Délibération n° 2023-010 du 18 janvier 2023

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

« *Détection des fuites de données sur des accès internet des utilisateurs* »,

dénommé « *Contrôles des accès web externes* »,

présenté par la Société Générale Private Banking (Monaco)

Vu la Constitution du 17 décembre 1962 ;

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 Générale Private Banking (Monaco), le 28 septembre 2022, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité « *Détection des fuites de données sur des accès internet des utilisateurs* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 28 novembre 2022, 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 18 janvier 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Société Générale Private Banking (Monaco) est une société anonyme monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 96S03214, ayant pour activité « *d'effectuer (…) tant en Principauté de Monaco qu'à l'étranger : Toutes opérations de banque (…)* ».

Afin de détecter les échanges de documents internes à la Société Générale Private Banking (Monaco) vers un site extérieur (détection de la fuite de données), la Société Générale Private Banking (Monaco) souhaite mettre en place un système de surveillance avec blocage de l'envoi de données (exemple : pièces jointes), monitoring de l'activité web et une gestion des anomalies détectées.

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* », Société Générale Private Banking (Monaco) soumet la présente demande d'autorisation concernant le traitement ayant pour finalité *« Détection des fuites de données sur des accès internet des utilisateurs ».*

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Détection des fuites de données sur des accès internet des utilisateurs* ».

Les personnes concernées sont *« les collaborateurs (CDI, CDD, intérimaires), stagiaires, alternants, consultants et prestataires externes ».*

Les fonctionnalités du traitement sont les suivantes :

- blocage de l'envoi de données ;
- monitoring de l'activité web afin de déceler une fuite de donnée éventuelle ;
- gestion de l'anomalie détectée.

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

Elle considère 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 fondé sur le consentement des personnes concernées. 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.

Le responsable de traitement indique également que le traitement est justifié par la réalisation d'un intérêt légitime et ne méconnaît ni l'intérêt ni les libertés et droits fondamentaux des personnes concernées.

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, applicable à Monaco (dans les limites de l'article 275), dispose à l'article 88 que *« les entreprises assujetties déterminent le niveau de sécurité informatique jugé souhaitable par rapport aux exigences de leurs métiers. Elles veillent au niveau de sécurité retenu et à ce que leurs systèmes d'information soient adaptés »* et au c) de l'article 89 que *« l'intégrité et la confidentialité des informations sont en toutes circonstances préservées »*.

En outre, si le présent traitement permet au responsable de traitement de lire les flux http (en clair) ainsi que les flux https, la Commission constate qu'il existe une taille de fichier à compter duquel les données sont analysées, ne permettant pas de contrôler la totalité des flux https des personnes concernées.

A cet égard, 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.

De plus, les documents mis à la disposition des salariés, dont le règlement intérieur, les informent de l'existence de l'analyse des flux web, des modalités attendues de sorties de documents de la Banque, ainsi que de l'usage attendu d'Internet. Il est également indiqué que les procédures mises en place prennent en compte la protection de la vie privée et sont revues régulièrement.

En outre, dans l'hypothèse ou une alerte est générée, une analyse interne a lieu afin d'évaluer le degré de confidentialité de l'information ainsi que le contexte qui a justifié sa transmission. En tenant compte de ces données, le responsable de traitement prévoit une gradation des mesures pour les personnes concernées.

Sous la réserve évoquée au premier paragraphe du présent point, 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 :

- identité : nom, prénom, matricule ;
- adresse et coordonnées : pays ;
- formation-diplômes / vie professionnelle : type de contrat ;
- données d'identification électronique : adresse mail professionnelle, identifiant utilisateur ;
- informations temporelles : heure et jour de l'anomalie détectée ;
- autres : contenu du fichier envoyé, de l'information saisie, url du site web destinataire ;
- alerte : fichier bloqué, analyse, faux positif, cas avéré.

Ces informations sont générées par le système et par les personnes en charge du contrôle.

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 courrier adressé à l'intéressé, d'un document spécifique et d'une procédure interne accessible en Intranet.

