

Délibération n° 2024-035 du 21 février 2024

de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre de la modification du traitement automatisé d'informations nominatives ayant pour finalité

« *Gestion d'un outil de partage et de conservation sécurisés de documents* »  
du Secrétariat Général du Gouvernement

présentée par le Ministre d'Etat

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne 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 portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la délibération n° 2020-168 du 18 novembre 2020 de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion d'un outil de partage de documents sécurisés avec des partenaires internes et externes à l'administration monégasque* », du Secrétariat Général du Gouvernement présenté par le Ministre d'Etat ;

Vu la demande d'avis déposée par le Ministre d'Etat, le 24 octobre 2023, concernant la mise en œuvre de la modification du traitement automatisé ayant pour finalité « *Gestion d'un outil de partage et de conservation sécurisés de documents* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 21 décembre 2023, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 21 février 2024 portant examen du traitement automatisé susvisé.

## **La Commission de Contrôle des Informations Nominatives,**

### **Préambule**

Le Gouvernement a souhaité mettre en œuvre une solution lui permettant le partage et le stockage de manière sécurisée, quel que soit le contexte dans lequel se trouve l'utilisateur, de documents confidentiels.

Par délibération n° 2020-168 du 18 novembre 2020 ce traitement a reçu l'avis favorable de la Commission.

Désormais, le Ministre d'Etat souhaite modifier la finalité, ajouter de nouvelles fonctionnalités et mettre à jour la liste des informations traitées.

Ainsi, cette modification est soumise à l'avis de la Commission, conformément à l'article 9 de la Loi n° 1.165 du 23 décembre 1993.

### **I. Sur la finalité et les fonctionnalités du traitement**

Le responsable de traitement entend faire évoluer la finalité du traitement de « *Gestion d'un outil de partage de documents sécurisés avec des partenaires internes et externes à l'administration monégasque* » à « *Gestion d'un outil de partage et de conservation sécurisés de documents* ».

Il concerne les Fonctionnaires et Agents de l'Etat, les prestataires externes de l'Etat ainsi que tout utilisateur externe invité sur la solution.

Les fonctionnalités du traitement sont désormais :

- pour les administrateurs de la solution :
  - o gérer les habilitations d'accès à l'outil ;
  - o gérer les créations de comptes sur l'outil ;
  - o gérer les chartes d'utilisation et d'administration de l'outil ;
  - o gérer les licences attribuées et en maîtriser les coûts ;
  - o établir et suivre le respect des règles de suppression des comptes et des espaces de travail non utilisés ou qui ne seront plus utilisés, dans le respect de la confidentialité des informations et des documents échangés dans l'outil ;
  - o établir et suivre le respect des règles de modification de propriétaire en cas de suppression d'un compte « *mono-propriétaire* » ou en cas d'indisponibilité de propriétaire ;
  - o assurer le support utilisateur ;
  - o établir des statistiques nominatives et non nominatives.
  
- pour les utilisateurs de la solution :
  - o créer des espaces de travail (appelés « *workspaces* ») à des fins de stockage et de partage de documents ;
  - o inviter des personnes (internes ou externes à l'Administration) à accéder à un espace de travail spécifique ;
  - o échanger des documents de manière sécurisée avec des utilisateurs déterminés ;
  - o gérer les affectations et les révocations des accès aux documents grâce à la gestion des rôles des utilisateurs ;

- créer et envoyer des liens de partage sécurisés permettant de partager et télécharger un document ;
- accéder à ces documents sur PC et en mobilité.

Par complément d'information, le responsable de traitement indique que l'établissement de statistiques nominatives a pour objectif l'optimisation de l'utilisation de la solution notamment en réalisant un suivi, sans accès au contenu des espaces de travail, des utilisateurs qui disposent d'une licence mais qui ne l'utilisent pas.

La Commission en prend acte.

Enfin, le responsable de traitement indique que « *les fonctionnalités du traitement seront différentes selon les profils* » des utilisateurs. Il précise à ce sujet que 4 profils différents existent : utilisateur, administrateur, invité et anonyme.

La Commission constate 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 présent traitement est justifié par la réalisation d'un intérêt légitime sans que ne soient méconnus les droits et libertés fondamentaux de la personne concernée.

A cet égard le responsable de traitement indique que le traitement permet « *d'échanger et de stocker des documents de manière sécurisée avec d'autres utilisateurs, permettant ainsi de renforcer la sécurité autour des échanges et des partages de documents* ».

