Délibération n° 2020-134 du 22 octobre 2020

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre de la modification du traitement automatisé d'informations nominatives ayant pour finalité

« *Contrôle d'accès par badge aux différentes zones des bâtiments de CFM Indosuez Wealth* »

présenté par CFM Indosuez Wealth.

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention 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 la délibération n° 2010-43 du 15 novembre 2010 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les dispositifs de contrôle d'accès sur le lieu de travail mis en œuvre par les personnes physiques ou morales de droit privé ;

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 délibération n° 2012-121 du 23 juillet 2012 de la Commission de Contrôle des Informations Nominatives portant autorisation sur la demande présentée par le CFM Monaco relative à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle d'accès par badge aux différentes zones des bâtiments du CFM* » ;

Vu la demande d'autorisation modificative déposée par le CFM Indosuez Wealth, le 25 juin 2020, concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle d'accès par badge aux différentes zones des bâtiments de CFM Indosuez Wealth* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 24 août 2020, conformément à l'article 11-1 de Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 22 octobre 2020 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, 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* ».

Conformément aux dispositions de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, la Commission a autorisé la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle d'accès par badge aux différentes zones des bâtiments du CFM* », objet de la délibération n° 2012-121 du 23 juillet 2012.

Le CFM Indosuez Wealth souhaite désormais modifier le traitement dont s'agit, en application de l'article 9 de la Loi n° 1.165 du 23 décembre 1993, afin notamment de renforcer la sécurité de son système et de modifier en conséquence la technologie de badge utilisée.

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 traitement a pour finalité « *Contrôle d'accès par badge aux différentes zones des bâtiments de CFM Indosuez Wealth* ».

Les personnes concernées sont les collaborateurs, les visiteurs hors clients et les prestataires.

Enfin, les fonctionnalités du traitement sont les suivantes :

- gestion des habilitations d'accès (profil, droits d'accès,…) ;
- gestion de l'ouverture des portes d'accès ;
- gestion des évènements (logs) ;
- gestion des accès aux bâtiments de toutes les personnes concernées ;
- sécurité des biens et des personnes au sein de la banque ;
- constitution de preuves en cas d'infractions.

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 responsable de traitement indique que le traitement est justifié par la réalisation d'un intérêt légitime, sans que ne soient méconnus les droits et libertés fondamentaux de la personne concernée ;

A cet égard, la Commission prend acte des précisions du responsable de traitement selon lesquelles le système est mis en place par l'établissement uniquement afin de gérer efficacement les entrées de ses collaborateurs et des prestataires de service intervenant de manière ponctuelle ou pour une durée contractuelle et qu'il permet également de recenser les accès aux locaux des visiteurs occasionnels (hors clients).

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 traitées

Le responsable de traitement indique que les informations exploitées aux fins du présent traitement sont :

- identité/situation de famille : nom patronymique, prénom, matricule et photographie pour les collaborateurs, nom patronymique et prénom pour les prestataires, nom, prénom et signature pour les visiteurs ;
- formation – diplômes – vie professionnelle : service interne d'affectation et profil d'accès, type de contrat, catégorie d'information pour les collaborateurs/ prestataires, nom de l'employeur pour les visiteurs ;
- informations temporelles : date, heure ouverture et fermeture porte sous contrôle d'accès pour les collaborateurs/ prestataires, date, heure d'arrivée et heure de départ pour les visiteurs ;
- visite : personne visitée et motif de la visite pour les visiteurs ;
- données d'identification électronique : journalisation des accès et actions du personnel habilité sur la base collaborateurs/prestataires.

Il appert par ailleurs à l'étude du dossier que le numéro de badge est également collecté pour les collaborateurs et les visiteurs.

Les informations relatives à l'identité/situation de famille, à la formation, aux diplômes et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* » pour les collaborateurs, la Direction des Services et des Moyens Généraux (DSMG) pour les prestataires et la personne elle-même pour les visiteurs.

Par ailleurs, les informations temporelles sont générées par le système pour les collaborateurs/prestataires et ont pour origine la personne elle-même pour les visiteurs.

Enfin, la Commission constate que les données d'identification électronique ont pour origine le présent traitement.

Au vu de ce qui précède, la Commission considère que les informations traitées 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 des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est effectuée par une rubrique propre à la protection des données accessible en ligne et par une procédure interne accessible en Intranet.

Ces documents n'ayant pas été joints à la demande, la Commission rappelle qu'ils doivent impérativement contenir toutes les dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Elle rappelle par ailleurs que cette information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, y compris les prestataires et les visiteurs.

