Délibération n° 2017-025 du 15 mars 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 Supervision des activités sur les périphériques Multi-Fonction de la Banque* »

présenté par Crédit Suisse (Monaco) SAM

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° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;

Vu la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée ;

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, modifiée, susvisée ;

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'article 308 du Code pénal ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'autorisation déposée par Crédit Suisse AG le 23 novembre 2016 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion et Supervision des activités sur les périphériques Multi-Fonction de la Banque* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 20 janvier 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 15 mars 2017 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Crédit Suisse AG est une société suisse qui souhaite se faire représenter à Monaco par sa succursale Crédit Suisse (Monaco) SAM afin d'accomplir ses formalités légales.

Toutefois, 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, Crédit Suisse AG est établi à Monaco par sa succursale enregistrée au RCI sous le numéro 98S3517, ayant entre autres pour activité en Principauté de Monaco et à l'étranger, pour son compte ou pour le compte de tiers, directement ou en participation « *la réalisation de toutes opérations de banque ou connexes telles que définies par la loi bancaire applicable ».*

Dans le cadre de l'exercice de leurs fonctions, les employés de cette société disposent de périphériques multi-fonction faisant l'objet d'une supervision.

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 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Ce traitement a pour finalité « *Gestion et Supervision des activités sur les périphériques Multi-Fonction de la Banque».*

Le responsable de traitement indique que les personnes concernées sont les utilisateurs des équipements multi-fonction, à savoir principalement les employés de la banque.

Enfin, les fonctionnalités sont les suivantes :

- *« identifier les éventuels problèmes liés à l'utilisation des périphériques multi-fonction du réseau de la banque ;*
- *conserver les traces de l'utilisation des périphériques multi-fonction du réseau de la banque (fichiers journaux) en vue de détecter d'éventuels manquements aux obligations du secret professionnel ;*
- *permettre la constitution de preuves en cas de violation des intérêts de la banque ou en cas d'infractions civiles ou pénales ».*

La Commission constate ainsi que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

- ***Sur la licéité***

La Commission constate que dans le cadre de son activité, le responsable de traitement est soumis à l'article 33 de la Loi n° 1.338 du 7 septembre 2007 qui dispose que : « *Toute personne physique qui, à un titre quelconque, participe à l'administration, à la direction ou à la gestion d'une société agréée ou qui est employée par celle-ci est tenue au secret professionnel dans les conditions et sous les peines prévues à l'article 308 du Code pénal. […]* ».

Par ailleurs, l'article 3 de la Loi n°1.314 du 29 juin 2006 stipule que : « *Le teneur de compte-conservateur doit disposer des moyens et procédures nécessaires à l'exercice de son activité, notamment, en ce qui concerne les ressources humaines, les moyens informatiques, la comptabilité, les dispositifs de protection de la clientèle et les contrôles internes, tels que définis par arrêté ministériel.* ».

La Commission considère donc que le traitement est licite au sens de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

- ***Sur la justification***

Le responsable de traitement indique que le traitement est justifié par « *le respect d'une obligation légale à laquelle est soumis le responsable de traitement ou son représentant »*.

A cet égard, la Commission observe que ce traitement permet au responsable de traitement de respecter notamment les obligations découlant des Lois n° 1.338 du 7 septembre 2007 et n° 1.314 du 29 juin 2006.

Par ailleurs, le responsable de traitement indique que ce traitement répond à un objectif légitime essentiel puisqu'il permet de veiller au respect du secret professionnel auquel la banque est soumise, et d'assurer ainsi :

- la préservation des intérêts économiques, commerciaux et financiers du responsable de traitement ou de son représentant ;
- la protection contre tout acte susceptible d'engager sa responsabilité civile ou pénale, ou de lui porter préjudice.

Le responsable de traitement précise également que les droits et libertés des personnes concernées sont respectés puisque « *les procédures internes de la banque précisent que les équipements multi-fonction sont réservés à l'usage professionnel* ».

La Commission considère donc que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. <u>Sur les informations nominatives traitées</u>

Les informations nominatives traitées sont :

- <u>identité</u> : numéro d'utilisateur (User) ;
- <u>informations sur le document</u> : nom du fichier imprimé, le nom de pages et la taille des fichiers (cas des impressions) ;
- <u>informations temporelles</u> : date, heure ;
- <u>fichiers journaux</u> : opération réalisée (impression, scan, etc.), état de l'opération (en attente, erreur, réalisée, etc.), nom du périphérique réseau multifonction, nom de l'ordinateur, adresse IP source de l'impression et adresse IP destinatrice de l'impression.

