Délibération n° 2022-091 du 22 juin 2022

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 des prises de main à distance sur l'environnement CFM IW* »

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 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 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'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 CM/Rec(2015)5 du Conseil de l'Europe du 1er avril 2015 sur le traitement des données à caractère personnel dans le cadre de l'emploi ;

Vu la demande d'autorisation déposée par CFM Indosuez Wealth, le 15 mars 2022, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Gestion des prises de main à distance sur l'environnement CFM IW* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 12 mai 2022, 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 22 juin 2022 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Le CFM Indosuez Wealth est une société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 56S00341, et 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* ».

Afin de sécuriser les interventions à distance sur son système d'intervention et les actions des comptes à haut privilège, ce responsable de traitement souhaite mettre en place un dispositif permettant d'en assurer la maitrise.

Ce traitement 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 traitement a pour finalité *« Gestion des prises en main à distance sur l'environnement CFM IW* ».

Le responsable de traitement indique qu'il concerne les « *salariés et prestataires extérieurs* ».

Les fonctionnalités sont les suivantes :

- enregistrement des sessions des comptes à haut privilège (saisie clavier + capture vidéo) ;
- enregistrement des sessions de support utilisateur (saisie clavier + capture vidéo) ;
- conservation des enregistrements pendant une année et suppression automatique au terme de cette durée ;
- horodatage et logs au sein du SIEM de toutes les informations ;
- remontée automatique des alertes chez le RSSI en cas de lecture des enregistrements ;
- vérification sous contrôle en cas de litige ;
- vérification sous contrôle en cas de mauvaise configuration ;
- possibilité dans un cadre déterminé d'utiliser les données comme support de formation ;
- permettre un accès à distance à certains environnements précis et restreints du système d'information ;
- permettre la traçabilité des sessions et l'imputabilité des actions ;
- vérifier, a posteriori, si nécessaire, les actions réalisées par les utilisateurs de la solution et disposer, le cas échéant, de preuves ou de débuts de preuves si de besoin ;
- conserver des éléments retraçant la réalisation des opérations réalisées par les agents.

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 du 23 décembre 1993.

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 ne soient méconnus ni les intérêts, ni les droits et libertés fondamentaux des personnes concernées.

A cet égard, il doit mettre en place des mesures de sécurisation de son système d'information et permet en l'espèce « *de s'assurer de l'usage adéquat des ressources des accès privilégiés* ».

Concernant les mesures mises en place pour ne pas méconnaitre les droits des personnes, l'établissement précise que les salariés sont informés de l'enregistrement de leurs sessions quand ils se connectent à l'environnement sécurisé et les salariés sur les postes desquels la prise en main à distance est effectuée sont également informés de cet enregistrement, et ces derniers doivent l'accepter pour qu'elle ait lieu.

La Commission relève en outre qu'il résulte de l'article 270-2 de 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 que « *Les entreprises assujetties organisent la gestion de leur risque informatique de façon à :*

- *identifier le risque informatique auquel elles sont exposées pour l'ensemble de leurs actifs informatiques et de leurs données utilisées pour leurs différentes activités opérationnelles, de support ou de contrôle ;*
- *évaluer ce risque, au regard de leur appétit pour le risque, en tenant compte des menaces et des vulnérabilités connues ;*
- *adopter des mesures adéquates de réduction du risque informatique, y compris des contrôles ;*
- *surveiller l'efficacité de ces mesures et informer les dirigeants effectifs et l'organe de surveillance de leur bonne exécution.*

Les entreprises assujetties s'assurent à cette fin que le contrôle interne de leur risque informatique est organisé conformément aux dispositions des articles 12 et 14 du présent arrêté ».

Au vu de ce qui précède, la Commission considère que le traitement est justifié, conformément à l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité : nom, prénom des salariés ; nom, prénom des prestataires ;
- données d'identification électronique (logs) : pour les salariés : email, login, numéro de pc ou de client léger ainsi que l'adresse IP ; pour les prestataires : adresse mail, login, adresse IP ;
- session : enregistrement des sessions ;
- informations temporelles : horodatages.

Concernant les salariés, les informations d'identité proviennent du traitement ayant pour finalité « *Gestion administrative des salariés* » tandis que les données d'identification électronique ont pour origine le traitement ayant pour finalité « *Gestion des habilitations* ».

Les prestataires communiquent au responsable de traitement les informations relatives à leurs personnels.

Enfin, l'enregistrement des sessions et l'horodatage sont issus du système.

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 des personnes concernées est assurée au moyen d'une procédure interne accessible en Intranet et par l'affichage « *d'un pop-up avec la nécessité d'un clic d'acceptation de ce traitement* ».

L'information délivrée sur le pop-up est jointe au dossier et concerne à la fois les salariés ou prestataires qui font la prise en mains, ou les salariés qui en sont l'objet.

La Commission constate que l'information des personnes concernées est effectuée de manière conforme aux dispositions de 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 responsable de traitement indique que le droit d'accès s'effectue par voie postale, sur place ou par courrier électronique auprès du « *Data Protection Officer* ».

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit s'exercer 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.

V. Sur les communications d'informations et les personnes ayant accès au traitement

- ***Sur les accès***

Le responsable de traitement indique qu'ont accès aux informations :

- les RSI : gestion et administration de la solution, accès aux enregistrements qu'en cas d'accord et validation des RSSI ;
- les RSSI : consultation, contrôle et validation ;
- l'utilisateur (support interne et administrateurs systèmes et réseaux), accès à ses propres enregistrements.

La Commission rappelle qu'une liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit lui être communiquée à première réquisition

Elle considère que ces accès sont justifiés.

- ***Sur les communications d'informations :***

S'agissant d'un traitement mis en œuvre dans le cadre d'obligations prudentielles pesant sur le responsable de traitement la Commission considère que les informations peuvent être communiquées aux Autorités dûment habilitées à en connaître.

VI. Sur les rapprochements et interconnexions avec d'autres traitements

Le responsable de traitement indique des interconnexions avec les traitements légalement mis en œuvre ayant pour finalités respectives la « *Gestion administrative des salariés* » et la « *Gestion des habilitations informatiques et traçabilité des accès* », à des fins d'identification.

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

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.

Cependant les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

En outre, la Commission rappelle que la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

La Commission rappelle enfin 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.

VIII. Sur la durée de conservation

Le responsable de traitement indique que les informations sont conservées 1 an à compter de leur collecte ou production.

La Commission considère que cette durée de conservation 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 ;

- que les informations peuvent être communiquées aux Autorités dûment habilitées à en connaître.

Rappelle que :

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

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé ;

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

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 CFM Indosuez Wealth, du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des prises en main à distance sur l'environnement CFM IW* ».**

Le Président

Guy MAGNAN