Délibération n° 2024-150 du 26 juillet 2024

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 supervision de la messagerie instantanée à des fins de surveillance et de contrôle* »

présenté par Union Bancaire Privée - 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 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, et son protocole additionnel ;

Vu le Code pénal monégasque ;

Vu le Code monétaire et financier français ;

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 ;

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, susvisée ;

Vu l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 fixant les modalités d'application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, susvisée ;

Vu l'Ordonnance Souveraine n° 3.559 du 5 décembre 2011 rendant exécutoire l'Accord monétaire entre l'Union européenne et la Principauté de Monaco ;

Vu l'Arrêté français du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution ;

Vu la demande d'autorisation déposée par la société Union Bancaire Privée (Monaco), le 15 avril 2024, concernant la mise en œuvre d'un traitement automatisé d'informations

nominatives ayant pour finalité « *Permettre la collaboration interne par messagerie instantanée avec un contrôle DLP »* ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 14 juin 2024, conformément à l'article 11-1 de la Loi n° 1.165, susmentionnée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 26 juillet 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

L'Union Bancaire Privée (UBP) est la succursale à Monaco de UBP SA, établissement bancaire suisse (Genève), immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 14S06257, qui a pour activité « *la réalisation de toutes opérations de banque ou connexes telles que définies par la loi bancaire applicable (…)* ».

Le responsable de traitement souhaite *« favoriser et faciliter les interactions entre collaborateurs »* en mettant à leur disposition un outil de messagerie instantanée *« accessible depuis leur poste de travail ou leur téléphone mobile professionnel ».*

Afin de prévenir la fuite de données confidentielles ou sensibles, susceptible d'intervenir dans le cadre de l'utilisation de ce service de messagerie instantanée, le responsable de traitement souhaite également déployer un outil de prévention des fuites de données ou Data Leak Prevention (DLP).

Le traitement objet de la présente demande étant mis en *œuvre « à des fins de surveillance »* il est donc soumis au régime de l'autorisation conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Permettre la collaboration interne par messagerie instantanée avec un contrôle DLP* ».

Les personnes concernées sont les salariés ainsi que les collaborateurs externes disposant d'un compte UBP.

Les fonctionnalités du traitement sont les suivantes :

- envoi de messages à un ou plusieurs destinataires ;
- capacité pour l'utilisateur de supprimer ou modifier ses messages instantanés, tout en conservant un enregistrement de ces messages dans le système ;
- partage de textes, de liens ou d'images par copier-coller dans les messages instantanés ;
- stockage et rétention des données dans les datacenters du prestataire d'hébergement en Suisse pour garantir la sécurité et la conformité ;
- filtrage des messages *via* un outil de prévention de la fuite de données (DLP) pour interdire le partage de certaines informations dans les discussions instantanées.

La Commission constate que le traitement permet également la constitution de preuve en cas de litiges.

La Commission rappelle toutefois que tout traitement d'informations nominatives doit avoir une finalité « *déterminée, explicite et légitime* », aux termes de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

Aussi, en l'espèce, elle considère que la finalité du traitement doit être plus explicite pour les personnes concernées en indiquant que le responsable de traitement supervise l'utilisation faite par les collaborateurs de la messagerie instantanée à des fins de surveillance et de contrôle.

Par conséquent, la Commission modifie la finalité comme suit : « *Gestion et supervision de la messagerie instantanée à des fins de surveillance et de contrôle* ».

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le présent traitement est justifié par le consentement de la personne concernée ainsi que par la réalisation d'un intérêt légitime qu'il poursuit sans que ne soient méconnus ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

S'agissant du consentement de la personne concernée, le responsable de traitement précise que les collaborateurs de la Banque doivent avant toute utilisation du service procéder à l'acceptation des Conditions d'Utilisation.

A ce sujet, la Commission considère que ce traitement ne peut être fondé sur le consentement de la personne concernée qui ne peut être librement donné dans la présente situation de subordination.

En ce qui concerne la réalisation d'un intérêt légitime, le responsable de traitement indique que *« l'utilisation d'outils de collaboration/communication vise à favoriser et faciliter les interactions entre les collaborateurs d'UBP ».* La Commission en prend acte.

En outre, la Commission observe qu'il incombe aux professionnels visés de respecter le secret professionnel auquel ils sont liés aux termes de l'article 308 du Code pénal, et le secret bancaire, qui est régi à Monaco par l'article L. 511-33 du Code monétaire et financier français.

