Délibération n° 2021-164 du 21 juillet 2021

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 des habilitations et des accès informatiques et utilisation des moyens informatiques* »

présenté par JUTHEAU-HUSSON

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, 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° 2.318 du 3 août 2009, modifiée, 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, modifiée ;

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 JUTHEAU-HUSSON le 30 mars 2021 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion et supervision des habilitations et des accès informatiques et utilisation des moyens informatiques* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 27 mai 2021, 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 21 juillet 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

JUTHEAU-HUSSON est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 56S00160, ayant pour activité « *Toutes opérations de courtage ayant trait aux assurances et aux réassurances, la gestion de tous portefeuilles d'assurances et toutes opérations mobilières ou immobilières se rattachant à l'objet social* ».

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 et supervision des habilitations et des accès informatiques et utilisation des moyens informatiques ».*

Les personnes concernées sont les salariés.

Enfin, les fonctionnalités de ce traitement 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 avec l'appui du service des ressources humaines ;
- 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 :

- prévenir et limiter les fausses manœuvres réalisées par des utilisateurs identifiés et prévenir et/ou le contrôle d'accès par des personnes extérieures non autorisées ;
- établir des preuves en cas de litige.

Dans le cadre de la sécurité anti-virus :

- mettre en place des remontées d'alertes sur les risques d'intrusion ;
- empêcher la collecte massive de données par des mécanismes de type Data Loss Prevention ;
- établir des rapports (ex : audit de sécurité, détection de risques…).

Le responsable de traitement indique par ailleurs que le dispositif permet « *Plus généralement la surveillance des systèmes d'information afin de se conformer aux exigences des normes internationales dont les normes ISO 27001 et ISO 9001* ».

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, à savoir les obligations particulières de vigilance ainsi que de traçabilité des opérations effectuées imposées par 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, en raison « *des données sensibles susceptibles d'être collectées* ».

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 prend acte qu'il est important pour la société « *de pouvoir assurer la disponibilité, l'intégrité et la fiabilité des données qu'elle collecte »* et que « *Compte tenu des catégories de personnes avec qui elle est en relation d'affaires (institutions monégasques, personnes politiquement exposées, etc…), elle se doit de préserver ses intérêts économiques, commerciaux et financiers ainsi que sa réputation* ».

Au vu de ce qui précède, 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, prénom et service de l'employé, nom, prénom et signature du supérieur pour la gestion des habilitations ;
- 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.

Les informations relatives à l'identité, aux données d'identification électronique et au compte utilisateur ont pour origine le traitement ayant pour finalité « *Gestion administrative du salarié* ».

Par ailleurs, les informations temporelles ont pour origine le système de contrôle des accès.

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 s'effectue par le biais d'une procédure interne accessible en Intranet.

Cette procédure n'ayant pas été jointe à la demande, la Commission rappelle que celle-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 ou par courrier électronique.

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, la Commission considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle 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° 2015-116 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous ces conditions, 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.

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 judiciaires dans le cadre de leurs missions légalement conférées.

La Commission estime ainsi 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.

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 Responsable RH : demande de création des comptes utilisateurs ;
- le Responsable LAB : vérification des niveaux d'habilitation des personnes en charge des traitements relatifs à la lutte contre le blanchiment ;
- la Direction Informatique : création, modification et suppression des utilisateurs, des groupes de profils, extraction des preuves et réalisation des contrôles.

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

La Commission rappelle 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.

Elle rappelle par ailleurs que si des prestataires techniques devaient avoir accès au traitement, leurs droits d'accès devront être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, et qu'ils seront soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de l'article 17 de la Loi n° 1.165 du 23 décembre 1993.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet de trois interconnexions avec les traitements ayant respectivement pour finalité « *Passation, gestion, exécution et gestion des sinistres des contrats d'assurance* », « *Gestion du contentieux et du précontentieux* » et « *Gestion administrative des salariés* ».

A cet égard, la Commission prend acte que ces traitements ont été légalement mis en œuvre et qu'ils 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 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 les durées de conservation

Le responsable de traitement indique que les informations relatives à l'identité, les données d'identification électronique et les données liées au compte utilisateur sont conservées toute la durée de présence au sein de l'organisme.

Par ailleurs, les informations temporelles sont conservées 3 mois.

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

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 que l'expéditeur du courriel est effectivement la personne concernée par les informations ;

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 ;

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

- 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 ;

- si des prestataires techniques devaient avoir accès au traitement, leurs droits d'accès devront être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, et qu'ils seront soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de l'article 17 de la Loi n° 1.165 du 23 décembre 1993 ;

- 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 de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par JUTHEAU-HUSSON du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion et supervision des habilitations et des accès informatiques et utilisation des moyens informatiques* ».**

Le Président

Guy MAGNAN