Délibération n° 2022-167 du 16 novembre 2022

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

« *Permettre la création et la gestion d'un profil de révocation des certificats électroniques en ligne* »

dénommé « *Profil de révocation MConnect* »

exploité par la Direction des Services Numériques

présenté 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 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° 1.483 du 17 décembre 2019 relative à l'identité numérique ;

Vu l'Ordonnance Souveraine n° 8.696 du 17 juin 2021 relative à la carte d'identité monégasque ;

Vu l'Ordonnance Souveraine n° 8.697 du 17 juin 2021 portant modification de l'Ordonnance Souveraine n° 3.153 du 19 mars 1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté ;

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'Arrêté Ministériel n° 2021-430 du 17 juin 2021 portant application de l'article 4 de l'Ordonnance n° 3.153 du 19 mars 1964 sur les conditions d'entrée et de séjour des étrangers dans la Principauté, 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 d'informations nominatives ;

Vu la délibération n° 2021-105 du 2 juin 2021 de la Commission de Contrôle des Informations Nominatives portant avis sur la consultation du Ministre d'Etat sur un projet d'Ordonnance Souveraine relative à la carte d'identité monégasque et sur un projet d'Ordonnance Souveraine portant modification de l'Ordonnance n° 3.153 du 19 mars 1964 relative aux conditions d'entrée et de séjour des étrangers dans la Principauté et son Arrêté Ministériel portant application de l'article 4 de l'Ordonnance n° 3.153 du 19 mars 1964 sur les conditions d'entrée et de séjour des étrangers dans la Principauté ;

Vu la délibération n° 2021-111 du 2 juin 2021 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 des moyens d'utilisation de l'identité numérique inscrits sur les cartes d'identité monégasque et les cartes de séjour (certificats, code CAN et PUK)* » dénommé « *CLCM* » exploité par la Direction des Services Numériques présenté par le Ministre d'Etat ;

Vu la délibération n° 2021-112 du 2 juin 2021 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 « *Fourniture des services de confiance pour l'identité numérique* » ;

Vu la demande d'avis déposée par le Ministre d'Etat le 11 aout 2022 concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité *« Permettre la création et la gestion d'un profil de révocation des certificats électroniques en ligne* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 7 octobre 2022, 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 16 novembre 2022 portant examen du traitement automatisé susvisé.

## La Commission de Contrôle des Informations Nominatives,

### Préambule

La Principauté a mis à dispositions des monégasques et de ses résidents une identité numérique sur leurs cartes d'identité ou de résidents, dérivable sur mobile, et dont les traitements permettant sa mise en œuvre ont reçu des avis favorables en 2021.

Le responsable de traitement souhaite désormais mettre à disposition de ces personnes un téléservice leur permettant de révoquer à tout moment et à distance leurs certificats si elles les estiment compromis, comme en cas de perte ou de vols de leurs cartes supports de leur identité numérique.

Ainsi, le traitement y relatif est soumis à l'avis de la Commission, conformément à l'article 7 de la Loi n° 1.165 du 23 décembre 1993.

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

Le traitement a pour finalité « *Permettre la création et la gestion d'un profil de révocation des certificats électroniques en ligne* » et est dénommé « *Profil de révocation MConnect* ».

Le responsable de traitement précise qu'il concerne les monégasques et résidents disposant d'une identité numérique, les agents de la Direction des Services Numériques (DSN) administrateurs du téléservice ainsi que les administrateurs de base de données du prestataire.

En outre, les fonctionnalités permettent à toute personne détentrice d'une identité numérique de :

- créer son profil de révocation MConnect ;
- gérer son profil de révocation et ses moyens de contact ;
- consulter la date d'expiration de ses certificats ;
- être notifié de l'expiration prochaine de ses certificats ;
- être notifié de toute interruption de service MConnect planifiée ou imprévue ;
- révoquer en ligne les certificats électroniques liés à son identité numérique, en cas de vol ou de perte de sa carte notamment.