De surcroît, elle relève que l'Arrêté français du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution, dispose à l'article 270-3 *« les entreprises assujetties établissent par écrit une politique de sécurité du système d'information qui détermine les principes mis en œuvre pour protéger la confidentialité, l'intégrité et la disponibilité de leurs informations et des données de leurs clients, de leurs actifs et services informatiques. (…) En application de leur politique de sécurité du système d'information, les entreprises assujetties formalisent et mettent en œuvre des mesures de sécurité physique et logique adaptées à la sensibilité des locaux, des actifs et services informatiques, ainsi que des données* ».

La Commission relève par ailleurs que le responsable de traitement a joint au dossier un document intitulé *« Sécurité du traitement soumis à demande d'autorisation »* qui décrit le fonctionnement de l'outil DLP.

Ce dernier permet d'analyser/ inspecter les données transmises *via* la messagerie instantanée au regard des données de référence insérées dans l'outil.

Le responsable de traitement précise que dans l'hypothèse où l'outil DLP détecte une infraction, c'est-à-dire si des données confidentielles ou sensibles ont été saisies /transmises *via* la messagerie instantanée, une alerte est générée. Il indique à cet égard que *« selon la criticité de l'alerte basée sur des seuils de détection prédéfinis par l'équipe sécurité d'UBP, l'alerte est classée comme étant en Audit ou bien en mode Bloquant ».*

A cet égard, le responsable de traitement précise que lorsqu'une alerte est générée, et qu'elle est classée par l'outil en « *mode audit* », le message est transmis à son destinataire. Dans l'hypothèse où l'alerte est classée « *en mode bloquant* », le message est bloqué sans envoi au destinataire. Dans ce dernier cas, le responsable de traitement indique qu'une fenêtre apparait sur l'écran du salarié à l'origine de l'alerte, l'informant du blocage de son envoi.

La Commission appréciera le caractère proportionné de la mise en œuvre de cet outil au regard de l'information préalable fournie aux personnes concernées, au point IV de la présente délibération.

Enfin, la Commission rappelle que le traitement, dont la finalité est limitée à la prévention des fuites de données confidentielles, ne saurait conduire à une surveillance permanente et inopportune des salariés, et ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165.

Le responsable de traitement précise à ce sujet que l'alerte générée par l'outil DLP déployé fera dans tous les cas l'objet d'une analyse humaine.

La Commission en prend acte et considère 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 traitées

Les informations nominatives traitées sont :

- identité : nom, prénom, langue de l'utilisateur, identifiant de l'utilisateur, civilité ;
- coordonnées : adresse email professionnelle, adresse de redirection de messagerie, numéro de téléphone professionnel (personnel si renseigné) ;
- formation-diplômes / vie professionnelle : service/ département, ville/ pays de rattachement, fonction, statut professionnel, organigramme (identité de l'assistant et/ ou du manager) ;
- données d'identification électronique : statut du compte, paramètre des profils utilisateurs, certificats, identifiant et mot de passe ;
- données de connexion : logs de connexion à l'outil de messagerie instantanée ainsi qu'à l'outil DLP;
- informations temporelles : date et heure d'envoi des messages instantanés ;
- données de contenu : contenu des messages instantanés ;
- alertes : réception des alertes automatiques DLP.

Les informations relatives à l'identité, à la vie professionnelle ainsi que les coordonnées proviennent du traitement, légalement mis en œuvre ayant pour finalité *« Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au système d'information »*.

Les autres informations sont générées par le système.

La Commission considère que les informations traitées 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, modifiée.

IV. Sur les droits des personnes concernées

- ***Sur l'information des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est assurée au moyen d'un document spécifique.

A cet égard, le responsable de traitement à joint au dossier les Conditions d'Utilisation de la messagerie instantanée. Ledit document informe les salariés que l'outil mis à leur disposition est destiné *« à un usage professionnel uniquement et peut occasionnellement être utilisé pour communiquer avec des clients externes, mais ne doit pas être utilisé pour partager des données personnelles, des informations sur les clients ou toute autre information sensible ».*

Cependant, les Conditions d'Utilisation n'informent pas les collaborateurs de l'existence d'une surveillance par un outil DLP et qu'en cas de transmission d'informations confidentielles ou sensibles une alerte est générée et qu'elle sera analysée par le service informatique. Enfin, le document n'informe pas les personnes concernées de leurs droits.

Par complément d'information, le responsable de traitement indique que l'information des collaborateurs est également assurée par des directives Groupe. Ainsi il a transmis deux directives intitulées « *Technological Security* » et « *Monitoring Regulation* » rédigées à l'attention des collaborateurs de la Banque.

