Délibération n° 2024-181 du 9 octobre 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 de la surveillance des évènements sur le Système d'Information* »

présenté par la Société Anonymes des Bains de Mer et du Cercle des Etrangers à Monaco

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention 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 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

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, modifiée, susvisée ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'autorisation déposée par la Société Anonyme des Bains de Mer et du Cercle des Etrangers à Monaco le 17 juin 2024 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion de la surveillance des évènements sur le Système d'Information* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 14 août 2024, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 9 octobre 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

La Société des Bains de Mer et du Cercle des Etrangers à Monaco (S.B.M.) est une personne morale de droit privé qui bénéficie du privilège des jeux, conformément aux dispositions de l'Ordonnance Souveraine n° 15.732 du 13 mars 2003.

Elle souhaite assurer la sécurité du système d'information au travers d'outils de collecte, de corrélation, d'analyse d'événements et d'intervention à distance afin de détecter les actions malveillantes sur le Système d'Information (SI) avant même que l'attaque ne soit réellement déclenchée.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance, il relève donc 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 « *Gestion de la surveillance des évènements sur le Système d'Information* ».

Les personnes concernées sont les collaborateurs de la S.B.M. ainsi que les collaborateurs du prestataire externe.

Enfin, les fonctionnalités de ce traitement sont les suivantes :

S'assurer de la collecte des évènements sur le SI *:*

- collecter des évènements (Logs système) provenant des équipements de la S.B.M. ainsi que leurs accès aux différentes applications ;
- gérer les remontées d'alertes sur les risques d'intrusion et les vulnérabilités.

S'assurer de l'analyse des évènements collectés :

- détecter une faille de sécurité afin d'y remédier rapidement.

S'assurer de la détection des menaces et la qualification des incidents :

- retrouver l'origine d'un incident de sécurité et le résoudre ;
- établir des alertes et/ou des rapports qui permettent de détecter tout risque de malveillance et de s'assurer de la cohérence des accès avec les habilitations délivrées ;
- identifier un accès frauduleux ;
- établir des rapports de suivi (ex : nombre d'alertes, nombre de tickets ouverts, détection des alertes, délai de résolution d'incident…) ;
- disposer d'éléments de preuve si l'incident implique un contentieux.

La Commission constate ainsi 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 justifié par le respect d'une obligation légal, notamment la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, et par « *la réalisation d'un intérêt légitime poursuivi [par lui et qui] ne méconnait ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée* ».

La Commission prend acte que « *Ce traitement n'est pas utilisé à des fins de surveillance et/ou de contrôle de manière systématique et permanente des activités des personnes physiques sur le Système d'Information* » et que « *La S.B.M. cherche uniquement à protéger le Système d'Information des attaques ou atteintes à son fonctionnement, à sa disponibilité, son intégrité, sa confidentialité (telles que mentionnées dans sa PSSI) qu'elles soient volontaires ou accidentelles, qui pourraient alors avoir des conséquences sur l'ensemble des activités des services de l'entreprise, que les données exploitées soient ou non nominatives* ».

Au vu de ce qui précède, 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 nominatives traitées

Les informations nominatives traitées sont :

- identité des collaborateurs de la S.B.M. et du prestataire externe : nom, prénom, fonction ;
- données d'identification électronique des collaborateurs ayant accès à la solution : login, mot de passe ;
- logs de connexion des collaborateurs de la S.B.M. : user ID, adresse MAC, traces d'exécution, login, date/heure de création, éléments techniques d'un terminal (poste de travail, serveurs), adresse IP du terminal ;
- logs de connexion des collaborateurs du prestataire externe au système de détection et d'analyse des menaces : identifiants utilisateur, adresse IP du terminal ;
- logs de connexion des collaborateurs du prestataire externe au système de gestion de journalisation des logs : user ID, adresse MAC, traces d'exécution, login, date/heure de création, éléments techniques d'un terminal (poste de travail, serveurs), adresse IP du terminal ;
- logs applicatifs : historique de l'activité.

Le responsable de traitement indique que les informations relatives à l'identité ont pour origine les personnes concernées.

Par ailleurs, les données d'identification électronique, les logs de connexion et les logs applicatifs ont pour origine les systèmes du présent traitement.

La Commission considère ainsi que les informations collectées 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 du 23 décembre 1993.