Il est précisé que ce téléservice « *permet à l'usager de révoquer ses certificats à tout moment et à distance sans l'intervention d'un opérateur (…). La révocation des certificats est alors immédiatement prise en compte par le système. La carte en tant que document de voyage reste néanmoins valide* ».

En outre, la DSN gère les notifications envoyées en cas d'interruption de service MConnect planifiée ou imprévue.

La Commission relève enfin qu'il est possible pour les usagers de se connecter à leur compte *via* leur identité numérique, soit par lecteur de carte, soit par l'identité numérique dérivée sur l'application mobile.

Elle 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 une mission d'intérêt public ainsi que par la réalisation d'un intérêt légitime qu'il poursuit sans méconnaitre ni l'intérêt, ni les droits et libertés fondamentaux des personnes concernées.

En ce qui concerne le motif d'intérêt public, le responsable de traitement, citant les Ordonnances Souveraines n° 8.696 et 8.697 portées au visa de la présente délibération, indique que « *la mise à disposition de ce téléservice s'inscrit dans le cadre de la gestion et du cycle de vie des certificats inscrits sur les cartes d'identité et les cartes de séjours monégasques et permet aux usagers de révoquer leurs certificats en ligne* ».

Il est en outre précisé qu'à la suite d'un audit commandité par l'AMSN, il a été rappelé la nécessité de permettre à tout usager de révoquer ses certificats avec prise en compte de la demande d'invalidation dans un délai de 24h.

Cette obligation d'invalidation sous 24h, qui se retrouve dans la règlementation eIDAS et dans la norme ETSI 319411 « *est un prérequis à la qualification des autorités de certification (Gouvernement Princier et Mairie) en tant que PSCO (Prestataire de Services de Confiance) et reconnu par l'Organisme COFRAC* ».

La Commission relève toutefois que l'article 8 alinéa 2 de l'Ordonnance Souveraine 8.696, susvisée dispose que « *En cas de perte, de vol, de changement de situation du titulaire du titre ou de suspicion de compromission, les certificats électroniques associés à l'identité numérique figurant au sein de la carte doivent être révoqués. Cette révocation est réalisée par les services compétents de la Commune, sur demande du titulaire de la carte selon un processus qui lui sera communiqué lors de la remise de sa carte* », tandis que l'article 6 de l' Arrêté Ministériel n° 2021-430 du 17 juin 2021 portant application de l'article 4 de l'Ordonnance n° 3.153 du 19 mars 1964 sur les conditions d'entrée et de séjour des étrangers dans la Principauté, modifiée, dispose qu'« *En cas de perte, de vol, de détérioration, de changement de situation du titulaire du titre ou de suspicion de compromission, les certificats électroniques associés à l'identité numérique figurant au sein de la carte de séjour doivent être révoqués. Cette révocation est réalisée par les services compétents de l'État, sur demande du titulaire de la carte selon un processus qui lui sera communiqué lors de la remise de sa carte* ».

Il s'en infère ainsi que la révocation doit être réalisée par les Services de la Communes pour les titulaires d'une carte d'identité et par les Services de l'Etat pour les titulaires d'une carte de séjour, ce qui n'est pas le mécanisme prévu par le présent traitement. Si la Commission s'accorde sur le principe qu'une plus grande sécurité existe si un certificat peut être révoqué par son titulaire sous 24heures, elle considère néanmoins que le cadre textuel doit être mis en conformité avant la mise en œuvre du présent traitement.

A cet égard, elle rappelle que par délibération n° 2021-105 du 2 juin 2021, susvisée, elle avait observé « *que la révocation des certificats relève des « services compétents de l'Etat », quel que soit le support de l'identité numérique* », marquant l'inadéquation des dispositions de l'Ordonnance Souveraine avec les modalités mises en œuvre en pratique.