A cet égard, le responsable de traitement a joint un document intitulé *« Modalités d'information préalable de la personne concernée »* contenant un *« Extrait de l'instruction pour l'information préalable des employés »*.

A l'examen du document, la Commission observe qu'il n'informe pas les personnes concernées conformément à l'article 14 de la Loi n° 1.165, modifiée, s'agissant notamment des catégories de destinataires et de la finalité du traitement.

Par ailleurs, le responsable de traitement indique qu'*« un répertoire des traitements exploitant des données nominatives est tenu à jour et mis à la disposition de ses salariés »* et communique le lien menant vers celui-ci.

La Commission estime qu'informer la personne concernée de la tenue d'un *« répertoire des traitements »*, qui nécessite de sa part une démarche active, n'équivaut pas au fait de l'avertir, en ce que son abstention ne doit pas la priver d'être dûment informée.

Toutefois, à l'étude du dossier la Commission constate que le responsable de traitement met à la disposition des personnes concernées les informations relatives à la finalité poursuivie par le traitement dans un courrier adressé à l'intéressé dont une copie a été jointe.

En outre, la Commission constate que l'information des personnes est également assurée dans le règlement intérieur qui prévoit que des mesures de contrôle peuvent être mises en place afin de *« filtrer les flux échangés sur Internet ».*

Au vu de ce qui précède, la Commission demande que l'information de l'ensemble des personnes concernées soit complète, préalable et conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, notamment dans le document intitulé *« Extrait de l'instruction pour l'information préalable des employés »*.

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

Le responsable de traitement indique que le droit d'accès s'exerce par courrier électronique ou par voie postale auprès du Data Protection Officer.

S'agissant de l'exercice du droit d'accès par voie électronique, la Commission rappelle qu'une procédure doit 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.

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 personnes ayant accès au traitement

Les accès sont désormais définis comme suit :

- les équipes InfoSec (DCS) Gsc localisées en Roumanie ont accès aux données en consultation afin de qualifier l'anomalie détectée (Premier niveau de contrôle) ;
- les équipes GBSU/RMP/DCS localisées à Paris ont accès en consultation, modification, inscription, suppression afin d'analyser et évaluer l'anomalie détectée (Deuxième niveau de contrôle) ;
- des équipes spécifiques de Monaco ont accès en consultation.

Il est également indiqué qu'*« en cas de nécessité, les agents des autorités de tutelle sont susceptibles, dans le cadre de leur mission, d'avoir accès sur place aux informations objets du traitement ainsi que les auditeurs / contrôleurs internes ».*

La Commission rappelle qu'en ce qui concerne les entités du groupe Société Générale qui agissent en tant que prestataire, leurs droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service et sont soumises aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993.

La Commission considère que ces accès sont justifiés.

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

Le responsable de traitement indique que le présent traitement fait l'objet d'un rapprochement avec le traitement ayant pour finalité « *Gestion administrative des salariés* », légalement mis en œuvre.

Le responsable de traitement indique également que le traitement fait l'objet d'une interconnexion avec le traitement ayant pour finalité *« Gestion et traçabilité des habilitations informatiques »*.

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

La Commission considère que cette interconnexion et ces 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 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.

Elle rappelle par ailleurs que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

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 nominatives collectées sont « *automatiquement supprimées dans l'outil au bout d'un an* ».

Le responsable de traitement précise que des *« exceptions peuvent être paramétrées si des procédures sont encore en cours au terme de cette période ».*

La Commission 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.

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

Après en avoir délibéré, la Commission :

Demande que l'information de l'ensemble des personnes concernées soit complète, préalable et conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, notamment dans le document intitulé *« Extrait de l'instruction pour l'information préalable des employés »*.

Rappelle que :

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

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

- une procédure doit 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 ;

- 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.

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 la Société Générale Private Banking (Monaco), du traitement automatisé d'informations nominatives ayant pour finalité « *Détection des fuites de données sur des accès internet des utilisateurs* ».**

Le Président

Guy MAGNAN