Délibération n° 2023-135 du 20 septembre 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 instantanée à des fins de surveillance et de contrôle et de visioconférence* »,

présentée par Edmond de Rothschild (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 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'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 déclaration ordinaire n° 2022.11075 déposée par Edmond de Rothschild (Monaco) le 30 novembre 2022, concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Services de Communication de Visioconférence et messagerie instantanée* », dont il a été délivré récépissé le 15 décembre 2022 ;

Vu la demande d'autorisation déposée par la société Edmond de Rothschild (Monaco), le 7 juin 2023, concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Services de Communication de Visioconférence / Messagerie instantané et prévention des Fuites de Données relatives* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 4 août 2023, 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 20 septembre 2023 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La société Edmond de Rothschild (Monaco) immatriculée au RCI sous le numéro 92S02760 a notamment pour activité « *[…] d'effectuer toutes opérations de banque […]* ».

Le 30 novembre 2022 cette société a déclaré à la Commission un traitement automatisé d'informations nominatives ayant pour finalité *« Services de communication de visioconférence et messagerie instantanée* ». La Commission a émis un récépissé de mise en œuvre de ce traitement le 15 décembre 2022.

Toutefois, dans sa délibération n° 2023-041 du 15 mars 2023 relative à la *« Prévention des fuites de données confidentielles relative à l'utilisation d'Internet par les salariés* » la Commission avait relevé que « *la messagerie instantanée (Teams) a fait l'objet d'une déclaration ordinaire sans mention d'une quelconque finalité de surveillance. Afin que les finalités des traitements susvisés soient « déterminées, explicites et légitimes » et que les personnes concernées soient valablement informées quant aux modalités d'utilisation attendues des outils mis à leur disposition, elle demande que ladite déclaration soit modifiée dans les meilleurs délais et soit soumise au régime de demande d'autorisation* ».

Aussi le responsable de traitement soumet le traitement de « *Services de communication de visioconférence et messagerie instantanée* » à modification et sollicite l'autorisation de la Commission afin d'y intégrer les éléments relatifs à l'outil DLP (Data Leak Prevention) destiné à prévenir les fuites de données confidentielles.

Le traitement objet de la présente demande est désormais mis en œuvre « *à des fins de surveillance* ». Ainsi il relève 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 « *Services de communication de visioconférence / messagerie instantanée et prévention des fuites de données confidentielles* ».

Les personnes concernées sont les salariés de la société, les clients et les tiers.

Les fonctionnalités du traitement sont les suivantes :

- appel en visioconférence ;
- communication par messagerie instantanée ;

- surveillance et analyse automatique des données transmises via l'outil afin de vérifier l'absence ou l'existence d'une fuite de données ;
- constitution de preuve en cas de litige.

Le responsable de traitement indique que les fonctionnalités suivantes ne sont pas déployées : le transfert de documents et l'enregistrement des visioconférences. La Commission en prend acte.

Elle 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 de l'outil de visioconférence et de messagerie instantanée par les salariés.

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

II. Sur la licéité et la justification du traitement

Le présent traitement est justifié par la réalisation d'un intérêt légitime poursuivi par le responsable de traitement et ne méconnaît ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée.

A cet égard, le responsable de traitement précise que le traitement permet *« l'amélioration de l'expérience des collaborateurs de la banque par le déploiement de nouveaux outils de communication ».*

Le responsable de traitement indique par ailleurs que le traitement est également justifié par l'existence d'une obligation légale à laquelle il est soumis.

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.

Par complément d'information, le responsable de traitement indique que l'outil DLP qui sera déployé sur la messagerie instantanée lui permet de « *filtrer la copie d'image* » et ainsi *« bloquer purement et simplement la copie d'image dans le chat* ». A cet égard, le responsable de traitement précise que le contenu (texte ou image) du copier-coller est filtré par rapport à des données de référence notamment, des mots clés, des données financières ou l'identité des interlocuteurs.

Dans l'hypothèse où l'utilisateur tente d'effectuer un copier-coller, le responsable de traitement indique qu'une fenêtre s'ouvre l'informant que le système a bloqué leur action afin d'éviter la transmission de données confidentielles qui violerait les règles de l'entreprise. La Commission en prend acte.

En outre, le responsable de traitement explique qu'une alerte est alors générée et qu'un email est envoyé au Service Informatique pour investigation. A cet égard, il indique que l'alerte passe par plusieurs niveaux de contrôle ce qui permet de garantir l'objectivité de l'analyse, afin de qualifier l'incident et de prendre des mesures adaptées.

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 des salariés ;
- adresse et coordonnées : numéro de téléphone professionnel, adresse professionnelle ;
- données d'identification électronique : adresse de messagerie électronique des salariés, clients et tiers participants à la conférence ;
- informations temporelles : identifiants de connexion et logs de connexion des personnels habilités à avoir accès au traitement ;
- messages : contenu ;
- informations temporelles : date et heure réception/ envoi de messages ;
- alertes : réception des alertes automatiques DLP.

Les informations relatives à l'identité, les coordonnées ainsi que les données d'identification électronique des salariés ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* », légalement mis en œuvre.

A l'étude du dossier, la Commission relève que les données d'identification électronique relatives aux clients et aux tiers participants aux conférences ont pour origine le traitement ayant pour finalité *« Gestion et supervision de la messagerie à des fins de surveillance et de contrôle »,* légalement mis en œuvre.

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 préalable des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est assurée au moyen d'un document spécifique, d'une mention ou clause particulière intégrée dans un document remis à l'intéressé ainsi que d'une procédure interne accessible en Intranet.

