Délibération n° 2020-116 du 16 septembre 2020

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 habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle des accès au Système d'Information* »

présenté par Barclays Bank PLC (succursale de Monaco)

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 la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée ;

Vu la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, modifiée ;

Vu la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;

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'Ordonnance Souveraine n° 1.284 du 10 septembre 2007, modifiée, portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 7.065 du 26 juillet 2018 portant modification de l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la loi n° 1.362 du 3 août 2009, modifiée, relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

Vu l'Arrêté Ministériel n° 2012.199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers ;

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 Barclays Bank PLC (succursale de Monaco) le 25 mai 2020 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle des accès au Système d'Information* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 23 juillet 2020, 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 16 septembre 2020 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Barclays Bank PLC est une société anglaise établie à Monaco par sa succursale enregistrée au RCI sous le numéro 68S01191, ayant pour activité « *la réalisation de toutes opérations de banque et connexes, telles que définies par la Loi bancaire* ».

Afin de sécuriser l'accès à son système d'information (SI), cette société souhaite mettre en place un système d'habilitations.

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 « *Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle des accès au Système d'Information ».*

Les personnes concernées sont l'ensemble des utilisateurs du système d'information.

Enfin, les fonctionnalités de ce traitement sont les suivantes :

Dans le cadre de la gestion des habilitations *:*

- octroyer / délivrer aux utilisateurs du SI les moyens techniques et fonctionnels permettant de s'authentifier au système d'information afin de pouvoir exercer la fonction et les missions pour lesquelles ils ont été recrutés ;
- gérer les évolutions de droits, les mobilités internes et les départs ;
- mettre à jour les comptes systèmes dans le cadre de changement d'informations administratives (ex : changement de patronyme) ;
- permettre la réalisation de l'ensemble des tâches d'activation/ désactivation/suppression de comptes ;

- procéder à des revues de contrôles périodiques afin de s'assurer de la conformité des droits délivrés par rapport aux demandes et aux règles édictées en matière d'accès à l'information.

Dans le cadre de la supervision des accès aux applications :

- collecter des évènements systèmes (logs) permettant de tracer les accès des utilisateurs aux applications et données ;
- établir des alertes et/ou des rapports qui permettent de détecter tout risque de malveillance et de s'assurer de la cohérence des accès avec les habilitations délivrées ;
- établir des preuves en cas de litige avec tout utilisateur (employé, prestataire…).

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 tout d'abord justifié par le respect d'une obligation légale, à savoir les obligations particulières de vigilance ainsi que de traçabilité des opérations effectuées imposées aux établissements bancaires ou assimilés.

Il précise ainsi que ces obligations sont prévues, entre autres, par les textes suivants :

- la Loi n° 1.338 du 7 septembre 2007 sur les activités financières et son Ordonnance Souveraine d'application ;
- la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, et son Ordonnance Souveraine d'application – modifiée le 6 juillet 2018 (JO 8389) ;
- la Loi n° 1.314 du 29 juin 2006 relative à l'exercice d'une activité de conservation ou administration d'instruments financiers ;
- l'Arrêté Ministériel n° 2012-199 du 5 avril 2012 relatif aux obligations professionnelles des établissements de crédit teneurs de comptes-conservateurs d'instruments financiers.

Le responsable de traitement indique par ailleurs que le traitement est également 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 observe que ledit traitement va permettre :

- « *l'optimisation de l'accomplissement des missions de travail de ses employés ;*
- *la sécurité et le bon fonctionnement technique du réseau ou système informatique ;*
- *la préservation des intérêts économiques, commerciaux ou financiers du responsable de traitement ou de son représentant ;*
- *la prévention et la détection a priori et a posteriori de toute activité non-conforme ou illicite, par des utilisateurs* ».

Elle considère donc que le traitement est justifié, conformément aux dispositions de l'article 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, prénom et matricule de l'employé, nom, prénom et matricule du responsable ;
- adresses et coordonnées : numéros de téléphone fixe et mobile professionnels, adresse email professionnelle ;
- formation, diplômes, vie professionnelle : entité, service, poste occupé (titre), localisation ;
- données d'identification électronique : identifiants de la personne habilitée ;
- informations temporelles : logs, horodatage, fichiers journaux ;
- compte utilisateur : nom et domaine du compte d'utilisateur, type de droits attribués.

