Délibération n° 2021-246 du 17 novembre 2021

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

« *Mise en place d'un dispositif de surveillance, de détection et d'alerte des menaces internes à la cybersécurité de Barclays, dénommé EXABEAM* »

présenté par Barclays Execution Services Limited,
représenté en Principauté 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 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 demande d'autorisation déposée par Barclays Execution Services Limited, représentée en Principauté par Barclays Bank PLC (succursale de Monaco) le 23 juillet 2021 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Mise en place d'un dispositif de surveillance, de détection et d'alerte des menaces internes à la cybersécurité de Barclays, dénommé EXABEAM* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 21 septembre 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 17 novembre 2021 portant examen du traitement automatisé susvisé.

## La Commission de Contrôle des Informations Nominatives,

### Préambule

Barclays Execution Services Limited est une société anglaise, représentée en Principauté par Barclays Bank PLC, 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 se prémunir contre les menaces internes de cybersécurité, cette société souhaite se doter d'un outil d'agrégation qui rassemble les alertes de détection des comportements anormaux et risqués des utilisateurs du système d'information de Barclays.

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 « *Mise en place d'un dispositif de surveillance, de détection et d'alerte des menaces internes à la cybersécurité de Barclays, dénommé EXABEAM ».*

Les personnes concernées sont les « *Salariés de Barclays Bank PLC Monaco* ».

Enfin, les fonctionnalités de ce traitement sont de permettre grâce à l'outil d'agrégation EXABEAM de rassembler « *les alertes de détection des comportements anormaux et risqués des utilisateurs du système d'information de Barclays, qui indiquent des menaces de cybersécurité dans l'environnement de Barclays* ».

A cet égard, la Commission prend note que « *Les principales menaces contre lesquelles EXABEAM protège sont les suivantes :*

- *exfiltration de données : email (taille/nombre), USB (accès/volumes), impression (taille/volume) ;*
- *actions d'obfuscation : utilisation du réseau TOR (navigation anonyme) ou d'outils d'évitement de proxy ;*
- *contexte : visites de sites Web indiquant un risque (risque de fuite) ;*
- *violation de l'utilisation acceptable des accès : accès à des sites Web inappropriés (tels que les sites de jeux d'argent ou pornographiques), accès anormal aux locaux et bureaux (utilisation anormale des badges vu les habilitations délivrées) ;*
- *activité logicielle malveillante/non autorisée : accès à des domaines malveillants/risqués ;*
- *accès non autorisé : changement de compte, activités de gestion de compte, utilisation par un personnel non-exécutif d'identifiants réservés au personnel exécutif, connexion anormale à un actif essentiel, utilisation de comptes désactivés ».*

Elle relève également que « *EXABEAM comprend le comportement habituel des utilisateurs et met en évidence les activités anormales grâce à un système de notation basé sur les règles suivantes :*

- *règles basées sur les faits : par ex., une personne cherche à utiliser un dispositif de stockage portable sur le réseau Barclays, une personne cherche à utiliser un badge pour accéder aux locaux ;*
- *règles basées sur des modèles : EXABEAM comprend la compréhension du comportement typique des utilisateurs dans l'environnement Barclays et met en évidence les activités qui s'écartent de ce comportement normal, par ex. un nombre anormal d'e-mails sortants.*

*Ces règles peuvent être utilisées en trois catégories : organisation (première fois qu'une alerte de sécurité a été vue dans l'organisation), groupe (accès anormal à un actif pour le groupe), utilisateur (activité anormale pour un utilisateur).*

*Si les conditions de la règle sont remplies, des points risque sont attribués à l'utilisateur. Lorsque le nombre de points risque attribués à un utilisateur dans un laps de temps défini atteint un seuil critique (80 pour la surveillance standard), cette activité sera examinée et évaluée par l'équipe chargée des menaces internes de Barclays ».*

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. <u>Sur la licéité et la justification du traitement</u>

Le traitement est tout d'abord justifié par « *le respect d'une obligation légale à laquelle est soumis le responsable de traitement ou son représentant* ».

