Délibération n° 2022-099 du 20 juillet 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

« *Gérer les comptes ayant des accès privilégiés* »

présenté par EFG BANK (MONACO) SAM

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° 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 demande d'autorisation déposée par EFG BANK (MONACO) SAM le 16 mai 2022 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gérer les comptes ayant des accès privilégiés* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 15 juillet 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 20 juillet 2022 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

EFG BANK (MONACO) SAM est une société monégasque, immatriculée au Répertoire du Commerce et de l'industrie sous le numéro 90S02647, ayant entre autres pour objet de « *faire dans la Principauté de Monaco et à l'étranger, pour elle-même, pour le compte de tiers ou en participation, toutes opérations de banque, de crédit, de financement, d'escompte, de garantie, de détention, de conservation, de dépôt, d'administration, de gestion, de bourse, de courtage, de change, ainsi que toutes opérations d'acquisition, d'offre et de cession de valeurs mobilières, d'effets de commerce, de métaux précieux et d'autres instruments d'investissement et de placement* ».

Afin de fournir un accès privilégié et sécurisé aux ressources informatiques et répondre aux exigences règlementaires en gérant et en surveillant les comptes à forts privilèges, cette société souhaite mettre en place une solution de gestion des accès privilégiés.

Le traitement objet de la présente demande permet de surveiller les accès au système d'information, 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 « *Gérer les comptes ayant des accès privilégiés ».*

Les personnes concernées sont les salariés.

Enfin, les fonctionnalités de ce traitement sont les suivantes :

- permettre un accès à certains environnements précis et restreints du Système d'Information de l'établissement financier de Monaco de manière sécurisée ;
- gérer les comptes à forts privilèges à l'aide d'une solution de gestion des accès privilégiés ;
- assurer la rotation des mots de passe des comptes à forts privilèges ;
- permettre la traçabilité des sessions et l'imputabilité des actions ;
- vérifier, *a posteriori*, si nécessaire, les actions réalisées par les administrateurs de la solution (levée de doutes) et disposer, le cas échéant, de preuves ou de début de preuves si de besoin ;
- conserver des éléments retraçant la réalisation des opérations effectuées par les administrateurs à des fins, le cas échéant, de vérification et de compréhension d'une situation donnée ;
- assurer les opérations de suivi et de maintenance des équipements et ressources de la solution ;
- enregistrer les sessions (vidéo des actions réalisées par les utilisateurs de la solution).

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 poursuivi [par lui et qui] ne méconnait ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée* ».

A cet égard, la Commission prend acte que la mise en place du traitement dont s'agit « *permet d'assurer la disponibilité des ressources informatiques de EFG Bank en environnement sécurisé* ».

Elle note également qu'« *Une note d'information sera transmise aux salariés pour les informer que leurs sessions seront enregistrées* ».

Au vu de ce qui précède, 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 :

- données d'identification électronique : compte accès à la solution ;
- informations temporelles : logs de connexion sur le réseau, à savoir données d'horodatage, identifiant de l'utilisateur, serveur cible, login, adresse IP de la connexion (pare-feu) ;
- éléments de la solution : identifiant de l'utilisateur, enregistrements des sessions (vidéo des actions réalisées par l'utilisateur) .

Les informations relatives aux données d'identification électronique ont pour origine le traitement ayant pour finalité « *Gestion administrative du salarié* ».

Par ailleurs, les informations temporelles et les éléments de la solution ont pour origine le présent traitement.

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.

IV. Sur les droits des personnes concernées

➢ *Sur l'information préalable des personnes concernées*

L'information préalable des personnes concernées s'effectue par le biais d'une mention ou clause particulière intégrée dans un document remis à l'intéressé.

Ce document n'ayant pas été joint à la demande, la Commission rappelle que celui-ci doit 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 responsable de traitement indique que le droit d'accès s'exerce par courrier électronique.

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 considère 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***

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

La Commission estime ainsi 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 donc que de telles transmissions sont conformes aux exigences légales.

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

Les personnes habilitées à avoir accès au traitement sont :

- le RSSI (Monaco) : tout accès dans le cadre des ses missions de validation et de contrôle ;
- les administrateurs Groupe de la solution : tout accès ;
- les administrateurs de Monaco et du Groupe infra et réseaux : accès aux ressources qu'ils doivent administrer et à leurs propres enregistrements de session.

A cet égard, le responsable de traitement indique que « *Les enregistrements des sessions ne peuvent être lus que par la personne qui les a générés, son responsable direct et les membres de son équipe* ».

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

La Commission rappelle par ailleurs 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 présent traitement fait l'objet d'une interconnexion avec le traitement ayant pour finalité « *Gestion administrative des salariés* ».

A cet égard, la Commission prend acte que ce traitement a été légalement mis en œuvre et souligne que cette interconnexion est conforme 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 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 également que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

Enfin, la Commission rappelle 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 les durées de conservation

Le responsable de traitement indique que les données d'identification électronique sont conservées 3 mois après le départ du salarié afin de permettre « *d'identifier le salarié en cas d'acte malveillant effectué avant son départ et ayant des conséquences dans les trois mois qui suivraient son départ* ».

Par ailleurs, les informations temporelles et les éléments de la solution sont conservés 12 mois glissants.

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 :

- l'information préalable 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 ;

- 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 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 devra être chiffrée sur son support de réception.

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 EFG BANK (MONACO) SAM du traitement automatisé d'informations nominatives ayant pour finalité « *Gérer les comptes ayant des accès privilégiés* ».**

Le Président

Guy MAGNAN