Délibération n° 2022-161 du 16 novembre 2022

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

« *Délivrance de Certificats qualifiés de signature et de cachet électroniques aux personnes dûment habilitées des Organismes du Secteur Public* »

exploité par la Direction des Ressources Humaines et de la Formation de la Fonction Publique (DRHFFP)

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° 1.383 du 2 août 2011 pour une Principauté Numérique, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009, modifiée, fixant les modalités d'application de la Loi n°1.165 du 23 décembre 1993, susvisée ;

Vu l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la Loi n° 1.383 du 2 août 2011 pour une Principauté Numérique, modifiée, relative aux services de confiance ;

Vu l'Ordonnance Souveraine n° 1.635 du 30 avril 2008 fixant les attributions de la Direction des Ressources Humaines et de la Formation de la Fonction Publique, modifiée ;

Vu l'Arrêté Ministériel n° 2020-894 du 18 décembre 2020 portant application des articles 20, 29 et 34 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la Loi n° 1.383 du 2 août 2011 pour une Principauté Numérique, modifiée, relative aux services de confiance ;

Vu l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la Loi n° 1.383 du 2 août 2011 pour une Principauté Numérique, modifiée, relative aux services de confiance ;

Vu l'Arrêté Ministériel n° 2022-429 du 29 juillet 2022 portant application du chiffre 13 de l'article premier portant modification de l'Ordonnance Souveraine n° 1.635 du 30 avril 2008 fixant les attributions de la Direction des Ressources Humaines et de la Formation de la Fonction Publique ;

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 demande d'avis déposée par SEM le Ministre d'Etat le 11 août 2022, concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité la « *Délivrance de Certificats qualifiés de signature et de cachet électroniques aux personnes dûment habilitées des Organismes du Secteur Public* » ;

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 Loi n° 1.482 a modifié la Loi n° 1.383 sur l'économie numérique, qui est ainsi devenue la Loi pour une Principauté Numérique, et qui a introduit à Monaco, la notion de Service de confiance qui comprend, en son sein, la signature électronique et le cachet électronique.

Par délibération n° 2021-114 du 2 juin 2021, la Commission de Contrôle des Informations Nominatives a rendu un avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Délivrance de certificats de signature et cachet électroniques destinés aux personnes morales* » exploité par la Direction de l'Expansion Économique et qui lui permet de proposer aux entreprises monégasques des solutions de signature et de cachet électroniques.

Poursuivant l'objectif de transformation numérique de la Principauté, les Organismes Publics doivent désormais accepter des documents signés électroniquement et peuvent en émettre.

Aussi, la Direction des Ressources Humaines et de la Formation de la Fonction Publique (DRHFFP) a été désignée comme Autorité d'Enregistrement afin de délivrer des Certificats qualifiés de signature et de cachet électroniques aux personnes dûment habilitées des Organismes du Secteur Public.

Il est indiqué par le Responsable de Traitement que la DRHFFP pourra délivrer trois types de certificats aux personnes physiques représentant un organisme du secteur public,

ceux permettant la signature électronique ; ceux qui pourront faire office de cachet et enfin, ceux permettant l'authentification.

Conformément aux dispositions de l'article 7 de la Loi n°1.165 du 23 décembre 1993 modifiée, SEM le Ministre d'Etat soumet ainsi, à l'avis de la Commission, le traitement susvisé.

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

Le présent traitement a pour finalité « *Délivrance de Certificats qualifiés de signature et de cachet électroniques aux personnes dûment habilitées des Organismes du Secteur Public* ».

Il concerne les personnes physiques dûment habilitées représentant les Organismes du Secteur Public de Monaco ainsi que le personnel de l'Administration et du prestataire.

Les fonctionnalités associées au présent traitement sont :

- Habilitation de la personne à détenir un Certificat électronique au sein de l'Etat :

  - l'Autorité du Département (Conseiller - Ministre ou Secrétaire Général du Gouvernement, assisté de son Référent Signature Electronique désigné) qui nomme les fonctions et/ou noms des personnes habilitées à détenir un Certificat électronique dans le cadre de leurs fonctions au sein du Département dans le « *Référentiel des personnes habilitées à détenir des Certificats électroniques au sein de l'Etat* ». Cette opération est réalisée avec l'accompagnement du Référent de Signature Electronique. Ce Référent collecte et gère les demandes d'habilitation. Il se charge de l'inscription dans le Référentiel ainsi que de sa signature et validation par l'Autorité. Ce Référentiel est composé d'un fichier sous forme de tableau sécurisé dans un espace Cryptobox, auquel les agents de la DRHFFP en charge de la délivrance des certificats électroniques ont accès.

