Délibération n° 2019-153 du 16 octobre 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 des habilitations des accès mis en œuvre à des fins de contrôle desdits accès au Système d'Information* »

présenté par DOCAPOST BPO

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 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 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 DOCAPOST BPO le 15 juillet 2019 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Gestion des accès – logiciel BASTION – SCB* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 13 septembre 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 16 octobre 2019 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

DOCAPOST BPO est une société française établie à Monaco par sa succursale enregistrée au RCI sous le numéro 01S03976, ayant pour objet le traitement des chèques.

Afin de sécuriser l'accès à son système d'information, cette société souhaite mettre en place un système de contrôle d'accès qui permet de contrôler, superviser et auditer les accès des administrateurs systèmes aux serveurs et périphériques réseaux et sécurité.

Le traitement objet de la présente demande permettant 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 responsable de traitement indique que le traitement a pour finalité « *Gestion des accès – logiciel BASTION – SCB ».*

Les personnes concernées sont les salariés disposant notamment de « *comptes à privilèges* ».

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 ;
- 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 systèmes* » :

- 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…).

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 objet la gestion des habilitations aux accès et qu'il est mis en œuvre à des fins de contrôle de ces accès au Système d'Information.

Par conséquent, elle modifie la finalité comme suit : « *Gestion des habilitations des accès mis en œuvre à des fins de contrôle desdits accès au Système d'Information* ».

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le traitement est 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 dans *« le cadre des activités de traitement documentaires comprenant notamment le traitement de documents bancaires pour le compte des établissements bancaires situés sur le territoire monégasque, DOCAPOST a besoin de sécuriser l'accès à son système d'information* ».

Le responsable de traitement précise en outre que l'outil mis en place est « *une bonne pratique reconnue sur le marché des prestations SI* ».

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 ;
- coordonnées : adresse email ;
- informations relatives à la demande : projet, cible de l'accès, rattachement hiérarchique, date début/fin habilitation, statut habilitation ;
- identifiant : première lettre du prénom et nom complet ;
- identifiant de connexion : première lettre du prénom, nom complet ;
- données de connexion : adresse IP au serveur, protocole ;
- logs de connexion : donnée d'horodatage de la connexion, adresse IP, source et destination, port et protocole ;
- identifiant piste d'audit : première lettre du prénom, nom complet ;
- piste d'audit : enregistrement des sessions.

Les informations relatives à l'identité et aux coordonnées, les informations relatives à la demande, le statut de la demande et l'identifiant ont pour origine la matrice Habilitation.

Toutes les autres informations ont pour origine le système de contrôle d'accès au SI.

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 d'une clause particulière intégrée dans un document remis à l'intéressé et par le biais d'une procédure de gestion des habilitations « *BASTION* ».

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.

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

Le droit d'accès s'exerce par voie postale ou par courrier électronique.

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 cette condition, 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 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 les personnels du Centre de sécurité informatique DOCAPOST en création, suppression et modification.

Considérant les attributions 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.

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

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

Le responsable de traitement indique par ailleurs que le traitement est interconnecté avec le traitement lié à l'Outil de ticketing : HPSM.

Ce traitement n'ayant pas fait l'objet de formalité auprès de la CCIN, 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 recommande toutefois que le fichier Excel (matrice d'habilitation) soit sécurisé en tenant compte de la nature des informations qu'il contient.

Elle rappelle par ailleurs 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.

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

Le responsable de traitement indique que les informations sont conservées le temps des habilitations + 18 mois.

Concernant les identifiants de connexion et les données de connexion, la Commission rappelle toutefois, conformément à sa délibération n° 2010-13 du 3 mai 2010, 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, au regard des fonctionnalités du présent traitement, elle fixe la durée de conservation des identifiants de connexion et des données de connexion à 1 an.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Gestion des habilitations des accès mis en œuvre à des fins de contrôle desdits accès au Système d'Information* ».

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.

Recommande que le fichier Excel soit sécurisé en tenant compte de la nature des informations qu'il contient.

Rappelle que :

- les documents d'information préalable des salariés doivent 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 ;

- 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.

Demande que le traitement lié à l'Outil de ticketing : HPSM lui soit soumis dans les plus brefs délais.

Fixe la durée de conservation des identifiants de connexion et des données de connexion à 1 an.

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 DOCAPOST BPO du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion des habilitations des accès mis en œuvre à des fins de contrôle desdits accès au Système d'Information* ».**

Le Président

Guy MAGNAN