Sous ces conditions, la Commission considère que les modalités d'information préalable sont conformes aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

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

Le droit d'accès s'exerce par voie postale, par courrier électronique ou sur place auprès du « *Data Protection Officer de CFM Indosuez* ».

A cet égard, la Commission rappelle que la réponse à ce 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 cette condition, la Commission estime 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 destinataires et les personnes ayant accès au traitement

- ***Sur les destinataires***

Les informations sont susceptibles d'être communiquées à la Direction de la Sûreté Publique.

La Commission estime qu'une telle communication peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

La Commission considère donc que ces transmissions sont conformes aux exigences légales.

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

Les personnes ayant accès au traitement sont :

- la Direction des Services et des Moyens Généraux (DSMG) : inscription, modification, mise à jour et consultation ;
- le PC Sécurité : consultation des deux bases (collaborateurs/prestataires et visiteurs), inscription et modification uniquement pour la base visiteurs ;
- l'accueil : consultation, inscription et modification uniquement pour la base visiteurs ;
- l'Inspection Générale, l'Audit, la Direction des Ressources Humaines et le Responsable de la Sécurité des Systèmes d'Information : consultation exclusivement sur demande ;
- le personnel habilité du prestataire informatique : tous droits dans le cadre des opérations de maintenance et support.

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

Concernant la Direction des Ressources Humaines, la Commission rappelle qu'un tel accès en consultation ne peut s'effectuer que dans le cadre d'une procédure disciplinaire en lien avec les fonctionnalités du présent traitement.

Elle exclut donc l'utilisation des données par la Direction des Ressources Humaines à des fins disciplinaires autres que celles prévues expressément par les fonctionnalités du traitement.

En ce qui concerne le prestataire, elle 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 son contrat de prestation de service. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

La Commission 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

Le responsable de traitement indique que le présent traitement fait l'objet de rapprochements et d'interconnexions avec les traitements ayant respectivement pour finalité « *Gestion administrative des salariés* », « *Contrôle d'accès aux locaux d'importance stratégique par badge biométrique reposant sur la reconnaissance de l'empreinte digitale* » et « *Gestion et supervision de la messagerie électronique* ».

La Commission relève par ailleurs à l'étude du dossier un rapprochement avec un traitement ayant pour finalité *« Gestions des habilitations informatique et traçabilité des accès* ».

Elle constate que tous ces traitements ont 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 rappelle néanmoins que 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.

Elle rappelle que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception, conformément à la délibération n° 2010-13 du 3 mai 2010.

La Commission rappelle également 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 relatives à l'identité/situation de famille, à la formation, aux diplômes et à la vie professionnelle sont conservées le temps de la présence dans l'entreprise pour les collaborateurs/ prestataires et l'année en cours plus 2 ans pour les visiteurs.

Concernant ces derniers, la Commission rappelle que, conformément à sa délibération n° 2010-43 du 15 novembre 2010, les informations les concernant ne doivent pas être conservées au-delà d'une durée de trois mois.

Elle fixe donc la durée de conservation des données relatives aux visiteurs à trois mois à compter de leur collecte.

Le responsable de traitement indique enfin que les informations temporelles sont conservées 30 jours et les données d'identification électronique 5 mois conformément à ses obligations réglementaires.

La Commission considère que ces durées sont conformes 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 :

- les documents d'information préalable doivent impérativement contenir toutes les dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;
- l'information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, y compris les prestataires et les visiteurs ;
- la réponse au droit d'accès doit intervenir dans le mois suivant la réception de la demande ;
- la Direction de la Sûreté Publique ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées ;

- tout accès en consultation par la Direction des Ressources Humaines ne peut s'effectuer que dans le cadre d'une procédure disciplinaire en lien avec les fonctionnalités du présent traitement ;

- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit 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 du présent traitement et de traitements faisant l'objet de rapprochements avec celui-ci devra être chiffrée sur son support de réception.

Exclut l'utilisation des données par la Direction des Ressources Humaines à des fins disciplinaires autres que celles prévues expressément par les fonctionnalités du traitement.

Fixe la durée de conservation des données relatives aux visiteurs à trois mois à compter de leur collecte.

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 de la modification du traitement automatisé d'informations nominatives ayant pour finalité « *Contrôle d'accès par badge aux différentes zones des bâtiments de CFM Indosuez Wealth* ».**

Le Président

Guy MAGNAN