Le responsable de traitement indique ainsi qu'en vertu de l'article de l'article 23 de la Loi n° 1.138 du 7 septembre 2007 sur les activités financières, modifiée, « *Les sociétés agréées sont tenues d'observer les règles prudentielles et de bonne conduite définies par ordonnance souveraine.* »

Il précise également qu'en vertu de l'article 6 de l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007, modifiée, les sociétés agréées doivent entre autres « *disposer d'une organisation administrative et comptable, ainsi que des mécanismes de sécurité et de contrôle interne et externe adéquats, notamment en ce qui concerne les opérations pour compte propre et les opérations personnelles de leurs salariés* ».

Le traitement est par ailleurs 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 au responsable de traitement d'assurer :

- *« la sécurité et le bon fonctionnement technique du réseau et du système d'information de Barclays ;*
- *la préservation des intérêts économiques, commerciaux ou financiers de Barclays ;*
- *le contrôle du respect des règles internes d'usage des outils de communication électronique ;*
- *la prévention et la détection de toute activité non-conforme ou illicite par des utilisateurs ;*
- *la protection contre tout acte susceptible d'engager la responsabilité civile ou pénale de Barclays, ou de lui porter préjudicie, ainsi qu'à ses clients ;*
- *la prévention des faits illicites et la constitution de preuves* ».

Elle prend acte par ailleurs que « *Le traitement respecte l'intérêt, les droits et libertés fondamentaux des salariés, dont les correspondances privées, les interactions personnelles et la productivité ne sont pas contrôlées* ».

La Commission 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

Le responsable de traitement indique que les informations nominatives traitées sont :

- identité : situation de famille : nom, prénom et identifiant Barclays du salarié, nom, prénom et identifiant Barclays du responsable ;
- adresses et coordonnées : adresse de la messagerie professionnelle du salarié, coordonnées de contact des équipes Compliance et RH Barclays Monaco ;
- formation, diplômes, vie professionnelle : entité, service, poste occupé (titre), localisation ;
- données d'identification électronique : profil des utilisateurs (réglages et opérations autorisées), logs VPN d'accès à distance, logs Web, logs de connexion des personnels habilités à avoir accès au traitement, adresse IP pour l'hôte ;
- informations temporelles : horodatages, date et heure de la réception et de l'envoi des messages électroniques, de navigation, des accès aux locaux, d'impression, de l'alerte, des actions effectuées par les équipes dans le cadre du traitement des incidents ;
- utilisation des systèmes et appareils : détails de l'utilisation des appareils accédant au réseau Barclays, historique de navigation, évènement du client Windows, utilisation USB, volume d'impression, nombre de messages entrants et sortants, nombre de messages nettoyés, nombre de spams, volume, format, pièces jointes, noms de domaine expéditeurs de message, accès aux locaux, alertes haute-fidélité de réponse aux incidents des opérations de cybersécurité ;
- habilitations et logs d'accès : identité des personnes habilitées à avoir accès au traitement, type de droits attribués, logs de connexion des personnels habilités à avoir accès au traitement.

Les informations relatives à l'identité, la situation de famille, les adresses et coordonnées, la formation, les diplômes et la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion du personnel* ».

Les données d'identification électronique ont pour origine les traitements ayant respectivement pour finalité « *Gestion du personnel* », « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance* » et « *Gestion et contrôle des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle des accès au Système d'Information* ».

Les informations temporelles et les données relatives à l'utilisation des systèmes et appareils ont pour origine les traitements ayant respectivement pour finalité « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance* », « *Gestion et contrôle des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle des accès au Système d'Information* » et « *Détection et réponse aux attaques cyberavancées* ».

Enfin, les habilitations et logs d'accès ont pour origine les traitements ayant respectivement pour finalité « *Gestion du personnel* » et « *Gestion et contrôle des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle des accès au 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'une procédure interne accessible en Intranet et par le biais des délégués du personnel.

