Délibération n° 2021-165 du 21 juillet 2021

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

« *Gestion et traçabilité des habilitations informatiques* »

présenté par la Compagnie Monégasque de Banque

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° 1.338 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 délibération n° 2017-206 du 20 décembre 2017 de la Commission de Contrôle des Informations Nominatives portant recommandation sur la gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au système d'information ;

Vu la délibération n°2017-100 du 21 juin 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 traçabilité des habilitations informatiques* » présenté par la Compagnie Monégasque de Banque ;

Vu la demande d'autorisation modificative déposée par la Compagnie Monégasque de Banque le 15 avril 2021 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion et Traçabilité des Habilitations Informatiques* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 14 juin 2021, 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 21 juillet 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Compagnie Monégasque de Banque (CMB) est une société anonyme monégasque immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 76S01557, qui a pour objet « *de faire dans la Principauté de Monaco (…) toutes opérations bancaires et financières (…)* ».

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 « *Gestion et traçabilité des habilitations informatiques* » présenté par la Compagnie Monégasque de Banque, objet de la délibération n° 2017-100 du 21 juin 2017.

La Compagnie Monégasque de Banque souhaite modifier le traitement dont s'agit, en application de l'article 9 de la Loi n° 1.165 du 23 décembre 1993 afin de modifier l'infrastructure technique et conserver sur un fichier un référentiel administratif des habilitations informatiques attribuées aux collaborateurs de CMB.

La licéité et la justification du traitement ainsi que les droits des personnes concernées sont inchangés.

I. Sur les nouvelles fonctionnalités du traitement

Le responsable de traitement indique que le traitement a pour finalité « *Gestion et Traçabilité des Habilitations Informatiques* ».

Les personnes concernées sont les collaborateurs du Groupe CMB et les prestataires.

Enfin, les fonctionnalités sont désormais les suivantes :

Dans le cadre de la Gestion des Habilitations *:*

- octroyer et délivrer aux personnes concernées les moyens techniques et fonctionnels permettant de s'authentifier aux différents Systèmes d'Information afin d'exercer la fonction et les missions pour lesquelles elles ont été recrutées, ceci dans le respect du « *Moindre Privilège* » et du « *Besoin d'en connaître* » ;
- créer et gérer des profils utilisateurs standard, s'assurant notamment de la séparation des tâches, en cohérence avec les fonctions de chacun au sein de la société ;
- administrer les droits d'accès aux applications et aux dossiers hébergés sur les serveurs ;
- gérer les évolutions des droits, les mobilités et les départs ;
- mettre à jour les comptes système et les informations administratives s'y rapportant (changement de patronyme, type et échéance de contrat, coordonnées professionnelles,…) ;

- permettre la réalisation de l'ensemble des tâches d'activation/désactivation/suppression de comptes système, de mise à jour des listes de contrôles d'accès, des groupes de privilèges auxquels la personne concernée appartient ou est habilitée ;
- procéder à des contrôles afin de s'assurer de la conformité des droits délivrés par rapport aux règles édictées en matière d'accès à l'information.

Dans le cadre de la supervision :

- collecter des évènements systèmes permettant de tracer les habilitations octroyées, visant à prévenir le risque de fraude et à s'assurer de la cohérence des accès ;
- procéder à la détection éventuelle de comportements anormaux ;
- établir des reportings à usage interne ;
- conserver sur un fichier un référentiel administratif des habilitations informatiques attribuées aux collaborateurs de CMB.

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 les données collectées

Les informations nominatives traitées sont désormais les suivantes :

➢ Pour les habilitations

- identité : nom, prénom ;
- adresses et cordonnées professionnelles : adresse postale, coordonnées téléphoniques (mobile/fixe) ;
- formation – diplômes – vie professionnelle : fonction professionnelle ;
- données d'identification électronique : comptes système, identifiant numérique, adresse mail ;
- informations temporelles : date, heure ;
- biens techniques et fonctionnels : énumération des outils, applications et profils associés ;
- journalisation : logs, évènements et accounting système, comptes utilisateurs.

➢ Pour le référentiel administratif

- identité : nom, prénom ;
- adresses et cordonnées professionnelles : coordonnées téléphoniques (mobile/fixe) ;
- formation – diplômes – vie professionnelle : fonction professionnelle ;
- données d'identification électronique : comptes système, identifiant numérique, adresse mail ;
- biens techniques et fonctionnels : énumération des outils, applications et profils associés.