Il est également précisé que ce traitement « *n'a pas pour objet de surveiller l'activité des personnes concernées* ».

La Commission considère que ce 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 traitées**

Les informations traitées sont désormais :

- sur l'utilisateur de l'outil de partage sécurisé de documents :
  - identité : nom, prénom ;
  - coordonnées : adresse email professionnelle ;
  - vie professionnelle : entité ;
  - accès : profil, accès, droits de l'utilisateur liés à son compte ;
  - compte utilisateur : statut du compte (inscrit, supprimé), liste des trustees, liste des utilisateurs invités (nom, prénom, email, date et heure de l'inscription, date et heure de la dernière activité), zone d'observations ;
  - informations temporelles : date et heure de dépôt, consultation, suppression ou action effectuée sur le document (ex. téléchargement), date et heure de connexion, date et heure d'inscription, date et heure de la dernière activité/de la dernière connexion sur le compte/ sur le terminal, date et heure de la création d'un espace de travail, date et heure de la dernière modification sur l'espace de travail, logs des actions d'utilisation, traces d'exécution, fichiers journaux, adresse IP de connexion, terminaux, statut, empreinte du terminal ;
  - données d'identification électronique : login (adresse email), mot de passe ;

- documents : nom du document, taille, type de document (ex. Word, PDF), activité sur le document (ex. téléchargement), statut du téléchargement (terminé, en cours) ;
  - fichiers : nom du fichier, taille ;
  - espaces de travail : nom de l'espace de travail, nombre d'espaces de travail, utilisateurs de l'espace de travail, statut de l'espace de travail (actif, supprimé), nombre de propriétaires, nombres de membres, rôle de l'utilisateur dans l'espace de travail (propriétaire, membre, lecteur) ;
  - données d'usages (métadonnées) : date et heure à laquelle une action s'est déroulée, adresse email de l'utilisateur, nom du serveur sur lequel l'action a eu lieu, adresse IP de l'utilisateur, liste des trustees de l'utilisateur, liste des personnes invitées par un utilisateur, liste des espaces de travail dans lesquels un utilisateur est membre et le nom des espaces de travail, rôle de l'utilisateur dans chaque espace ;
  - charte utilisateur : signature, date de signature ;
  - statistiques.
- sur les administrateurs de l'outil de partage sécurisé de documents :
    - identité : nom, prénom ;
    - coordonnées : adresse email professionnelle ;
    - données d'identification électronique : login (adresse email), mot de passe ;
    - informations temporelles : date et heure de connexion et des logs des actions d'administration, IP de connexion ;
    - charte administrateur : signature, date de signature.
  - sur le témoin en cas de procédure de modification du propriétaire :
    - identité : nom, prénom, signature.
  - sur le Chef de Service en cas de procédure de modification du propriétaire :
    - identité : nom, prénom, signature.
  - sur l'utilisateur propriétaire d'un espace de travail « *mono-propriétaire* » :
    - identité : nom, prénom, signature.
    - coordonnées : adresse email ;
    - espaces de travail : liste des espaces de travail concernés par la procédure de modification de propriétaire, nom des espaces de travail.

S'agissant de la « *zone d'observations* », le responsable de traitement indique qu'elle est par exemple utilisée « *afin d'informer un administrateur de ne pas supprimer le compte [d'un] utilisateur en particulier* ». Par ailleurs, il précise que « *les administrateurs s'assureront du caractère proportionné des informations portées dans cet espace* ».

La Commission en prend acte.

Les informations relatives aux personnes concernées, disposant d'un compte utilisateur ou administrateur ont pour origine la personne concernée pour les informations sur l'identité, les coordonnées, les documents qui sont partagées ou stockées, la charte utilisateur et les données d'identification électronique. Les informations relatives aux accès accordés aux comptes utilisateurs proviennent de l'Administrateur. Les autres données sont générées par le système.

Les informations sur le témoin et le Chef de Service en cas de procédure de modification de propriétaire ainsi que les informations sur l'utilisateur propriétaire d'un espace de travail « *mono-propriétaire* » proviennent du Chef de Service.

La Commission considère 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 précise que les utilisateurs sont informés par la notice d'information diffusée sur l'intranet du Gouvernement, par la Charte Utilisateur de l'outil ainsi que par un email envoyé par la Direction des Systèmes d'Information (DSI) dans l'hypothèse où ils ont fait l'objet d'une procédure de modification de propriétaire.

