Délibération n° 2024-095 du 15 mai 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 des habilitations et des accès informatiques mis en œuvre à des fins de contrôle des accès au Système d'Information* »

présenté par DIAGNOSTIC COMPTABILITE AUDIT 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° 1.231 du 12 juillet 2000 relative aux professions d'expert-comptable et de comptable agréé ;

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, 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, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 7.065 du 26 juillet 2018 portant modification de l'Ordonnance Souveraine n° 2.318 du 3 août 2009 fixant les conditions d'application de la loi n° 1.362 du 3 août 2009, modifiée, relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la corruption ;

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 DIAGNOSTIC COMPTABILITE AUDIT SAM le 7 février 2024 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 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 5 avril 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 15 mai 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

DIAGNOSTIC COMPTABILITE AUDIT SAM (DCA SAM) est une société anonyme d'expertise comptable monégasque, membre de l'Ordre des Experts-Comptables de Monaco.

Afin de sécuriser l'accès à son système d'information (SI), cette société souhaite mettre en place un système d'habilitations.

Le traitement objet de la présente demande permet de surveiller les accès au système d'information, 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 des habilitations et des accès informatiques mis en œuvre à des fins de contrôle des accès au Système d'Information ».*

Les personnes concernées sont tous les collaborateurs et stagiaires de DIAGNOSTIC COMPTABILITE AUDIT SAM.

Enfin, les fonctionnalités de ce traitement sont les suivantes :

Dans le cadre de la gestion des habilitations *:*

- octroyer et délivrer aux utilisateurs les moyens techniques et fonctionnels permettant de s'authentifier au Système d'Information afin d'exercer la fonction et les missions pour lesquelles ils ont été recrutés, ceci dans le respect du « *Moindre Privilège* » et du « *Besoin d'en connaître* » ;
- créer et gérer des profils utilisateurs standard, s'assurant notamment de la séparation des tâches, en cohérence avec les fonctions de chacun au sein de la société ;
- administrer les droits d'accès aux applications et aux dossiers hébergés sur les serveurs ;
- gérer les évolutions des droits, les mobilités internes et les départs ;
- mettre à jour les comptes système et les informations administratives s'y rapportant (ex : changement de patronyme) ;
- permettre la réalisation de l'ensemble des tâches d'activation/ désactivation/suppression de comptes ;
- procéder à des contrôles afin de s'assurer de la conformité des droits délivrés par rapport aux règles édictées en matière d'accès à l'information.

Dans le cadre de la supervision des accès aux applications :

- collecter des évènements systèmes permettant de tracer les habilitations octroyées, visant à prévenir le risque de fraude et s'assurer de la cohérence des accès ;
- établir des alertes qui permettent de détecter tout risque de malveillance ou tout comportement anormal et de s'assurer de la cohérence des accès avec les habilitations délivrées.

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 tout d'abord justifié par le respect d'une obligation légale.

Il précise ainsi qu'en tant que société d'expertise-comptable, il est soumis à l'application de la Loi n° 1.231 du 12 juillet 200 relative aux professions d'expert-comptable et de comptable agréé, qui dispose à son article 29 que « *les membres de l'Ordre sont tenus au secret professionnel sous les peines prévues à l'article 308 du Code Pénal* ».

La Commission relève que le responsable de traitement est également soumis à l'application de la Loi n° 1.362 du 3 août 2009 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive et la corruption, en vertu de l'alinéa 20 de l'article 1er qui vise « *les professionnels relevant de la loi 1.231 du 12 juillet 2000 relative à la profession d'expert-comptable et de comptable agréé* ».

Elle note qu'à ce titre, le responsable de traitement est tenu « *à l'identification de ses clients personnes physiques et morales, y compris les bénéficiaires effectifs de ces personnes morales, et à la conservation desdits documents d'identification* » et qu'il « *doit assurer la confidentialité des données, notamment des données clients* ».

Le responsable de traitement indique par ailleurs que le traitement est également justifié 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 ledit traitement va ainsi notamment permettre « *la sécurité et le bon fonctionnement technique du réseau ou Système Informatique* » et « *la protection des intérêts économiques et financiers de la société auxquels est attaché un caractère de confidentialité* ».

Elle 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, prénom ;
- adresses et coordonnées : coordonnées téléphoniques professionnelles ;
- formation, diplômes, vie professionnelle : titre, fonction ;
- données d'identification électronique : identifiant numérique, adresse mail, applications et profils associés ;
- informations temporelles : horodatage, outil informatique utilisé, traces d'exécution.

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

Les données d'identification électronique ont pour origine le Département IT.

Enfin, les informations temporelles 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 mention ou clause particulière intégrée dans un document remis à l'intéressé.

A la lecture de la charte informatique jointe au dossier, la Commission rappelle toutefois que l'information préalable des personnes concernées doit impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, et notamment les modalités d'exercice du droit d'accès.

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

Le droit d'accès s'exerce sur place.

A cet égard, la Commission rappelle que la réponse à un droit d'accès doit s'effectuer dans un délai d'un mois à compter de la demande.

Sous cette réserve, elle 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.

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.

A cet égard, la Commission rappelle qu'en cas de transmission, ces Autorités ne pourront avoir communication des informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

Sous ces conditions, elle considère 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 :

- le Département IT : tous droits ;
- le Département RH : inscription pour les informations administratives, inscription et mise à jour pour les droits d'accès.

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

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 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.

Le responsable de traitement indique que le présent traitement est également interconnecté avec tous les traitements déjà mis en place ou à venir.

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.

Enfin, la Commission 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 la durée de conservation

Les informations relatives à l'identité, aux adresses et coordonnées, à la formation, aux diplômes et à la vie professionnelle sont conservées jusqu'à trois mois après le départ de la personne concernée.

Les données d'identification électronique sont conservées tant que la personne est en poste.

Enfin, les informations temporelles sont conservées 1 an.

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

Après en avoir délibéré, la Commission :

Rappelle que :

- l'information préalable des personnes concernées doit impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993, et notamment les modalités d'exercice du droit d'accès ;

- la réponse à un droit d'accès doit s'effectuer dans un délai d'un mois à compter de la demande ;

- les Autorités judiciaires et administratives ne peuvent avoir communication des 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 ;

- que 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 de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par DIAGNOSTIC COMPTABILITE AUDIT SAM du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations et des accès mis en œuvre à des fins de contrôle des accès au Système d'Information* ».**

Le Président

Guy MAGNAN