- Traitement d'une demande de Certificat par l'Opérateur d'enregistrement (agent de la DRHFFP) :

  - Saisie de la demande dans le guichet en ligne par l'agent de la DRHFFP :
    - Création de l'Organisme du Secteur Public dans le Front Office ;
    - Enregistrement et contrôle des informations du dossier du demandeur dans le Back Office.
  - Validation :
    - Vérification de l'inscription du nom et/ou de la fonction du futur porteur (ou du Responsable du Certificat) dans le « *Référentiel des personnes habilitées à détenir des Certificats électroniques au sein de l'Etat* » du Département ;
    - Vérification des informations et du statut du futur porteur (ou du Responsable du Certificat) dans le dossier RH des fonctionnaires et agents ;
    - Vérification des documents d'identité du futur porteur (ou du Responsable du Certificat) ;
    - Validation de la demande par l'agent lorsque les trois conditions précédentes sont réunies.
  - Émission du certificat : la demande de génération de certificat est opérée par l'agent de la DRHFFP avec l'outil de guichet en ligne. Cet outil génère et envoie un flux de demande de Certificat (format CSR : Certificate Signing

Request), auprès de l'infrastructure de gestion des clés (IGC) nationale. Celle-ci produit le certificat et le renvoie à l'outil guichet en ligne ;
- Impression : production de la carte à puce contenant ledit Certificat, le cas échéant ;
- Contrôle qualité des Certificats : vérification du Certificat contenu dans la puce de la carte, le cas échéant. Dans le cas du cachet serveur, il est envoyé par email au Responsable du Certificat, qui devra valider le contenu du cachet lors de sa mise en œuvre ;
- Remise : remise en main propre au porteur ;
- Fourniture du code d'activation et du code de révocation au porteur ou Responsable du Certificat.

- Renouvellement des Certificats : après expiration (durée de validité des Certificats : 3 ans) ou en cas de compromission du Certificat.

- Révocation (expiration, compromission du Certificat : perte ou vol de la carte, sortie d'un porteur des effectifs de l'Organisme du Secteur Public, mutation d'un porteur, renouvellement d'un Certificat (encore en cours de validité) entraînant la révocation du précédent, fin d'habilitation du porteur dans le « *Référentiel des personnes habilitées à détenir des Certificats électroniques au sein de l'Etat* »).

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 un motif d'intérêt public.

A cet égard, il précise que « *dans le cadre de son programme de transformation digitale, le Gouvernement Princier développe et met à disposition des solutions, procédés et outils numériques à ses usagers et plus généralement à tout acteur présent sur le territoire de la Principauté afin de proposer des services numériques de confiance bénéficiant d'un haut niveau de sécurité et d'intégrité de la donnée* ».

Il indique que « *la délivrance de Certificats qualifiés de signature et de cachet électroniques par la DRHFFP aux personnes dûment habilitées par les Organismes du Secteur Public, permet à la DRHFFP, d'exercer, de manière pertinente et appropriée, la mission dont la Direction est investie en application de l'Ordonnance Souveraine n° 1.635 du 30 avril 2008 fixant les attributions de la DRHFFP, son Arrêté Ministériel d'application ainsi que de manière générale l'ensemble des dispositions du corpus règlementaire prévu par la Loi n° 1.482 du 17 décembre 2019 pour une Principauté Numérique et les textes encadrant la délivrance des Certificats en Principauté* ».

La Commission souligne en ce sens que si la Loi n° 1.383 du 2 août 2011, l'Ordonnance Souveraine n° 8.099 du 16 juin 2020, modifiée relative aux services de confiance et le Référentiel Général de Sécurité pour la Principauté de Monaco annexé à l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 viennent encadrer les conditions de délivrance des cachets électroniques qualifiés et la sécurité y afférente, elle a d'ores et déjà eu l'occasion de relever, dans son avis sur les projets d'Ordonnances Souveraines portant application de la Loi n° 1.483 relative à l'identité numérique et dans sa délibération n° 2021-114, l'apparente perméabilité du périmètre d'application de la Loi pour une Principauté Numérique avec celui de la Loi relative à l'identité numérique. En effet, elle estime que les certificats qualifiés délivrés par la DRHFFP correspondent à la définition de l'article 2 de la Loi sur l'identité numérique. En l'espèce, lesdits certificats sont appelés à contenir les nom et

prénom et l'identifiant unique du porteur et sont délivrés à des personnes physiques dûment habilitées représentant les Organismes du Secteur Public de Monaco. Or, la Commission relève que pour répondre à d'éventuels besoins futurs, il pourra également être délivrés auxdits porteurs des certificats d'authentification qui pourront être provisionnés sur les cartes de certificats de signature. Dès lors, elle estime, de nouveau, qu'il sera nécessaire de lever cette ambiguïté en ce qu'elle risque d'emporter de nombreuses conséquences. La Commission relève toutefois qu'aucune information n'est fournie dans le présent traitement concernant le certificat d'authentification. Elle rappelle qu'elle devra être saisie pour avis, le cas échéant. En outre, s'agissant du certificat de signature électronique, celui-ci est délivré aux personnes habilitées désignées par les Départements. La Commission rappelle que la capacité à engager l'Administration doit être effective, prévue par des bases textuelles claires prévoyant la fonction éligible à en disposer et les délégations de signatures possibles comme par exemple le prévoit l'article 2 de l'Ordonnance Souveraine n° 1.635 du 30 avril 2008 fixant les attributions de la Direction des Ressources Humaines et de la Formation de la Fonction Publique, modifiée.