IV. Sur les droits des personnes concernées

➢ *Sur l'information préalable des personnes concernées*

Le responsable de traitement indique que l'information préalable s'effectue par le biais d'un document spécifique et d'une procédure interne accessible en Intranet.

Ces documents n'ayant pas été joints à la demande, la Commission rappelle que ceux-ci doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

La Commission rappelle par ailleurs que cette information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, à savoir les collaborateurs de la S.B.M. et les collaborateurs du prestataire externe.

- ***Sur l'exercice du droit d'accès, de modification et de mise à jour***

Le droit d'accès s'exerce par courrier électronique auprès du DPO.

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.

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, elle considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer en cas de doute que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, la Commission précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous cette réserve, elle constate 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 destinataires et les personnes ayant accès au traitement

- ***Sur les destinataires***

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées à la Direction de la Sûreté Publique dans le cadre de ses missions légalement conférées.

La Commission estime que la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

La Commission considère donc que ces transmissions sont conformes aux exigences légales.

- ***Sur les personnes ayant accès au traitement***

Les personnes habilitées à avoir accès au traitement sont :

- le Directeur des systèmes d'information et le Directeur de la Sécurité Numérique : consultation ;
- l'Administrateur système de la S.B.M. : consultation ;
- les collaborateurs du prestataire externe (Monaco Cyber sécurité) : consultation.

Considérant les attributions de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

En ce qui concerne le prestataire, la Commission rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

La Commission rappelle par ailleurs qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993 la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet de deux interconnexions avec les traitements ayant respectivement pour finalité « *Gestion administrative des salariés* » et « *Gestion de la messagerie professionnelle* ».

La Commission constate que ces deux traitements ont été légalement mis en œuvre et sont conformes aux exigences légales.

Elle considère par ailleurs que le traitement dont s'agit est également interconnecté avec tout autre traitement et/ou applicatif du SI collectant les évènements tels que les logs de connexion, les identifiants et adresses IP.

La Commission relève enfin à la lecture du dossier une interconnexion avec un traitement lié à la gestion du contentieux. Celui-ci n'ayant fait l'objet d'aucune formalité auprès d'elle, la Commission demande au responsable de traitement de le lui soumettre dans les plus brefs délais.

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

La Commission rappelle en outre que les communications d'information doivent être sécurisées en tenant compte de la nature des informations transmises.

Enfin, elle rappelle 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 les durées de conservation

Le responsable de traitement indique que les informations relatives à l'identité des collaborateurs sont conservées 3 mois après le départ de ceux-ci.

Les données d'identification électronique des collaborateurs sont conservées 12 mois après le départ de ceux-ci.

Concernant celles-ci, la Commission rappelle que ces informations ne peuvent être conservées sous une forme permettant l'identification de la personne concernée que pendant une

durée n'excédant pas celle nécessaire à la réalisation de la finalité pour lesquelles elles ont été collectées.

Aussi, elle fixe la durée des données d'identification électronique à la durée d'utilisation du SI.

Par ailleurs, les logs de connexion des collaborateurs de la S.B.M. sont conservés 12 mois.

Enfin, les logs de connexion des collaborateurs du prestataire externe au système de détection et d'analyse des menaces sont conservés pendant la durée du contrat + 5 ans et les logs de connexion des collaborateurs du prestataire externe au système de gestion de journalisation des logs et les logs applicatifs sont conservés pendant la durée du contrat de travail.

A cet égard, la Commission fixe la durée de conservation des logs à 3 ans maximum à compter de leur collecte.

Après en avoir délibéré, la Commission :

Considère qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer en cas de doute que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Rappelle que :

- l'information préalable des personnes concernées doit impérativement se faire conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993 ;

- l'information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, à savoir les collaborateurs de la S.B.M. et les collaborateurs du prestataire externe ;

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

- la Direction de la Sûreté Publique ne peut avoir accès aux informations objet du traitement que dans le strict cadre de ses missions légalement conférées ;

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

- 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'information doivent être sécurisées en tenant compte de la nature des informations transmises.

Demande au responsable de traitement de lui soumettre dans les plus brefs délais le traitement lié à la gestion du contentieux.

Fixe la durée de conservation :

- des données d'identification électronique à la durée d'utilisation du SI ;
- des logs de connexion à 3 ans maximum à compter de leur collecte.

A la condition de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par la Société Anonyme des Bains de Mer et du Cercle des Etrangers à Monaco du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la surveillance des évènements sur le Système d'Information* ».**

Le Président

Robert CHANAS