La Commission avait également observé que les causes de révocation divergeaient selon que l'on soit titulaire d'une carte de séjour ou d'une carte d'identité. Si cela a en partie était corrigé, elle constate que seuls les titulaires d'une carte de séjour peuvent révoquer leur certificat pour une motif de détérioration.

Enfin, le responsable de traitement invoque l'intérêt légitime dans le cadre des mesures de simplification des relations Administration/administrés telles que prévues par l'Ordonnance Souveraine n° 2011-3413 du 29 aout 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré. A cet égard, la Commission relève qu'il est indiqué que la révocation par téléservice des certificats est optionnelle, l'usager pouvant choisir de se rendre à la Maire ou auprès de la Sûreté Publique pour en faire la demande. Il est précisé que les personnes concernées seront informées de la création du téléservice et des nouvelles modalités de révocation du certificat auprès de la Mairie/DSP. Les codes de révocation qui ont été donnés lors de l'attribution d'une carte d'identité ou de séjour ne seront plus nécessaires pour révoquer un certificat auprès de la Mairie ou de la DSP. Une révocation ne s'effectuant pas par le téléservice nécessitera de se déplacer en personne dans l'entité concernée par le titulaire d'une carte.

Sous la réserve susvisée, la Commission considère donc 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 nominatives traitées sont :

- Identité : données issues du processus d'authentification, à savoir nom d'usage si existant, prénoms, nom de naissance, sexe, date et heure de naissance, lieu de naissance ;
- Adresse et coordonnées : numéro de téléphone de l'usager dans les cas d'authentification par mobile, adresse email et/ou le numéro de téléphone renseigné dans les moyens de contact ;
- Données d'identification électronique : méthode d'authentification de l'usager (carte ou mobile), statut de l'identité (active, suspendue, inactive) ;
- Clé primaire : clé permettant de faire le lien entre le front-end, le back-end du module de révocation et les autres briques du CLCM pour identifier un individu lors de la création ou consultation du profil et lors d'une demande de révocation ;
- Clé technique : clé technique permettant de faire un lien entre l'individu, son accès et ses actions sur le téléservice. Cette clé est dérivée de la clé primaire ;
- Informations temporelles : logs de connexion des agents sur le back office (DSN), logs de connexion des administrateurs de bases de données du prestataire ;
- Autres données : autorité d'enregistrement (Mairie, Direction de la Sûreté Publique).
- Moyen de révocation : hash du code de révocation, questions choisies par l'usager et Hash des réponses secrètes.

Les informations relatives à l'identité et aux données d'identification électronique ont pour origine l'interconnexion avec le traitement ayant pour finalité « *Fourniture des services de confiance pour l'identité numérique* ». Celles relatives à la clé primaire et technique et aux « *autres données* » proviennent du traitement de « *Gestion des moyens d'utilisation de l'identité numérique inscrits sur les cartes d'identité monégasques et les cartes de séjour* ».

En ce qui concerne les adresses et coordonnées et les moyens de révocation, ils sont transmis par les usagers. L'horodatage est quant à lui produit par le système.

La Commission relève que sont collectés également les logs de connexion des usagers et rappelle que leur durée de conservation ne doit pas être inférieure à trois mois ni supérieure à un an. Enfin, la Commission constate que seuls des cookies techniques ou anonymisés sont utilisés sur le téléservice

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***

L'information des personnes concernées est réalisée par le biais d'une mention d'information particulière intégrée dans un document d'ordre général accessible en ligne.

Il est précisé que « *les mentions d'informations sont communiquées aux utilisateurs par le biais de CGUs* ».

Cette dernière étant jointe au dossier, la Commission relève que le contenu de cette mention d'information est conforme aux dispositions de l'article 14 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

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

Le droit d'accès est exercé par voie postale ou par courrier électronique auprès de la Délégation Interministérielle chargée de la Transition Numérique.

S'agissant de l'exercice du droit d'accès par voie électronique, la Commission rappelle qu'une procédure doit 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.

La Commission constate que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 la Loi n° 1.165, modifiée.

