Délibération n° 2018-055 du 18 avril 2018

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 des activités sur les périphériques multifonctions de la banque* »

présenté par CFM Indosuez Wealth

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 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 financier ;

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 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 CFM Indosuez Wealth le 24 janvier 2018 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Supervision des activités sur les périphériques multifonctions de la banque* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 22 mars 2018, 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 18 avril 2018 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

CFM Indosuez Wealth est une société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 56S00341, qui a pour objet social « *en Principauté de Monaco et à l'étranger, pour son compte, pour le compte de tiers ou en participation, 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 l'exercice de leurs fonctions, les employés de cette société disposent d'imprimantes multifonctions.

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

Le responsable de traitement indique que ce traitement a pour finalité « *Supervision des activités sur les périphériques multifonctions de la banque ».*

Les personnes concernées sont tous les collaborateurs utilisant ces périphériques, à savoir les salariés (CDI, CDD, stagiaires, alternants, etc.) et les prestataires.

Enfin, les fonctionnalités sont les suivantes :

- la conservation des traces de l'utilisation des périphériques multifonctions du réseau de la Banque : collecte des logs d'impression, des copies, des numérisations (scans), ainsi que des fax envoyés ou reçus ;
- la détection d'éventuels manquements aux obligations du secret professionnel ;
- l'établissement d'états de reporting sur le nombre d'impressions et/ou de copies réalisées au sein de l'établissement et les coûts associés, dans le cadre de la mission « *Développement Durable de la Banque* ».

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

Le traitement est justifié par le respect d'une obligation légale à laquelle est soumis le responsable de traitement.

A cet égard, la Commission constate que ce traitement permet au responsable de traitement de respecter les obligations découlant de la Loi n° 1.314 du 29 juin 2006, notamment de son article 3 sur les moyens et procédures nécessaires à l'exercice de l'activité, et de la Loi n° 1.338 du 7 septembre 2007, notamment de son article 33 sur le secret professionnel.

Il est également justifié par la réalisation d'un intérêt légitime poursuivi par le responsable du traitement, sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

La Commission relève ainsi que dans le cadre de la mission « *Développement Durable* » du responsable de traitement, « *la réduction des consommations de papier est un des axes de travail retenus* » et que dans cette optique, « l*a Direction de l'établissement souhaite disposer d'états de reporting sur le nombre de documents imprimés et les coûts associés, intérêt considéré légitime par CFM Indosuez* ».

Elle note par ailleurs que *« les droits et libertés des personnes sont considérés respectés car les procédures internes de la Banque précisent que les équipements multifonctions (ainsi que toute ressource du Système d'Information) sont réservés à l'usage professionnel* » et que cette mention « *est rappelée à tout utilisateur au moment de la connexion au Système d'Information de la Banque, et requiert une action d'acquittement du message délivré* ».

La Commission considère donc que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations nominatives traitées

Les informations nominatives traitées sont :

- identité : nom et prénom, identifiant de l'utilisateur (user Windows), service d'affectation ;
- informations temporelles : date et heure de l'opération, dans le cas des impressions, date et heure de la mise en attente (lancement de l'impression depuis le poste du collaborateur) et de l'impression du document depuis l'équipement ;
- information sur le document : nom du document imprimé, nombre de pages (cas des impressions) ;
- journaux/logs : type d'opération réalisée (fax, scan, copie, impression), détails de l'équipement (nom, adresse IP, emplacement).

La Commission constate que les informations relatives à l'identité ont pour origine le traitement ayant pour finalité « *Gestion des habilitations informatiques et traçabilité des accès »*.

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

Aussi, elle 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 Directive relative aux « *Droits et Obligations des collaborateurs* » qui comprend un chapitre couvrant les accès et l'utilisation des ressources du système d'information, y compris les équipements multifonctions, et par le biais d'une procédure interne accessible en intranet.

Ces documents n'ayant pas été joints à la demande, la Commission rappelle à cet égard que ceux-ci doivent impérativement comporter l'ensemble des mentions prévues 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 par courrier électronique ou sur place.

A cet égard, la Commission rappelle que la réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande.

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, la Commission considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-116 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous ces conditions, 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. <u>Sur les personnes ayant accès au traitement</u>

Les personnes habilitées à avoir accès au traitement sont :

- le Département Informatique : tous droits ;
- le Responsable de la mission « *Développement Durable* » : accès en consultation ;
- le Département Organisation (à savoir le Responsable du département et le service « *Développement et Support Logiciel Fonctionnel* ») : accès en consultation pour la constitution des rapports ;
- le Comité de Direction : accès en consultation, de façon ponctuelle ;
- le Département Audit Interne : accès en consultation, uniquement dans le cadre d'une mission d'audit ;
- le Service Déontologie (Direction de la Compliance) : accès en consultation, de façon ponctuelle ;
- les prestataires : accès dans le cadre des opérations 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 prend note que les supports de stockage destinés à la destruction font l'objet d'une procédure de protection particulière. A cet égard, elle demande toutefois qu'il en soit de même en cas de maintenance.

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.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le traitement dont s'agit ne fait l'objet d'aucune interconnexion avec un autre traitement.

Il appert toutefois à l'étude du dossier une interconnexion avec le traitement ayant pour finalité « *Gestion des habilitations informatiques et traçabilité des accès »,* qui a été légalement mis en œuvre.

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 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 que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception

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 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 données collectées sont conservées 1 an.

La Commission considère que cette durée est conforme aux exigences légales.

Après en avoir délibéré, la Commission :

Considère qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations ;

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 réponse à un droit d'accès doit intervenir dans le mois suivant la réception de la demande ;
- 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 ;

- la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

Demande que les supports de stockage fassent également l'objet d'une procédure de protection particulière en cas de maintenance.

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 CFM Indosuez Wealth du traitement automatisé d'informations nominatives ayant pour finalité « *Supervision des activités sur les périphériques multifonctions de la banque* ».**

Le Président

Guy MAGNAN