Délibération n° 2024-149 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

« Prévention des fuites de données confidentielles relatives à l'utilisation d'Internet par les salariés »

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 11 avril 2024, concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Supervision des Téléchargements vers les Services Web à des fins de Surveillance et de Contrôle* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 10 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

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 (…) ».*

Afin de prévenir et de remédier à la perte et au vol de données confidentielles, l'Union Bancaire Privée (Monaco) souhaite mettre en place un système de surveillance de toutes les données en texte libre ou document téléchargé vers des services web avec la mise en place d'une procédure de contrôle graduée.

A ce titre, en application de l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993, modifiée, relatif à la mise en œuvre de traitements automatisés d'informations nominatives « *à des fins de surveillance* », l'Union Bancaire Privée (Monaco), soumet la présente demande d'autorisation concernant le traitement ayant pour finalité « *Supervision des Téléchargements vers les Services Web à des fins de Surveillance et de Contrôle ».*

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Supervision des Téléchargements vers les Services Web à des fins de Surveillance et de Contrôle* ».

Il est dénommé « *DLP WEB* ».

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

Les fonctionnalités du traitement sont les suivantes :

- la mise en place d'une procédure de contrôle graduée ;
- la surveillance de toutes les données en texte libre ou document téléchargé vers des services web.

A cet égard, le responsable de traitement indique que « *l'application DLP protège les données en les comparant à un ensemble de politiques et de règles. En cas de violation des règles, un incident est généré dans l'interface de gestion qui est ensuite géré en conséquence par un responsable DLP approprié ».* L'analyse des informations sortantes sur les services web s'effectue au regard de données de référence insérées dans l'outil.

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 l'outil DLP permet de surveiller l'utilisation d'Internet par les salariés.

Par conséquent, la Commission modifie la finalité comme suit : « *Prévention des fuites de données confidentielles relative à l'utilisation d'Internet par les salariés* ».

II. Sur la licéité et la justification du traitement

Le présent traitement est justifié par l'existence d'une obligation légale à laquelle est soumis le responsable de traitement.

A cet égard, 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 ».*

A titre liminaire, 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.

Par ailleurs, le responsable de traitement indique qu'il est dans son intérêt d'assurer :

- *« la protection de la banque contre tout acte susceptible d'engager sa responsabilité civile ou pénale de la Banque ou de porter préjudice à cette dernière ;*
- *la prévention de tous faits illicites, notamment la fuite de tous documents et/ou informations dont la Banque est dépositaire ;*
- *le contrôle du respect des règles internes d'usages des outils de communication électronique ».*

De plus, les documents mis à la disposition des salariés, dont les deux directives du groupe intitulées *« Monitoring Regulation* » et « *Technological Security »,* les informent de l'existence de l'analyse de flux web, des modalités de sorties de documents de la Banque, ainsi que de l'usage attendu d'Internet. La Commission appréciera le caractère proportionné

de la mise en œuvre du contrôle web au regard de l'information préalable de la personne concernée, au point IV de la présente délibération.

Par ailleurs, le responsable de traitement indique que *« le flux HTTPS est intercepté par défaut sauf pour une liste de domaines revus par la sécurité pour des raisons d'incompatibilité technique avec le service lié la plupart du temps ».*

Par complément d'information, le responsable de traitement indique que pour l'outil DLP déployé *« le processus d'analyse des alertes pour le flux http/https est identique à celui des e-mails. Seule différence est que pour le flux http/https, il n'est pas possible de mettre en quarantaine. Le blocage est définitif ».*

Sous ces réserves, la Commission 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 :

- caractéristiques financières : numéro IBAN (Pattern), numéro Carte Crédit (Pattern) ;
- données d'identification électronique : adresse de messagerie électronique ;
- informations temporelles : identifiants de connexion, logs de connexion des personnels habilités à avoir accès au traitement ;
- gestion des alertes : réception des alertes automatiques ;
- autres : nom du fichier, document attaché, URL.

Le responsable de traitement indique que les informations relatives aux caractéristiques financières proviennent du traitement légalement mis en œuvre *« Tenue des comptes de la clientèle et le traitement des informations s'y rattachant ».*

Par ailleurs, les informations relatives aux données d'identification électronique ont pour origine le compte de messagerie pour les employés et le traitement légalement mis en œuvre *« Tenue des comptes de la clientèle et le traitement des informations s'y rattachant ».*

Enfin, 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, ainsi que d'un affichage.

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.