Il indique par ailleurs que l'information préalable des administrateurs est assurée par la notice d'information diffusée sur l'intranet ainsi que par la Charte Administrateur de l'outil.

A la lecture des documents joints au dossier, la Commission constate que les utilisateurs et les administrateurs sont informés de manière conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

La Commission relève en outre que les chartes d'utilisation de la solution, avertissent également les personnes concernées de leurs devoirs dans leur utilisation de l'outil, participant ainsi à la sécurisation du processus.

Par ailleurs, le responsable de traitement précise que les invités à l'outil sont informés par une mention insérée dans l'email d'invitation.

A l'analyse de la mention jointe au dossier, la Commission constate que les invités sont informés de manière conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

En toute fin, le responsable de traitement indique que des mentions relatives au traitement des informations nominatives sont également insérées dans les formulaires et les procès-verbaux relatifs à la modification de propriétaire ainsi que qu'à la suppression d'un espace de travail.

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

Le droit d'accès est exercé par voie postale et par courrier électronique auprès de la Direction Interministérielle chargée de la Transition Numérique (DITN).

Par ailleurs, il ressort à la lecture du dossier que le droit d'accès peut également être exercé au moyen d'un formulaire permettant de contacter la cellule protection des données personnelles de la DITN.

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit s'exercer dans le mois suivant la réception de la demande.

Elle rappelle en outre, que dans le cadre de l'exercice du droit d'accès par voie électronique une procédure doit être mise en place afin que le responsable de traitement puisse s'assurer, en cas de doute sur l'identité de la personne à l'origine du courriel, qu'il s'agit effectivement de 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° 2015-113 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 personnes ayant accès au traitement**

La Commission constate qu'il n'y a pas de destinataire des informations objets du présent traitement.

Par ailleurs, les accès ont été définis comme suit :

- fonctionnaires et agents de l'Etat disposant d'un compte « *utilisateur* » : en inscription, modification, consultation, invitation, suppression et partage ;
- prestataires externes de l'Etat qui disposent d'un compte « *utilisateur* » : en inscription, modification, consultation, invitation, suppression et partage ;
- les personnes disposant d'un compte « *invité* » : en lecture et/ou dépôt de documents sur les espaces de travail affectés ;
- utilisateur anonyme : en lecture ;
- administrateur : tous droits de fonctionnement sans accès aux documents ;
- prestataire de la solution : dans le cadre de ses opérations de maintenance sans accès aux documents.

En ce qui concerne le recours à des prestataires, 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 de ces derniers doivent être limités à ce qui est strictement nécessaire à l'exécution de leurs contrats de prestation de service. De plus, lesdits prestataires sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

Enfin, la Commission prend acte des précisions du responsable de traitement indiquant que le prestataire d'hébergement n'a pas accès aux données objet du présent traitement.

Aussi, la Commission considère que ces accès sont justifiés.

## **VI. Sur les interconnexions et rapprochements**

Le présent traitement est interconnecté avec le traitement relatif à la Gestion de la messagerie électronique professionnelle du Gouvernement, légalement mis en œuvre, afin de permettre les échanges. Le responsable de traitement précise en outre que cette interconnexion permet à la Direction des Systèmes d'Information de diffuser la Charte Utilisateur de l'outil, ainsi que les mentions d'informations préalablement à l'inscription.

Par ailleurs, le responsable de traitement indique que le traitement fait l'objet d'un rapprochement avec le traitement, légalement mis en œuvre, ayant pour finalité « *Assistance aux utilisateurs par le Centre de Service de la DSI* », afin de traiter une demande de création de compte selon une procédure établie.

Il indique enfin que le présent traitement est rapproché avec tout traitement utilisant la solution comme outil de partage de documents ou de conservation.

A cet égard la Commission rappelle que les rapprochements ne peuvent être effectués qu'entre des traitements 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.

Cependant, 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 Commission rappelle enfin 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 relatives au témoin et au Chef de Service en cas de procédure de modification de propriétaire ainsi que celles relatives à l'utilisateur propriétaire d'un espace de travail « *mono-propriétaire* » sont conservées « *1 an à partir de l'opération de modification de propriétaire* ».

En outre, il est indiqué que les statistiques sont conservées pendant 1 an.