Le responsable de traitement indique que les informations relatives à l'identité, aux adresses et coordonnées professionnelles, à la formation, aux diplômes et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* ».

La Commission considère toutefois que concernant les prestataires externes ces informations ont pour origine le contrat de prestation de service.

Les données d'identification électronique ont pour origine le service informatique et le département IT.

Les informations temporelles et la journalisation ont pour origine le système.

Enfin, les biens techniques et fonctionnels ont pour origine le Management.

La Commission considère ainsi 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.

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

➢ *Sur les destinataires*

Le responsable de traitement indique tout d'abord que les informations collectées dans le cadre de ce traitement peuvent être communiquées aux organes de contrôle interne de CMB (Audit interne, Contrôle Permanent et Compliance).

Il indique par ailleurs que les informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires dans le cadre de leurs missions légalement conférées.

La Commission considère ainsi que le Service d'Information et de Contrôle des Circuits Financiers (SICCFIN) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires d'informations nominatives traitées.

Par ailleurs, elle estime que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, la Commission rappelle qu'en cas de transmission, ces Autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

Sous ces conditions, elle considère que de telles transmissions 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 désormais les suivantes :

- le Département RH : inscription pour la saisie des informations administratives ;
- le Manager de la personne concernée : inscription et mise à jour pour formuler la demande de droits d'accès ;
- le Département Informatique : tous droits dans le cadre de leurs missions d'administration des objets système ;
- le HelpDesk Fonctionnel : maintenance récurrente et relation avec le prestataire hébergeur de la solution ;
- le prestataire hébergeur : tous droits pour l'administration des profils et objets système relevant de la plateforme qu'il opère, sur instruction et sous contrôle de CMB Monaco ;
- le RSSI/DPO : consultation sur l'ensemble du périmètre en sa qualité de contrôleur et valideur.

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

La Commission rappelle toutefois 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.

IV. Sur les interconnexions et rapprochements

Le responsable de traitement indique que « *Tous les traitements automatisés et exploités par CMB Monaco y compris les traitements externalisés, sont interconnectés avec ce traitement qui est le point de convergence et de contrôle des habilitations d'accès au Systèmes d'information* ».

La Commission en prend acte.

Elle considère par ailleurs que le présent traitement pourra également être interconnecté avec des traitements futurs de la Compagnie Monégasque de Banque, à des fins de sécurité.

V. 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 les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

Elle rappelle également que la copie ou l'extraction d'informations issues de ce traitement devra 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.

VI. Sur les durées de conservation

Le responsable de traitement indique que les informations liées à l'identité, aux adresses et coordonnées professionnelles, à la formation, aux diplômes et à la vie professionnelle ainsi que les données d'identification électronique et les informations liées aux biens techniques et fonctionnels sont désormais conservées 5 ans après le départ du salarié.

A cet égard, concernant les informations liées aux habilitations, la Commission rappelle que, conformément à sa délibération n° 2017-206 du 20 décembre 2017, celles-ci ne doivent pas être conservées au-delà d'une durée de 3 mois après le départ de la personne concernée.

De même, elle rappelle que les données d'identification électronique (login / mot de passe) ne doivent être conservées que le temps de présence dans la banque.

Le responsable de traitement indique par ailleurs que les informations temporelles et la journalisation sont conservées 1 an glissant.

Il précise de plus que les fichiers Excel contenant les données relatives aux droits d'accès d'un collaborateur (référentiel administratif) sont conservés 5 ans.

La Commission considère que ces durées de conservation sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Considère que le présent traitement pourra être également interconnecté avec des traitements futurs de la Compagnie Monégasque de Banque, à des fins de sécurité.

Rappelle que :

- le SICCFIN et la CCAF peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires des informations du traitement ;

- les Autorités judiciaires ne peuvent avoir accès aux informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- 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 les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort ;

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

Fixe les durées de conservation suivantes pour les informations liées aux habilitations :

- 3 mois après le départ de la personne concernée pour les informations liées aux habilitations ;

- le temps de présence dans la banque pour les données d'identification électronique (login / mot de passe).

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 la Compagnie Monégasque de Banque de la modification du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et Traçabilité des Habilitations Informatiques* ».**

Le Président

Guy MAGNAN