A titre liminaire, la Commission relève que lesdits documents sont disponibles uniquement en anglais et demande au responsable de traitement de mettre à disposition de ses collaborateurs une version française de celles-ci.

En outre, à l'analyse de la directive « *Technological Security* », la Commission relève qu'un paragraphe porte sur l'utilisation de la messagerie instantanée sans toutefois lister les comportements attendus concernant l'utilisation de celle-ci. En effet, il est simplement indiqué que les collaborateurs doivent uniquement utiliser des services de messagerie instantanée approuvés par la Banque ou mis à disposition par des tiers ayant conclu un contrat avec elle.

Par ailleurs, le document prévoit un paragraphe intitulé « *Supervision et contrôle* » indiquant que le responsable de traitement opère une surveillance du respect des règles prévues dans la directive et que tout manquement à celles-ci peut faire l'objet de mesures disciplinaires.

En outre, la Commission relève qu'un paragraphe similaire est présent dans la directive « *Monitoring Regulation* ». Celui-ci reprend sensiblement les mêmes informations que le paragraphe précédemment évoqué. Toutefois, la Commission relève que cette directive indique que des outils de prévention des fuites de données peuvent être déployés sur les postes de travail des collaborateurs et que dans l'hypothèse où ces derniers souhaitent avoir plus d'informations ils doivent contacter le responsable local en matière de sécurité notamment afin de savoir si un tel outil est effectivement déployé.

A cet égard, la Commission considère que le collaborateur doit être informé préalablement à la mise en œuvre de tout traitement et ne doit pas avoir une démarche proactive pour connaître s'il est concerné ou non par un outil de contrôle.

Enfin, le responsable de traitement a également joint au dossier un document ayant vocation à informer les collaborateurs de la liste des traitements les concernant mis en œuvre par la Banque. Il précise que ledit document fait l'objet d'un affichage et qu'il a également prévu de le transmettre par email à tous les collaborateurs.

A cet égard, la Commission considère que la transmission de la liste des traitements par email aux collaborateurs permet de s'assurer d'une information individuelle des personnes concernées. Elle rappelle que le responsable de traitement est tenu d'avertir les personnes concernées dès lors que cette liste fait l'objet d'une mise à jour.

Au vu de ce qui précède, la Commission constate que l'information fournie aux salariés ne leur permet pas de comprendre et d'anticiper les comportements attendus par le responsable de traitement concernant l'utilisation de la messagerie instantanée mise à leur disposition. Elle considère par ailleurs, que l'information communiquée aux collaborateurs doit se faire dans un document unique.

A ce titre, elle demande que l'information de l'ensemble des personnes concernées soit adaptée et propre à l'outil mis à leur disposition, complète, préalable et conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

- ***Sur l'exercice du droit d'accès des personnes concernées***

Le responsable de traitement indique que le droit d'accès s'exerce par voie postale auprès du Chief Operating Officer.

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.

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, modifiée.

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

Les personnes ayant accès au traitement sont :

- les équipes juridique, conformité et contrôle interne : en consultation *via* une demande aux administrateurs UBP, sous supervision du DPO ;
- les administrateurs IT de UBP impliqués dans le traitement des données nécessaires à la fourniture des services : tous les droits ;
- l'équipe de sécurité de UBP : en consultation ;
- l'équipé SOC (Security Operation Center) de UBP : uniquement pour la consultation des logs d'audit transmis au SOC ;
- le prestataire et ses sous-traitants dans le traitement des données nécessaires à la fourniture des services : tous les droits (sous autorisation d'un administrateur UBP au travers du « *customer lockbox* »).

Par complément d'information, le responsable de traitement indique que les accès du prestataire et de ses sous-traitants sont opérés depuis *« des pays disposant d'un niveau de*

protection considéré comme adéquat en matière de données personnelles, par la Commission ». Cependant, il précise que dans le cadre du support 24/7, les accès peuvent avoir lieu depuis des pays ne disposant pas d'un niveau de protection adéquat au sens de la législation monégasque. Dans ce cas le responsable de traitement précise qu'il est *« notifié de ce transfert et qu'il peut refuser ».* A cet égard, si l'hypothèse qu'une telle situation se présente n'est pas écartée par le responsable de traitement, la Commission demande à ce qu'une demande d'autorisation de transfert lui soit soumise.

En outre, le responsable de traitement indique que les informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires légalement habilités.

A cet égard, la Commission rappelle que les Autorités administratives et judiciaires ne peuvent avoir accès aux informations objet du traitement que dans le strict cadre de leurs missions légalement conférées.

