilitation d'accès au système d'information* ».

La Commission en prend acte et l'invite à s'assurer que les interconnexions avec le traitement dont s'agit figurent expressément dans chacun des traitements concernés conformément à l'article 8 – 6°) de la Loi n° 1.165, modifiée, et le cas échéant, à procéder aux modifications nécessaires visées à l'article 9 de ladite Loi.

Subsidiairement, elle rappelle que les interconnexions ne peuvent avoir lieu qu'entre des traitements légalement mis en œuvre.

Par ailleurs, il indique que « *dans le cadre des revues de contrôles périodiques, il y a un rapprochement des demandes d'accès (WorkFlow de gestion des accès aux outils informatiques) avec les configurations et les systèmes d'habilitations des applications* ».

A cet égard, il précise qu'il a pour objet de s'assurer que « *ce qui est codé dans les configurations système des applications est conforme aux demandes qui ont été formulées dans le WorkFlow)* » (Qui accède théoriquement à quoi ? Qui accède réellement à quoi ?). Le Service chargé du contrôle peut ainsi opérer « *un rapprochement ligne à ligne* » afin de s'assurer de l'absence de discordance.

Sous ces rappels et conditions, elle considère que ces interconnexions et ce rapprochement sont conformes à la Loi n° 1.165, modifiée.

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'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 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 sont conservées :

- 5 ans après le départ du collaborateur, s'agissant des informations relevant de l'identité et des biens techniques et fonctionnels ;
- le temps du contrat de travail, pour les données d'identification électronique ;
- 1 an, concernant les informations se rapportant à la journalisation.

En ce qui concerne les « *informations relevant de l'identité et des biens techniques et fonctionnelles* » le responsable de traitement précise que la « *la fiche [du collaborateur] fait en quelque sorte partie [de son] dossier individuel RH. Le besoin se justifie [pour] comprendre pourquoi ou comment une action a pu être exécutée par le passé et [le cas échéant apporter les corrections nécessaires à sa non-reproduction] (…). Ce besoin s'entend tant pendant la période de collaboration qu'après le départ du collaborateur et nous avons considéré (afin d'étayer certaines analyses) que cette période devrait être d'au moins 5 ans* ».

La Commission considère qu'une telle durée de conservation est disproportionnée au regard de la finalité du traitement. Aussi elle fixe à 5 ans la durée de conservation de ces informations.

Après en avoir délibéré, la Commission :

Considère que les personnes concernées sont les salariés et les prestataires du CFM Monaco.

Modifie la finalité du traitement comme suit : « *Gestion des habilitations informatiques et traçabilité des accès* ».

Rappelle que conformément à 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 être communiquée à la Commission à première réquisition ;

Demande que l'information préalable soit délivrée à l'ensemble des personnes concernées et conformément à l'article 14 de la Loi n° 1.165, modifiée.

Fixe à 5 ans la durée de conservation des informations relatives à l'identité et aux biens techniques et fonctionnels, sans préjudice de leur mise à jour tous les 5 ans, et ce, jusqu'au départ du salarié ou du prestataire.

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 le Crédit Foncier de Monaco (C.F.M.) du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations informatiques et traçabilité des accès* ».**

Le Président,

Guy MAGNAN