La directive « *Monitoring Regulation* », informe également les personnes concernées qu'elles doivent éviter d'utiliser leur adresse e-mail UBP lors de leur inscription sur des sites Web tiers, afin de minimiser l'exposition aux attaques de phishing sauf lorsque cela est strictement nécessaire à des fins professionnelles conformément à la description de leur poste.

En outre, ladite directive informe les personnes concernées qu'UBP dispose du droit de prendre des mesures disciplinaires en fonction de la gravité de l'abus constaté et de sa récidive, à l'encontre du collaborateur fautif si elle détecte un abus lié à l'utilisation des systèmes d'information et de communication de la banque.

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 de la directive « *Monitoring Regulation* » 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.

Par ailleurs, le responsable de traitement a également joint au dossier un autre document d'information préalable des salariés intitulé « *Déclaration de confidentialité pour les employés, les consultants et les mandataires* » mis à disposition sur l'Intranet. Le responsable de traitement y indique que ces derniers peuvent, sur simple demande par voie postale, obtenir la copie des informations personnelles détenues par la Banque.

Ledit document informe les personnes concernées des droits d'accès, de rectification, d'effacement et de limitation, dont ils disposent dans le cadre des traitements mis en œuvre par le responsable de traitement ainsi que des modalités d'exercice de ces droits.

De plus, le responsable de traitement indique également dans un document à usage interne joint en annexe, qu'il tient une liste des traitements automatisés mis en œuvre. 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 des téléchargements vers les services web mis à leur disposition. Elle considère par ailleurs, que l'information communiquée aux collaborateurs doit se faire dans un document unique disponible également en langue française.

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.

S'agissant de l'exercice du droit d'accès, la Commission rappelle que la réponse à ce droit d'accès doit intervenir dans le mois suivant la réception de la demande.

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 personnes ayant accès au traitement

Les personnes habilitées à avoir accès au traitement sont :

- le Local Security Officer et son deputy (Security Team) : consultation des alertes, logs et traitement des alertes ;
- l'administrateur DLP du service IT Securite du Groupe (Role Super Adminstrator), trois responsables (Role Super Adminstrator) du Service security du groupe (sur sollicitation) disposent des droits d'accès à ce traitement, dans le strict cadre de l'accomplissement de leurs missions de contrôle, techniques, maintenance, configuration du système et support en cas de sollicitation du local security officer.

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 les traitements, légalement mis en œuvre, ayant pour finalité respective :

- « *Gestion tenue des comptes de la clientèle* » légalement mis en œuvre ;

- « *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 ;
- « *Gestion administrative des salariés* » légalement mis en œuvre.

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

A l'analyse du dossier, il appert un rapprochement avec le traitement de la messagerie professionnelle, légalement mis en œuvre.

La Commission prend acte que ces traitements ont été légalement mis en œuvre et considère que ces interconnexions et rapprochements sont conformes 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 par ailleurs que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception, conformément à la délibération n° 2010-13 du 3 mai 2010, et que les communications d'informations doivent être sécurisées en tenant compte de la nature des informations transmises.

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 l'ensemble des informations objet du présent traitement sont conservées pendant 12 mois à l'exception identifiants de connexion et des logs de connexion des personnels habilités à avoir accès au traitement qui ne sont pas « *effacés* ».

S'agissant des identifiants de connexion des personnels habilités la Commission considère que ceux-ci permettent aux personnes concernées de se connecter à l'outil afin d'exercer leurs missions ainsi elle fixe la durée de conservation à la période pendant laquelle la personne est habilitée à avoir accès au traitement.

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.

Enfin, elle prend acte de ces durées de conservation et elle rappelle que dans le cadre de l'ouverture d'une procédure judiciaire, toute information nécessaire, notamment à des fins probatoires, pourra être conservée jusqu'au terme de la procédure.

Sous cette réserve, la Commission considère que ces durées de conservation sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Modifie la finalité comme suit *« Prévention des fuites de données confidentielles relatives à l'utilisation d'Internet par les salariés ».*

Demande que l'information de l'ensemble des personnes concernées soit disponible dans un document unique rédigé également en langue française, adaptée et propre à l'outil de téléchargements vers les services web mis à leur disposition, complète, préalable et conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

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 ;

- les Autorités 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 identifiants de connexion des personnels habilités à la période pendant laquelle la personne est habilitée à avoir accès au traitement ;

- des logs de connexion à l'outil DLP à 1 an.

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 Privée Bancaire, du traitement automatisé d'informations nominatives ayant pour finalité *« Prévention des fuites de données confidentielles relatives à l'utilisation d'Internet par les salariés ».***

Le Président

Robert CHANAS