Délibération n° 2019-047 du 20 mars 2019

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 solution sécurisée de stockage et de partage de fichiers par des collaborateurs habilités* »

présenté par Tavira Monaco SAM

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° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

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 l'Ordonnance Souveraine n° 2.318 du 3 août 2009, modifiée, fixant les conditions d'application de la Loi n° 1.362 du 3 août 2009, 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 délibération n° 2017-206 du 20 décembre 2017 de la Commission de Contrôle des Informations Nominatives portant recommandation sur la gestion des habilitations et des accès informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au système d'information ;

Vu la demande d'autorisation déposée par Tavira Monaco SAM le 14 janvier 2019 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des Habilitations et des Accès Informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 26 mars 2019, 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 20 mars 2019 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Tavira Monaco SAM est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 09S05059 ayant entre autres pour objet « *La gestion pour le compte de tiers, de portefeuilles de valeurs mobilières ou d'instruments financiers à terme* ».

Afin d'optimiser l'accomplissement des missions de travail de son personnel et de ses prestataires, cette société souhaite fournir à ceux-ci un emplacement centralisé pour accéder à leurs fichiers et partager lesdits dossiers, grâce à une application de bureau sécurisée.

Le traitement objet de la présente demande permet de surveiller les accès au système d'information en lien avec la solution sécurisée de stockage et de partage de fichiers, 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 responsable de traitement indique que le traitement a pour finalité « *Gestion des Habilitations et des Accès Informatiques mis en œuvre à des fins de surveillance ou de contrôle des accès au Système d'Information ».*

Les personnes concernées sont tout le personnel de Tavira Monaco SAM ainsi que les prestataires, y compris les consultants externes.

Enfin, les fonctionnalités de ce traitement qui a pour objet de rassembler tous les fichiers des collaborateurs en un seul et même endroit sont les suivantes :

Dans le cadre de la gestion des habilitations *:*

- octroyer / délivrer aux utilisateurs du SI les moyens techniques et fonctionnels permettant de s'authentifier au système d'information afin de pouvoir exercer la fonction et les missions pour lesquelles ils ont été recrutés ;
- gérer les évolutions de droits, les mobilités internes et les départs ;
- mettre à jour les comptes systèmes dans le cadre de changement d'informations administratives (ex : changement de patronyme) ;
- permettre la réalisation de l'ensemble des tâches d'activation/ désactivation/suppression de comptes ;
- procéder à des revues de contrôles périodiques afin de s'assurer de la conformité des droits délivrés par rapport aux demandes et aux règles édictées en matière d'accès à l'information.

Dans le cadre de la supervision des accès aux applications :

- collecter des évènements systèmes (logs) permettant de tracer les accès des utilisateurs aux applications et données ;
- 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 ;
- établir des preuves en cas de litige avec tout utilisateur (employé, prestataire…).

Dans le cadre de la sécurité anti-virus :

- mettre en place des remontées d'alertes sur les risques d'intrusion ;
- établir des rapports (ex : audit de sécurité, détection de risques…).

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.

En l'espèce, la finalité du présent traitement doit être plus explicite c'est-à-dire être claire et précise pour les personnes concernées en indiquant que le traitement a pour vocation la gestion de la solution sécurisée qui va permettre aux collaborateurs, une fois habilités, de stocker et partager des fichiers.

Par conséquent, elle modifie la finalité comme suit : « *Gestion de la solution sécurisée de stockage et de partage de fichiers par des collaborateurs habilités* ».

II. Sur la licéité et la justification du traitement

- ***Sur la licéité***

Dans le cadre de sa recommandation n° 2017-206 du 20 décembre 2017, la Commission rappelle les conditions de licéité d'un traitement lié aux habilitations et accès informatiques, au sens de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

Elle relève notamment que la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption, et son Ordonnance Souveraine d'application impose aux sociétés de gestions telles que Tavira Monaco SAM de « *mettre en place des procédures de surveillance ou de contrôle des habilitations informatiques* » et donc de « *contrôler les accès aux applicatifs de l'entreprise, lesquels ont un impact sur la gestion des ordres* ».

La Commission considère donc que le traitement est licite au sens de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

- ***Sur la justification***

Le responsable de traitement indique que le traitement est justifié par « *le respect d'une obligation légale à laquelle est soumis le responsable de traitement ou son représentant* », 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* ».

A cet égard, la Commission observe que ce traitement permet au responsable de traitement de respecter notamment les obligations découlant de la Loi n° 1.362 du 3 août 2009.