Le responsable de traitement indique par ailleurs que les informations relatives à l'utilisateur et à l'administrateur de l'outil de partage sécurisé de documents sont conservées comme suit :

- l'identité, les coordonnées, les informations sur la vie professionnelle, les informations sur les accès et celles relatives au compte : pendant la durée de vie du compte puis pendant une durée maximale de 12 mois suite à l'arrêt du service ;
- les documents, les fichiers ainsi que les espaces de travail : jusqu'à la suppression du document, du fichier ou de l'espace de travail par un propriétaire de cet espace. Le responsable de traitement précise que le log relatif à la suppression des « *documents, fichiers et espaces de travail* » est ensuite conservé pendant 1 an ;
- la charte utilisateur/administrateur : « *désactivation au départ de l'utilisateur, puis conservation pendant 5 ans à compter de la désactivation* » ;
- les informations temporelles, les données de connexion, les données d'usage ainsi que les données d'identification électronique : 1 an à compter de la date d'enregistrement puis suppression.

La Commission considère que la durée de conservation des informations d'identité, les coordonnées, les informations sur la vie professionnelle, les informations sur les accès et celles relatives au compte utilisateur et administrateur est excessive. En effet, si une conservation de ces informations est essentielle pendant la durée de vie du compte, la conservation après suppression dudit compte pendant 12 mois n'est pas justifiée. Dès lors, la Commission fixe la durée de conservation de ces informations à 3 mois après la suppression du compte.

S'agissant ensuite des données d'identification électronique des personnes concernées, la Commission considère que la conservation *pendant « 1 an à compter de la date d'enregistrement »* est insuffisante. En effet, les données d'identification électronique sont celles permettant à la personne concernée de se connecter à son compte. Ainsi, la Commission fixe la durée de conservation de ces informations à la durée de vie du compte.

S'agissant enfin de la durée de conservation de la charte utilisateur/administrateur, la Commission relève des précisions du responsable de traitement que *« ce délai de conservation est nécessaire afin de pouvoir « réactiver » la charte, notamment si la personne revient au sein de l'Administration (...), ou en cas de contentieux pour prouver que l'utilisateur avait bien signé la charte »*. A cet égard, la Commission relève que la durée de conservation de 5 ans à compter de la désactivation du compte est excessive. D'une part les autres informations objet du traitement répondent à une durée de conservation plus courte et dès lors une conservation à 5 ans de la charte à des fins probatoires apparaît sans effet en absence d'éléments d'imputabilité. La Commission estime en outre qu'il s'agit d'un document de gestion administrative des agents et fonctionnaires qui n'a pas vocation à être conservé au-delà de sa période d'emploi. D'autre part, dans l'hypothèse où un utilisateur revient sur la plateforme il convient de lui faire signer à nouveau la charte afin qu'il en approuve à nouveau son contenu notamment en raison du caractère évolutif du document. Ainsi, la Commission fixe la durée de conservation de la charte signée à 1 an après la suppression du compte.

#### **Après en avoir délibéré, la Commission :**

##### **Rappelle que :**

- la réponse au droit d'accès doit s'exercer dans le mois suivant la réception de la demande ;
- une procédure relative au droit d'accès par voie électronique doit être mise en place afin que le responsable de traitement puisse s'assurer, en cas de doute sur l'identité de la personne à l'origine du courriel, qu'il s'agisse effectivement de la personne concernée par les informations ;
- les rapprochements ne peuvent être effectués qu'entre des traitements légalement mis en œuvre ;
- 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 passe réputé fort, régulièrement renouvelé.



**Fixe** les durées de conservation comme suit :

- les données d'identité, les coordonnées, les informations sur la vie professionnelle, les informations sur les accès et celles relatives au compte utilisateur et administrateur : 3 mois après la suppression du compte ;
- les données d'identification électronique : tant que la personne dispose d'un compte ;
- la charte utilisateur/administrateur signée : 1 an après la suppression du compte.

**Sous le bénéfice de la prise en compte de ce qui précède,**

la Commission de Contrôle des Informations Nominatives **émet un avis favorable à la mise en œuvre de la modification, par le Ministre d'Etat, du traitement automatisé d'informations nominatives ayant pour finalité « *Gestion d'un outil de partage et de conservation sécurisés de documents* » du Secrétariat Général du Gouvernement.**

Le Président

Guy MAGNAN