## V. Sur les personnes ayant accès au traitement

Le responsable de traitement indique qu'ont accès au traitement :

- les agents de la Direction des Services Numériques tous droits sur le back-office dans le cadre des notifications envoyées aux usagers sur le moyen de contact choisi (sans aucun accès aux données) ;
- les administrateurs de base de données du prestataire, en paramétrage dans le cadre de la maintenance et de l'administration de la plateforme ;
- les usagers, tous droits sur leur profil.

La Commission rappelle qu'en ce qui concerne les prestataires, leurs accès doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat de prestation de service, conformément à l'article 17 de la Loi n° 1.165. De plus, ils sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement.

Elle considère que ces accès sont justifiés.

## VI. Sur les interconnexions avec d'autres traitements

Le responsable de traitement indique que le présent traitement fait l'objet d'une interconnexion avec les traitements légalement mis en œuvre ayant pour finalités respectives :

- « *Fourniture des services de confiance pour l'identité numérique* », afin de permettre l'authentification MConnect ;
- « *Gestion des moyens d'utilisation de l'identité numérique inscrits sur les cartes d'identité monégasque et les cartes de séjour (certificats, code CAN et PUK)* », dénommé « *CLCM* », afin de gérer techniquement les révocations et les alertes en lien avec les dates d'échéances des certificats ;
- « *Gestion du compte permettant aux usagers d'entreprendre et suivre des démarches par téléservices* », dénommé « *MonGuichet.mc* », afin de le mettre à disposition sur MonGuichet.mc.

La Commission constate que ces interconnexions sont conformes aux finalités initiales des traitements susvisés.

## 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.

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.

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 de la session de l'usager en ce qui concerne les données d'identité, le numéro de téléphone de l'usager, et les données d'identification électronique ;
- 1 an pour les données d'horodatage ;
- jusqu'à la suppression du profil par l'utilisateur en ce qui concerne les autres informations, afin qu'il puisse à tout moment révoquer ses certificats.

En ce qui concerne cette dernière durée de conservation, il a été précisé par complément d'informations la mise en place d'un processus organisationnel annuel de suppression des données pour les personnes décédées ou ayant quitté la Principauté (fin de résidence). Les données sont conservées au maximum une année après le décès ou le départ de la Principauté (fin de résidence). L'administrateur du Registre National Monégasque de l'Identité Numérique (RNMIN) a pour mission de procéder annuellement à la suppression des données associées à ces personnes dans le téléservice de révocation. Pour cela, l'administrateur du RNMIN relève les statuts inactifs et suspendus dans le RNMIN. Il lance le processus d'effacement des données associées à ces personnes dans la base de données du téléservice (code de révocation, questions secrètes, données de contact, les données Nom, Prénom, Lieu de naissance, Date de Naissance, Heure de naissance, n'étant jamais présentes dans la base de données du téléservice).

La Commission en prend acte et constate que ces durées de conservation sont conformes aux exigences légales.

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

**Constate que** sont également collectés les logs de connexion des usagers et rappelle que leur durée de conservation ne doit pas être inférieure à trois mois ni supérieure à un an.

**Subordonne** la mise en œuvre du présent traitement à la modification de l'article 8 de l'Ordonnance Souveraine n° 8.696 et de l'article 6 de l'Arrêté Ministériel n° 2021-430 afin que le présent traitement soit exploité en cohérence avec le cadre textuel régissant la matière.

**Rappelle que :**

- une procédure relative au droit d'accès par voie électronique doit 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 ;

- 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 ;

**A la condition de la prise en compte des éléments qui précèdent,**

la Commission de Contrôle des Informations Nominatives **émet un avis favorable à la mise en œuvre, par le Ministre d'Etat, du traitement automatisé d'informations nominatives ayant pour finalité « *Permettre la création et la gestion d'un profil de révocation des certificats électroniques en ligne* ».**

Le Président

Guy MAGNAN