Délibération n° 2023-041 du 15 mars 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

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

dénommé « *Data Leak Prevention (DLP)* »,

présenté par Edmond de Rothschild (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 délibération n° 2020-011 du 15 janvier 2020 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 à des fins de surveillance et de contrôle* » présenté par Edmond de Rothschild (Monaco) ;

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* », et dont il a été délivré récépissé le 15 décembre 2022 ;

Vu la demande d'autorisation déposée par la société Edmond de Rothschild (Monaco), le 30 novembre 2022, concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Prévention des fuites de données confidentielles »* ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 30 janvier 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 15 mars 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 […]* ».

Afin de prévenir les risques inhérents à l'utilisation par les salariés, des canaux de communications électroniques (messagerie électronique, Internet, messagerie instantanée Teams) la Société Edmond de Rothschild (Monaco) souhaite mettre en place un outil DLP (Data Leak Prevention) destiné à prévenir les fuites de données confidentielles.

La Commission décide toutefois de restreindre la présente demande d'autorisation à la seule prévention des risques inhérents à l'utilisation d'Internet (upload de fichiers et saisie de données sensibles) par les salariés de la Société Edmond de Rothschild (Monaco) afin de prévenir les fuites de données confidentielles.

Elle constate en effet que la messagerie électronique du responsable de traitement, qui est soumise à une mesure de surveillance *via* un outil DLP, a déjà fait l'objet d'une formalité légale ayant conduit à son autorisation par délibération n° 2020-011 du 15 janvier 2020.

Par ailleurs, la Commission relève 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.

Dès lors, 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* », la Commission analysera la présente demande d'autorisation concernant le traitement ayant pour finalité *« Prévention des fuites de données confidentielles »* à l'aune de la seule utilisation d'Internet.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Prévention des fuites de données confidentielles* ».

Il est dénommé « *Data Leak Prevention (DLP)* ».

Les personnes concernées sont les salariés de la société.

Les fonctionnalités du traitement sont les suivantes :

- la surveillance et l'analyse automatique des documents uploadés et/ou des données sensibles saisies sur les sites Internet externes d'Edmond de Rothschild (Monaco) afin de vérifier l'absence ou l'existence d'une fuite de données ;
- la constitution de preuves en cas de litige.

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, 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 »*.

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.

En outre, le présent traitement permet au responsable de traitement de lire les flux http (en clair) ainsi que les flux https, ce qui inclut les correspondances privées ou les paiements par carte bancaire.

Par ailleurs, la Commission relève que le document joint au dossier intitulé *« Gestion des incidents relevés par l'outil DLP »* décrit le fonctionnement du DLP.

L'outil DLP du responsable de traitement permet de filtrer les noms de domaines sur lesquels les utilisateurs ont uploadé des fichiers ou saisi des données sensibles. Une analyse du contenu de ces fichiers ou de ces données est effectuée au regard des données de référence insérées dans l'outil.

De plus, dans l'hypothèse où l'outil DLP détecte une infraction, c'est-à-dire si des fichiers confidentiels ou des données sensibles ont été saisis sur des noms de domaines externes à Edmond de Rothschild (Monaco), une alerte est générée. Le responsable de traitement indique à cet égard que l'alerte passe par plusieurs niveaux de contrôle ce qui permet de garantir une certaine objectivité dans son analyse ainsi que pour la qualification finale de l'incident. En tenant compte du résultat du contrôle, le responsable de traitement prévoit de prendre des mesures adaptées pour les personnes concernées.

Par ailleurs, le responsable de traitement précise que lorsqu'une alerte est générée, le salarié à l'origine de l'alerte reçoit un email l'informant du blocage de sa recherche sur Internet.

A cet égard, 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.