Les documents d'information 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 responsable de traitement indique que le droit d'accès s'exerce sur place, par voie postale ou par courrier électronique.

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, elle 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 considère 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.

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 :

- les équipes CSO Cyber Operations de Barclays Execution Service Ltd (Royaume-Uni), Barclays Global Service Centre Private Ltd (Inde), Barclays Services Corporation (Etats-Unis) et Barclays Services LLC (Etats-Unis) : consultation (accès aux données en lecture seule), extraction après évaluation ;
- les équipes Security Operations Technology Support de Barclays Execution Service Ltd (Royaume-Uni), Barclays Global Service Centre Private Ltd (Inde), Barclays Services Corporation (Etats-Unis) et Barclays Services LLC (Etats-Unis) : maintenance et consultation limitée (support applicatif, accès possible aux logs et aux données de destination, mais pas au contenu des documents ou communications associés ;
- le prestataire externe (Etats-Unis) : maintenance (Pas d'accès aux données. Accès à distance limité uniquement au système pour effectuer des dépannages, si nécessaire).

La Commission prend acte des précisions du responsable de traitement selon lesquelles les équipes de conformité et RH de Barclays Bank PLC (Succursale de Monaco) ne sont pas des utilisateurs habilités puisqu'elles ne recevront que « *les informations extraites d'EXABEAM, qui sont évaluées et fournies par le petit nombre d'utilisateurs habilités de l'équipe CSO Cyber Operations, lorsqu'elles sont nécessaires pour traiter un problème de sécurité locale ou de conformité* ».

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

La Commission relève toutefois que certains des destinataires des informations sont situés en Inde et aux Etats-Unis.

Aussi, ces pays 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.

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 et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet de cinq interconnexions avec les traitements ayant respectivement les finalités suivantes :

- « *Gestion du personnel* » ;
- « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance* » ;
- « *Gestion et contrôle des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle des accès au Système d'Information* » ;
- « *Détection et réponse aux attaques cyberavancées* » ;
- « *Contrôle d'accès par badge non biométrique* ».

La Commission constate que ces traitements ont été légalement mis en œuvre.

Elle attire toutefois l'attention du responsable de traitement sur le fait qu'il lui appartient de s'assurer que le traitement dont s'agit n'est pas également alimenté par d'autres traitements devant potentiellement faire l'objet de formalités auprès d'elle.

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

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 données ne seront fournies que si elles ont été identifiées comme pertinentes pour une alerte EXABEAM par un autre système de surveillance. S'il est alors déterminé que l'alerte concerne un faux positif, les données liées sont rapidement supprimées pour éviter d'être utilisées dans des analyses futures* ».

Il précise par ailleurs qu' « *En ce qui concerne la conservation des données au sein du système EXABEAM, une fois communiquées au système EXABEAM, les informations historiques des alertes sont activement utilisées pour développer des profils d'utilisation pour des groupes ou des individus* ».

Le responsable de traitement explique enfin que « *Les données sont constamment rafraîchies avec de nouvelles données, les plus anciennes étant écrasées de manière sécurisée. Par conséquent, les données d'EXABEAM ne sont conservées que le temps de leur utilisation active, puis elles sont écrasées et supprimées* ».

La Commission constate que « *Les données ne seront ainsi pas conservées pendant une période supérieure à 12 mois après la fin de leur utilisation active par EXABEAM* ».

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 ;

- la réponse à ce droit d'accès doit s'exercer dans le mois suivant la réception de la demande ;

- 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 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 de ce qui précède,**

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par Barclays Execution Services Limited, représentée en Principauté par Barclays Bank PLC (succursale de Monaco) du traitement automatisé d'informations nominatives ayant pour finalité « *Mise en place d'un dispositif de surveillance, de détection et d'alerte des menaces internes à la cybersécurité de Barclays, dénommé EXABEAM* ».**

Le Président

Guy MAGNAN