Par ailleurs, le responsable de traitement indique que ce traitement répond à un objectif légitime essentiel puisqu'il permet :

- l'optimisation de l'accomplissement des missions de travail de ses employés ;
- la sécurité et le bon fonctionnement technique du réseau ou système informatique ;
- la préservation des intérêts économiques, commerciaux ou financiers du responsable de traitement ou de son représentant ;
- la prévention et la détection a priori et a posteriori de toute activité non-conforme ou illicite, par des utilisateurs.

La Commission considère donc que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations nominatives traitées

Les informations nominatives traitées sont :

- identité : nom et prénom de l'employé, nom, prénom et signature du supérieur pour la gestion des habilitations ;
- formation, diplômes et vie professionnelle : fonction et service de l'employé ;
- données d'identification électronique : identifiants de la personne habilitée (login et mot de passe) ;
- informations temporelles : logs, traces d'exécution, horodatage, fichiers journaux ;
- compte utilisateur : nom du compte, domaine du compte, groupe d'utilisateurs, type de droits ;
- contenus de la solution sécurisée : tous les dossiers et fichiers déposés dans la solution sécurisée.

Les informations relatives à l'identité, à la formation, aux diplômes et à la vie professionnelle ont pour origine le traitement ayant pour finalité « *Gestion administrative des salariés* ».

Par ailleurs les informations relatives aux données d'identification électronique, aux informations temporelles, au compte utilisateur et aux contenus de la solution sécurisée ont pour origine le Système d'Information.

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*

L'information préalable des personnes concernées est effectuée par le biais d'une procédure interne accessible en Intranet.

Ce document n'ayant pas été joint à la demande, la Commission rappelle que celui-ci doit impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n°1.165 du 23 décembre 1993.

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

Le droit d'accès s'exerce sur place auprès de la Direction administrative et financière.

La Commission constate ainsi 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 aux Autorités administratives et judiciaires dans le cadre de leurs missions légalement conférées.

La Commission considère que le Service d'Information et de Contrôle des Circuits Financiers (SICCFIN) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires d'informations nominatives traitées.

Par ailleurs, elle estime que la communication aux autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, la Commission rappelle qu'en cas de transmission, ces autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

Elle considère donc que de telles transmissions sont conformes aux exigences légales.

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

Les personnes habilitées à avoir accès au traitement sont :

- la Direction administrative et financière : tous droits ;
- le Supérieur hiérarchique : demande de création et de suppression ;
- le Responsable de conformité : consultation en cas de contrôle interne ;
- le personnel du service technique (SI) : tous droits dans le cadre de ses mission.

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

La Commission rappelle toutefois 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 d'une interconnexion avec un traitement ayant pour finalité « *Gestion administrative des salariés* ».

A cet égard, la Commission prend acte que ce traitement a été légalement mis en œuvre.

Par ailleurs, il appert à l'étude du dossier un rapprochement avec un traitement lié à la messagerie professionnelle, également légalement mis en œuvre.

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 demande par ailleurs que, comme le permet l'application, tout document dit confidentiel soit impérativement chiffré

Enfin, la Commission rappelle également 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

Les informations relatives à l'identité, à la formation, aux diplômes, à la vie professionnelle, aux données d'identification électronique, au compte utilisateur et aux contenus de la solution sécurisée sont conservées durant toute la durée de présence du salarié dans l'entreprise ou de la durée nécessaire à l'exécution de la mission du consultant.

Sur ce point la Commission considère que les documents placés dans ce traitement ne doivent être conservés que tant que le responsable de traitement en a l'utilité.

Par ailleurs, les informations temporelles sont conservées 1 an à compter de leur collecte.

La Commission considère que ces durées sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Gestion de la solution sécurisée de stockage et de partage de fichiers par des collaborateurs habilités* ».

Rappelle que :

- la procédure interne accessible en Intranet doit impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n°1.165 du 23 décembre 1993 ;

- le SICCFIN et la CCAF peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires des informations du traitement ;

- les Autorités judiciaires ne peuvent avoir accès aux informations objet du traitement que dans le strict cadre de leurs 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.

Considère que les documents placés dans ce traitement ne doivent être conservés que tant que le responsable de traitement en a l'utilité.

Demande que tout document dit confidentiel soit impérativement chiffré.

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 Tavira Monaco SAM du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion de la solution sécurisée de stockage et de partage de fichiers par des collaborateurs habilités* ».**

Le Président

Guy MAGNAN