Délibération n° 2023-189 du 20 décembre 2023

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 supervision de la messagerie professionnelle à des fins de surveillance* »

présentée par la Barclays Bank PLC (succursale de Monaco)

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° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, 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 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 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° 2015-111 du 18 novembre 2015 de la Commission de Contrôle des Informations Nominatives du 16 juillet 2012 portant recommandation sur les traitements automatisés d'informations nominatives ayant pour finalité « *Gestion de la messagerie électronique utilisée à des fins de surveillance ou de contrôle* » ;

Vu la délibération n° 2018-053 du 18 avril 2018 de la Commission de Contrôle des Informations Nominatives ayant pour finalité « *Gestion et supervision de la messagerie*

professionnelle à des fins de surveillance » présenté par Barclays Bank PLC (succursale de Monaco) ;

Vu la demande d'autorisation modificative déposée par la Barclays Bank PLC (succursale de Monaco) le 22 août 2023 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion et supervision de la messagerie professionnelle à des fins de surveillance* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 20 octobre 2023, 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 décembre 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Barclays Bank PLC (succursale de Monaco) représente à Monaco la Barclays Bank PLC, le responsable de traitement, sis à Londres au Royaume Uni. Elle a pour objet social « *la réalisation de toutes opérations de banque et connexes, telles que définies par la Loi bancaire* ».

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 supervision de la messagerie professionnelle à des fins de surveillance* », objet de la délibération n° 2018-053 du 18 avril 2018.

La Barclays Bank PLC (succursale de Monaco) 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 de prendre en compte l'utilisation d'un nouveau DLP (Data Loss Prevention) situé au Royaume-Uni, en plus de celui situé à Monaco.

La finalité, les fonctionnalités la justification, les destinataires, l'information des personnes concernées, et la durée de conservation sont en revanche inchangés.

I. Sur les informations nominatives traitées

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

- **Informations traitées par la messagerie électronique :**

- identité : nom, prénom, identifiant ;
- messages : contenu, objet, dossiers de classement ou d'archivage ;
- gestion des contacts : nom, prénom, raison sociale ;
- informations temporelles : date et heure de réception/envoi de messages ;
- données d'identification électronique : adresse de messagerie électronique ;
- logs d'accès : logs de connexion des personnels habilités à avoir accès au traitement ;
- fichiers journaux : nombre de messages entrants et sortants, de messages nettoyés, de spams ; volume, format, pièces jointes, noms de domaine expéditeurs de messages ;
- habilitations : identité des personnes habilitées à avoir accès à la messagerie, type de droits conférés, historisation des habilitations.

Les informations relatives à l'identité ont pour origine le traitement ayant pour finalité « *Gestion du personnel* ».

Les informations relatives aux messages et à la gestion des contacts ont pour origine l'utilisateur de la messagerie.

Enfin, les informations relatives aux informations temporelles, aux données d'identification électronique, aux logs d'accès, aux fichiers journaux et aux habilitations ont pour origine le compte de messagerie.

- **Informations traitées par le logiciel de prévention contre la fuite des données (DLP Monaco) :**

- identité : identifiant de l'utilisateur, données clients utilisées pour alimenter le logiciel de scanning (nom, prénom, email, adresse) ;
- messages : contenu, objet ;
- informations temporelles : date et heure de l'alerte, date et heure des actions effectuées par les équipes dans le cadre du traitement des incidents ;
- données d'identification électronique : adresse de messagerie électronique de l'expéditeur et du destinataire, numéro de poste de l'expéditeur ;
- logs d'accès : logs de connexion au système, logs d'accès et de modification des données dans le cadre de l'utilisation de la plateforme technique.

Les informations relatives à l'identité ont pour origine le système de messagerie et le traitement ayant pour finalité « *Tenue de la clientèle* ».

Les informations relatives aux messages, aux informations temporelles, aux données d'identification électronique et aux logs d'accès ont pour origine le système de messagerie.

- **Informations traitées par le logiciel de prévention contre la fuite des données (DLP Royaume-Uni) :**

- identité : identifiant de l'utilisateur ;
- messages : contenu, objet ;
- informations temporelles : date et heure de l'alerte, date et heure des actions effectuées par les équipes dans le cadre du traitement des incidents ;
- données d'identification électronique : adresse de messagerie électronique de l'expéditeur et du destinataire, numéro de poste de l'expéditeur ;
- logs d'accès : logs de connexion au système, logs d'accès et de modification des données dans le cadre de l'utilisation de la plateforme technique.

Les informations ont toutes pour origine le système de messagerie.

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.

II. Sur l'information préalable des personnes concernées

Le responsable de traitement indique que l'information préalable des personnes concernées est effectuée par le biais d'un document spécifique, d'une mention clause ou clause particulière intégrée dans un document remis à l'intéressé et d'une procédure interne accessible en intranet.

Cette information est inchangée.