La Commission considère que ces accès et transmissions sont conformes aux exigences légales et sont justifiés au regard de la finalité du traitement.

VI. Sur les interconnexions et rapprochements avec d'autres traitements

Le responsable de traitement indique que le présent traitement est interconnecté avec le traitement ayant pour finalité « *Gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au système d'information* », légalement mis en œuvre.

Il indique également que le traitement fait l'objet d'un rapprochement avec le traitement, légalement mis en œuvre suivant *« Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle »*.

La Commission considère que cette interconnexion et ce rapprochement sont conformes aux exigences légales.

En outre, eu égard aux éléments procéduraux communiquées dans le dossier, la Commission constate que ce traitement peut être rapproché avec le traitement ayant pour finalité *« Gestion du contentieux ».*

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.

Cependant, la Commission rappelle que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

Elle rappelle par ailleurs que les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.

En outre, la Commission rappelle que les ports non utilisés doivent être désactivés et que 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 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.

VIII. Sur la durée de conservation

Le responsable de traitement indique que les informations relatives à l'identité des salariés, à leur vie professionnelle, leurs coordonnées ainsi que les données d'identification électronique sont conservées « *par défaut, 10 ans après la suppression du compte, ou plus court sur demande préalable de la personne qui ne contrevient pas à une obligation légale ou réglementaire* ».

A cet égard, la Commission considère que les informations des comptes des collaborateurs de l'outil de messagerie instantanée doivent être supprimés 3 mois après leur départ. Elle fixe en conséquence la durée de conservation.

S'agissant des données d'identification électronique la Commission fixe leur conservation au temps d'habilitation de la personne concernée.

En outre, le responsable de traitement précise que les informations relatives aux alertes générées par l'outil DLP sont conservées 12 mois. La Commission en prend acte.

Enfin, le responsable de traitement indique que les logs de connexion à l'outil de messagerie instantanée sont conservés 1 an. Par ailleurs, le responsable de traitement indique que les logs de connexion à l'outil DLP sont conservés sans limitation de temps à des fins de préservation de l'intégrité du système. A cet égard, la Commission estime qu'il n'est pas possible de disposer d'informations nominative sans limitation de durée. Aussi, elle fixe la durée de conservation desdits logs à 1 an et invite le responsable de traitement à lui revenir pour formuler toute observation sur ce point.

Les informations temporelles ainsi que les données relatives au contenu des messages instantanés sont conservées 10 ans à compter de leur émission. A cet égard, la Commission relève que l'entité Suisse agit en l'espèce en tant que responsable de traitement. Les durées de conservation indiquées par le responsable de traitement en application de son droit interne, qui ne contrevient pas en l'espèce à l'ordre public monégasque, peuvent être acceptées.

Après en avoir délibéré, la Commission :

Modifie la finalité comme suit *: « Gestion et supervision de la messagerie instantanée à des fins de surveillance et de contrôle ».*

Demande que :

- l'information de l'ensemble des personnes concernées soit disponible dans un document unique rédigé en langue française, adaptée et propre à l'outil de messagerie instantanée mis à leur disposition, complète, préalable et conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- qu'une demande d'autorisation soit soumise à la Commission dans l'hypothèse où le prestataire dispose d'un accès depuis un pays ne disposant pas d'un niveau de protection adéquat.

Rappelle que :

- le présent traitement ne doit pas conduire à une surveillance permanente et inopportune des salariés ;

- le présent traitement ne doit pas méconnaître les dispositions de l'article 14-1 de la Loi n° 1.165 du 23 décembre 1993 ;

- la réponse au droit d'accès doit intervenir dans le mois suivant la réception de la demande ;

- la liste des personnes ayant accès au traitement doit être tenue à jour et doit lui être communiquée à première réquisition ;

- le responsable de traitement est tenu d'avertir les collaborateurs dès lors que la liste des traitements les concernant fait l'objet d'une mise à jour ;

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

- 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 ;

- les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.

Fixe la durée de conservation :

- des informations relatives au compte de messagerie instantanée à 3 mois après le départ du collaborateur ;

- des données d'identification électronique au temps d'habilitation de la personne concernée ;

- des logs de connexion à l'outil DLP à 1 an et invite le responsable de traitement à lui revenir pour formuler toute observation sur ce point.

A la condition de la prise en compte des éléments qui précèdent,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre, par l'Union Bancaire Privée, du traitement automatisé d'informations nominatives ayant pour finalité *« Gestion et supervision de la messagerie instantanée à des fins de surveillance et de contrôle ».***

Le Président

Robert CHANAS