Le responsable de traitement indique que les informations relatives à l'identité ont pour origine le traitement ayant pour objet « *Gestion des données personnelles et d'emploi des collaborateurs* ».

Toutes les autres informations ont pour origine le traitement lui-même.

Aussi, 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 du personnel se fait par le biais d'une procédure interne accessible en intranet.

Cette procédure n'ayant pas été jointe à la demande, la Commission rappelle que celle-ci doit impérativement informer les personnes concernées de la finalité du traitement, ainsi que de leurs droits 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***

Le droit d'accès s'exerce sur place. La réponse à ce droit d'accès s'exerce selon les mêmes modalités.

Le délai de réponse à une demande de droit d'accès est de 30 jours.

La Commission constate 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 destinataires

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

Les personnes habilitées à avoir accès au traitement sont :

- le Service « *Corporate Real Estates (CRES)* » : en inscription, modification, mise à jour et consultation ;
- la Direction : en consultation ;
- le Département Informatique : en consultation, inscription, modification et mise à jour ;
- le Département Audit Interne : en consultation dans le cadre de sa mission de contrôle ;
- le Département Juridique et Compliance : en consultation ;
- les prestataires : tous les accès dans le cadre de leurs missions de maintenance.

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

En ce qui concerne les prestataires, la Commission rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service. De plus, lesdits prestataires sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

Par ailleurs, la Commission constate que le responsable de traitement dispose d'une procédure destinée à effacer tous les supports disques durs des périphériques multi-fonction, en cas de réparation, de mise au rebus ou de réutilisation.

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.

- ***Sur les destinataires***

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées à la Commission de Contrôle des Activités Financières (CCAF).

A cet égard, la Commission considère que la CCAF peut, dans le cadre exclusif des missions qui lui sont conférées, être destinataire des informations nominatives traitées.

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 particulière.

La Commission relève néanmoins que l'architecture technique repose sur des équipements de raccordement (switchs, pare-feux) de serveurs et périphériques qui doivent être protégés par un login et un mot de passe réputé fort et que les ports non utilisés doivent être désactivés.

Elle rappelle par ailleurs 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.

VII. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion ou d'un rapprochement avec deux traitements ayant respectivement pour finalité « *Gestion des données personnelles et d'emploi des collaborateurs* » et « *Gestion des pistes d'Audit* ».

La Commission prend acte que ces traitements ont été légalement mis en œuvre.

Elle relève par ailleurs que ce traitement fait l'objet d'une interconnexion avec un traitement lié à la gestion des habilitations. Ce traitement n'ayant fait l'objet d'aucune formalité, la Commission demande que celui-ci lui soit soumis dans les plus brefs délais.

VIII. Sur la durée de conservation

Le responsable de traitement indique que les informations relatives à l'identité sont conservées 3 ans après le départ de l'utilisateur de la société et que les informations relatives aux informations sur le document, aux informations temporelles et aux fichiers journaux sont conservées 3 ans après la date de la collecte de l'information.

A cet égard, la Commission rappelle que les informations nominatives doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles sont collectées ou pour laquelle elles sont traitées ultérieurement* », conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

Elle demande donc que les informations relatives à l'identité du salarié soient désactivées et supprimées au plus tard 3 mois après le départ dudit salarié et fixe la durée de conservation des autres données à 1 an à compter de leur collecte.

Après en avoir délibéré, la Commission :

Considère que la CCAF peut, dans le cadre exclusif des missions qui lui sont conférées, être destinataire des informations du traitement.

Constate que le responsable de traitement dispose d'une procédure destinée à effacer tous les supports disques durs des périphériques multi-fonction, en cas de réparation, de mise au rebus ou de réutilisation.

Rappelle que :

- l'information des personnes concernées doit impérativement comporter l'ensemble des mentions prévues 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 ;

- l'architecture technique repose sur des équipements de raccordement (switchs, pare-feux) de serveurs et périphériques qui doivent être protégés par un login et un mot de passe réputé fort et que les ports non utilisés doivent être désactivés.

Demande que :

- le traitement lié à la gestion des habilitations lui soit soumis dans les plus brefs délais ;

- les informations relatives à l'identité du salarié soient désactivées et supprimées au plus tard 3 mois après le départ dudit salarié.

Fixe la durée de conservation des données relatives aux informations sur le document, aux informations temporelles et aux fichiers journaux à 1 an à compter de leur collecte.

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 Crédit Suisse (Monaco) SAM du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et Supervision des activités sur les périphériques Multi-Fonction de la Banque* ».**

Le Président

Guy MAGNAN