Sous cette réserve, 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 ;
- formation-diplômes / vie professionnelle : département de rattachement ;
- sites internet et données filtrées : URL des sites internet sur lesquels des uploads de fichiers ou la saisie de donnés sensibles ont été constatés, le contenu du ou des fichiers uploadés et le contenu de la ou des saisies de données sensibles, la date et l'heure de l'upload ou de la saisie, l'adresse IP du poste de travail à partir duquel l'upload ou la saisie a été effectuée ;
- logs de connexions aux système DLP : identifiants de connexion et logs de connexion des personnels habilités à avoir accès au traitement ;
- alertes : réception des alertes automatiques DLP (alertes positives, faux positifs).

Les informations relatives à l'identité ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* », légalement mis en œuvre. 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'une mention ou clause particulière intégrée dans un document remis à l'intéressé, d'une procédure interne accessible en intranet ainsi que d'un courrier adressé à l'intéressé.

De plus, le responsable de traitement précise que les nouveaux arrivants sont informés de l'existence de ce traitement lors d'une formation destinée à la sensibilisation à la sécurité informatique et à la confidentialité.

Le responsable de traitement a joint au dossier un document intitulé *« Gestion des incidents relevés par l'outil DLP »*.

A l'examen du document, 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 le fonctionnement de l'outil DLP 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 *« Informations Nominatives »*.

A l'étude de ce document, la Commission constate qu'il s'agit d'un guide reprenant les définitions, les principes généraux relatifs au traitement des informations nominatives, les différentes 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.

Enfin, 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* ».

A cet égard, 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 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 d'Internet, mais également des différents outils mis à leur disposition soumis à une mesure de surveillance, dont Teams et la messagerie professionnelle précédemment autorisée.

Aussi, elle demande que l'information de l'ensemble des personnes concernées soit adaptée et propre à chacun des outils mis à leur disposition, complète, préalable et conforme à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, y compris pour la messagerie professionnelle objet de la délibération n° 2020-011 du 15 janvier 2020 qui ne contenait pas de réserves sur ce point.

- ***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.

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 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 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. Ces personnes ont également accès aux liens URL recherchés lors de la navigation Internet à l'origine de l'alerte ainsi qu'à l'élément ayant généré l'incident.

Le responsable de traitement précise par ailleurs que les membres du COMEX reçoivent un email, lorsqu'un incident est détecté par l'outil DLP, reprenant le détail de cet 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.

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

A cet égard, la Commission rappelle que les Autorités administratives et judiciaires ne peuvent avoir communication des 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 fait l'objet d'une interconnexion 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 de deux rapprochements avec les traitements, légalement mis en œuvre, ayant respectivement pour finalités *« Tenue de compte de la clientèle »* et *« Gestion de l'identification et de la vérification des personnes soumises à la Loi n° 1.362 du 03 août 2009 »*.

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 ».*

En outre, il appert de l'analyse du dossier un rapprochement avec le traitement ayant pour finalité « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance et de contrôle* » légalement mis en œuvre.

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 relatives à l'identité des salariés ainsi que leur département de rattachement sont conservées « *1 mois maximum après le départ de l'employé* ».

Par ailleurs, le responsable de traitement précise que les logs de connexion et les informations relatives aux sites internet et données filtrées sont conservés pendant 1 an.

Enfin, le responsable de traitement indique que les informations relatives aux alertes sont conservées 7 jours.

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.

De plus, elle rappelle que les emails contenant les alertes ne doivent pas conduire à allonger les durées de conservation prévues dans le présent traitement ou dans celui relatif à la gestion du contentieux.

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 relative à l'utilisation d'Internet par les salariés ».*

Demande que :

- la déclaration ordinaire n° 2022-11.075 soit modifiée dans les meilleurs délais et soit soumise au régime de demande d'autorisation ;

- l'information de l'ensemble des personnes concernées soit adaptée et propre à chacun des outils 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 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 communication des informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- les emails contenant les alertes ne doivent pas conduire à allonger les durées de conservation prévues dans le présent traitement ou dans celui relatif à la gestion du contentieux ;

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

Le Président

Guy MAGNAN