A l'examen du document joint au dossier intitulé *« Gestion des incidents relevés par l'outil DLP »*, la Commission constate qu'il ne spécifie pas qu'il s'adresse aux salariés. Les uniques destinataires mentionnés sur le document étant le Service Informatique et le COMEX.

Par ailleurs, la Commission relève que le document développe la procédure de gestion de l'alerte sans informer les personnes concernées conformément à l'article 14 de la Loi n° 1.165, modifiée, s'agissant notamment de la finalité du traitement et des droits des personnes.

En outre, le responsable de traitement a également joint un second document intitulé *« Manuel des Directives - Informations Nominatives* ». A l'examen de celui-ci, la Commission constate qu'il s'agit d'un guide reprenant les principes généraux relatifs au traitement des informations nominatives, les formalités à accomplir ainsi que les éléments à fournir à la personne concernée au titre de l'information préalable sans en faire une application à ses propres activités de traitement.

Toutefois, la Commission relève que ce document informe les personnes concernées des droits d'accès, de rectification et de suppression, 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.

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.

En toute fin, la Commission relève que le responsable de traitement indique qu'il tient « *à la disposition de ses employés la liste des traitements automatisés portant sur leurs informations nominatives, reprenant pour chaque traitement les informations citées à l'article 14 de la Loi 1.165 relative à la protection des informations nominatives* ».

Elle relève en outre que dans l'extrait des conditions générales, fourni au titre de l'information préalable des clients, le responsable de traitement indique que ces derniers peuvent, sur simple demande par voie postale, obtenir la communication de la liste complète des traitements effectués par la Banque.

Au regard de ces mentions, la Commission rappelle, d'une part, qu'informer la personne concernée de la tenue à disposition d'une liste de traitements, qui nécessite de sa part une démarche active, n'est pas équivalent au fait de l'avertir, en ce que son abstention ne doit pas la priver d'être dûment informée, et, d'autre part, qu'il appartient au responsable de traitement de s'assurer que l'information préalable est délivrée à l'ensemble des personnes concernées.

Au vu de ce qui précède, la Commission demande que l'information de l'ensemble des personnes concernées soit adaptée et propre à l'outil de messagerie instantanée, 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 pour les employés et auprès du Service Conformité pour les clients et les tiers.

A cet égard, la Commission rappelle que la réponse à ce 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

- ***Sur les accès au traitement***

Les personnes habilitées à avoir accès au traitement sont :

- les administrateurs du prestataire localisés en Europe : accès en cas de support à la demande de la Banque ;
- le RSSI et les personnes habilitées du Service Informatique en charge du traitement des DLP ont accès en consultation au portail de management des incidents DLP qui stocke l'ensemble des alertes dans le strict cadre de leurs missions de contrôle. Ce portail leur permet également de gérer les incidents. Ces personnes en charge du traitement des outils de filtrage ont donc accès aux alertes (faux positifs et alertes positives) ;
- les administrateurs système du Service Informatique Local ont accès au paramétrage de la plateforme DLP dans le strict cadre de l'accomplissement de leurs missions techniques et de maintenance système.

Le responsable de traitement précise par ailleurs que les membres du COMEX, n'ont pas accès à la plateforme DLP. Ils reçoivent un email à chaque alerte reprenant le détail de l'incident.

La Commission prend acte des précisions du responsable de traitement selon lesquelles *« une liste nominative des personnes ayant accès au traitement est tenue à jour »,* et rappelle que cette liste doit lui être communiquée à première réquisition.

Elle considère que ces accès sont justifiés.

- ***Sur les destinataires***

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires légalement habilitées.

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.

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

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

Par ailleurs, le responsable de traitement indique que le présent traitement est interconnecté avec le traitement, légalement mis en œuvre ayant pour finalité « *Gestion administrative des salariés* », nécessaire à la collecte des données d'identité des salariés et à la gestion des habilitations.

Le responsable de traitement précise en outre que le présent traitement est également interconnecté avec le traitement relatif à la « *Tenue des comptes de la clientèle* », légalement mis en œuvre, afin de fournir des informations relatives à l'identité de la clientèle.

Toutefois, à l'étude du dossier, la Commission considère que l'information relative à l'identité des clients ne provient pas du traitement *« Tenue des comptes de la clientèle »* mais d'un rapprochement entre le traitement objet de cette demande d'autorisation et le traitement ayant pour finalité « *Gestion et supervision de la messagerie à des fins de surveillance et de contrôle* », légalement mis en œuvre.

Sous cette réserve, la Commission considère que ces interconnexions et ce rapprochement 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.

Cependant, 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 relatives à l'identité des salariés, les coordonnées, les données d'identification électronique, les informations temporelles relatives à l'outil de messagerie instantanée ainsi que le contenu des messages échangés sont conservées pendant 90 jours.

Le responsable de traitement précise en outre que les logs de connexion ainsi que les informations relatives aux alertes sont conservés pendant 1 an maximum.

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.

En conséquence, elle considère que ces durées de conservation sont conformes aux exigences légales.

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 et de visioconférence ».*

Demande que l'information de l'ensemble des personnes concernées soit adaptée et propre à l'outil de messagerie instantanée, 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 ;

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

- les Autorités administratives et judiciaires ne peuvent avoir accès aux informations objet du présent traitement que dans le strict cadre des 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 Edmond de Rothschild (Monaco), de la modification du traitement automatisé d'informations nominatives ayant pour finalité** ***« Gestion et supervision de la messagerie instantanée à des fins de surveillance et de contrôle et de visioconférence ».***

Le Président

Guy MAGNAN