Les informations relatives à l'identité, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle, aux données d'identification électronique et au compte utilisateur ont pour origine le traitement ayant pour finalité « *Gestion du personnel* ».

Par ailleurs, les informations temporelles ont pour origine le système d'information.

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 est effectuée par le biais d'un document spécifique et d'une procédure interne accessible en Intranet.

Ces documents n'ayant pas été joints à la demande, la Commission rappelle 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 voie postale ou par courrier électronique.

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 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 tout d'abord que les informations collectées sont communiqués à l'infocentre du Groupe Barclays, via le DTU (cloud privé pour les échanges de fichiers au sein du Groupe Barclays et avec des tiers autorisés), situé aux Etats-Unis.

Il indique également que « *Le Groupe Barclays dispose d'un Active Directory centralisé (domaine Intranet), répliqué sur les contrôleurs de domaines des différentes entités du Groupe Barclays* ».

Les pays concernés par ces communications ne disposant pas d'un niveau de protection adéquat au sens de la Loi n° 1.165 du 23 décembre 1993, la licéité de ces communications d'informations nominatives sera analysée dans les deux demandes d'autorisation de transfert concomitamment soumises.

Le responsable de traitement 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***

Les personnes habilitées à avoir accès au traitement sont :

- le Service Informatique de Barclays Monaco : tous droits dans le strict cadre de ses missions de gestion des habilitations informatiques sur le périmètre des systèmes hébergés à Monaco ;
- les équipes IAM (Identity and Access Management) : inscription, modification dans le strict cadre de leur mission de gestion des habilitations informatiques sur le périmètre des systèmes hébergés hors Monaco ;
- les équipes GTIS (Group Technology Infrastructure Services) : maintenance dans le strict cadre de leur mission de gestion des équipements informatiques du Groupe Barclays.

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

La Commission relève que les équipes IAM Support « *sont localisées en Inde en accord avec la stratégie de localisation des équipes support du Groupe* » et que « *leur rôle est principalement de gérer les actions d'octroi et de revue des accès informatiques dans le cadre des procédures d'arrivées, départs et mutations des employés* ».

Elle 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.

Elle rappelle enfin que si des prestataires techniques devaient avoir accès au traitement, leurs droits d'accès devront être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, et qu'ils seront soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de l'article 17 de la Loi n° 1.165 du 23 décembre 1993.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion avec un traitement ayant pour finalité « *Gestion du personnel* ».

A cet égard, la Commission prend acte que ce traitement a été légalement mis en œuvre.

Elle relève par ailleurs que ce traitement est également interconnecté avec les applications « *OneCert* » et « *GIS Metrics* », ainsi qu'avec le traitement lié à l'application « *Request* » pour, entre autres, l'octroi et la revue des accès informatiques dans le cadre des procédures d'arrivées, départs et mutations des employés.

Ces traitements n'ayant pas fait l'objet de formalité auprès de la CCIN, la Commission demande au responsable de traitement de les lui soumettre dans les plus brefs.

Le responsable de traitement indique enfin que le présent traitement est également interconnecté avec tous les traitements déjà mis en place ou à venir.

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, 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 l'ensemble des informations est conservée 15 mois après le départ de la personne concernée.

A cet égard, la Commission prend acte des précisions du responsable de traitement selon lesquelles « *les données relatives à la gestion des habilitations et accès informatiques servent d'évidences dans le cadre des audits externes que le Groupe Barclays subit chaque année* » et que *« Les données des employés ayant quitté le Groupe durant l'année fiscale auditée doivent donc être conservées jusqu'au mois de mars de l'année suivante* ».

Elle considère donc 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 :

- les documents d'information préalable des personnes concernées doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- 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 ;

- si des prestataires techniques devaient avoir accès au traitement, leurs droits d'accès devront être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, et qu'ils seront soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de l'article 17 de la Loi n° 1.165 du 23 décembre 1993 ;

- 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.

Demande que les traitements liés aux applications « *OneCert* », « *GIS Metrics* » et « *Request* » lui soient soumis dans les plus brefs délais.

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 Barclays Bank PLC (succursale de Monaco) du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations et des accès mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* ».**

Le Président

Guy MAGNAN