Ces documents n'ayant pas été joints ni à la demande initiale ni à la présente demande modificative, la Commission rappelle donc, conformément à sa délibération n° 2018-053 du 18 avril 2018 que lesdits documents doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Elle recommande par ailleurs au responsable de traitement ou à son représentant, si cela n'est déjà fait, de mettre en place une charte d'usage des outils de communication électronique, venant préciser, notamment :

- les procédures de contrôle et de surveillance mises en œuvre ;
- la ou les finalités de ces procédures ;
- les personnes habilitées à avoir accès au traitement ;
- la durée de conservation des données collectées ;
- les modalités d'exercice par les personnes de leurs droits d'accès à leurs données.

En outre, afin de limiter l'atteinte portée à la vie privée des utilisateurs, la Commission recommande également au responsable de traitement de définir dans la charte susmentionnée, la procédure d'accès à la messagerie électronique par les personnes habilitées, en cas d'absence temporaire ou définitive de l'utilisateur, et ce afin d'assurer la continuité des activités.

Elle rappelle enfin que cette information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, et notamment les tiers extérieurs.

A cet égard, la Commission recommande l'insertion d'une mention d'information au bas de tout message électronique sortant afin d'informer lesdits tiers de la finalité du traitement, ainsi que de leurs droits.

III. Sur les personnes ayant accès au traitement

Les personnes habilitées à avoir accès au traitement sont désormais les suivantes :

Dans le cadre de la messagerie (Monaco) :

- les utilisateurs de la messagerie: en inscription, consultation et modification dans le cadre de l'utilisation de leur messagerie ;
- le Service Technology : tous droits dans le strict cadre de l'accomplissement de leurs missions de contrôles techniques et de maintenance système ;
- les Services d'audit et de contrôle : consultation dans le strict cadre de l'accomplissement de leur mission de contrôle.

Dans le cadre de la prévention contre la fuite de données (Monaco) :

- les Services d'audit et de contrôle : consultation des incidents ;
- le Service Cyber & Information Security : consultation et traitement des incidents, paramétrage du logiciel ;
- les Services Compliance et Control Delivery : consultation et traitement des incidents uniquement en cas d'absence et d'indisponibilité du service Cyber & Information Security afin d'assurer et de garantir la continuité du service ;
- le Service Technology : maintenance (pas d'accès aux données).

Dans le cadre de la prévention contre la fuite de données (Royaume-Uni) :

- les Services d'audit et de contrôle (Royaume-Uni et Suisse) : consultation des incidents ;

- le Service Cyber Operations UK : consultation et traitement des incidents, paramétrage du logiciel ;
- les services « *Security Engineering & Tech Services* » : maintenance (pas d'accès aux données).

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 rapprochements et interconnexions avec d'autres traitements

La Commission constate que le traitement 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* » a désormais été légalement mis en œuvre.

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 que la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception, conformément à la délibération n° 2015-111 du 18 novembre 2015.

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

VI. Sur la durée de conservation

Les informations collectées dans le cadre de la prévention des fuites de données sont conservées 1 an.

La Commission considère que cette durée est conforme aux exigences légales.

Elle note par ailleurs que les habilitations sont conservées également 1 an.

A cet égard, la Commission rappelle que les informations ne peuvent être conservées que pour une durée n'excédant pas celle nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées.

Aussi, elle fixe la durée des habilitations au temps de l'affectation.

Les autres durées de conservation sont inchangées par rapport à la demande initiale.

La Commission relève ainsi que les informations liées à l'identité, aux messages et aux données d'identification électronique sont toujours conservées 10 ans.

En conséquence, la Commission fixe, conformément à sa délibération n° 2015 -111 du 18 novembre 2015 et à sa délibération n° 2018-053 du 18 avril 2018, la durée de conservation des données liées à l'identité et des données d'identification électronique à 3 mois maximum après le départ de l'utilisateur.

Par ailleurs, s'agissant du contenu des messages émis et reçus, la Commission demande qu'une politique d'archivage soit mise en place jusqu'à ce que la conservation desdits messages ne soit plus nécessaire.

Après en avoir délibéré, la Commission :

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 ;

- l'information des personnes concernées doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, et notamment les tiers extérieurs ;

- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et 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 doit être chiffrée sur son support de réception.

Recommande :

- l'insertion d'une mention d'information au bas de tout message électronique sortant afin d'informer les tiers extérieurs de la finalité du traitement, ainsi que de leurs droits ;

- la mise en place d'une charte d'usage des outils de communication électronique.

Fixe les durées de conservation de données suivantes :

- s'agissant des habilitations, au temps de l'affectation ;

- s'agissant des données liées à l'identité et des données d'identification électroniques à 3 mois maximum après le départ de l'utilisateur.

Demande, s'agissant du contenu des messages émis et reçus, qu'une politique d'archivage soit mise en place jusqu'à ce que la conservation desdits messages ne soit plus nécessaire.

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 Barclays Bank (succursale de Monaco) de la modification du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance* ».**

Le Président

Guy MAGNAN