Sous cette réserve, 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 modifiée.

## III. Sur les informations traitées

Le responsable de traitement indique que les informations nominatives traitées sont :

- identité : civilité, prénom, nom ;
- réponses personnelles pour déblocage code de révocation : réponses personnelles permettant d'identifier une personne à l'origine d'une demande de révocation ;
- adresses et coordonnées : adresse email professionnelle, numéro de téléphone professionnel (mobile ou fixe) ;
- vie professionnelle : nom, adresse et numéro de RCI de l'Organisme du Secteur Public, rôle au sein/ou pour le compte de l'Organisme de Secteur Public ;
- données d'identification électronique : données certificats : Cn = prénom, nom/ nom de l'Organisme du Secteur Public ; SerialNumber : identifiant unique ; SurName = Prénom ; sn = nom ; ou = organization unit : numéro de RCI ; Titre : rôle au sein/ou pour le compte de l'Organisme du Secteur Public ; O : Organization : nom de l'Organisme du Secteur Public ; C = MC (pays) ; adresse email professionnelle ;
- informations temporelles, horodatage : logs de connexion du personnel de l'Administration ;
- documents papier fournis par le demandeur : formulaires signés, copie de la pièce d'identité transmise (carte d'identité ou passeport) ;
- référentiel des personnes habilitées à détenir des Certificats électroniques au sein de l'Etat : Organisme du Secteur Public concerné (service), numéro de RCI de l'Organisme du Secteur Public, fonction, nom, prénom, email professionnel, date d'entrée dans le registre, date d'habilitation, le cas échéant.

La Commission relève par ailleurs que le matricule du porteur du Certificat est également susceptible d'être collecté et en prend acte. Elle relève en outre que les copies des documents d'identité des porteurs sont, de nouveau, collectées lors du renouvellement du certificat. La Commission demande en conséquence que les anciennes copies de ces documents soient supprimées.

Les informations ont pour origine le porteur, à l'exception des données d'identification électroniques et des informations temporelles qui sont générées par le système.

En outre, le Référentiel des personnes habilitées à détenir des Certificats électroniques au sein de l'Etat provient de l'Autorité de Département.

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 modifiée.

## IV. Sur les droits des personnes concernées

- ***Sur l'information préalable des personnes concernées***

L'information préalable des personnes concernées est réalisée par le biais d'une mention d'information particulière intégrée dans un document d'ordre général accessible en ligne sur le site du Gouvernement, à savoir les conditions générales d'utilisation dont les personnes concernées doivent attester avoir pris connaissance et qui doivent être acceptées sur le formulaire d'enregistrement du porteur.

A la lecture de la mention d'information précitée, la Commission constate qu'elle est conforme aux exigences légales.

Elle rappelle par ailleurs que les personnels de l'Administration doivent également être informés de leurs droits.

- ***Sur l'exercice du droit d'accès***

Le droit d'accès est exercé par voie postale ou par voie électronique suite à un renvoi par lien électronique auprès de la DRHFFP.

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° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous cette réserve, elle 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 destinataires et les personnes ayant accès au traitement

Les accès sont définis comme suit :

- les personnels de la DRHFFP (agents de la DRHFFP, également appelés « *opérateurs d'enregistrement* ») : en lecture, en validation, en traitement ;

- l'Officier de sécurité de l'AMSN (rôle de support technique et organisationnel entre le personnel de la DRHFFP et l'administrateur technique prestataire de la solution) : en lecture, en paramétrage, en modification et en suppression ;

- l'administrateur technique prestataire de la solution : en lecture et en configuration. Le responsable de traitement précise que ce dernier « *n'intervient qu'en cas de problème technique à résoudre ou configuration à modifier* » ;

- les personnels de la Direction des Systèmes d'Information (DSI) ou tiers intervenant pour son compte (dans le cadre des missions de maintenance, de développement des applicatifs nécessaires au fonctionnement du site et de sécurité du site et du système d'information de l'Etat) : en lecture et uniquement en cas d'intervention à la demande de l'opérateur de la DRHFFP ou de l'Officier de l'AMSN par le biais de l'ouverture d'un ticket ;

- les personnels de la Direction des Services Numériques : en lecture et uniquement en cas d'intervention à la demande de l'opérateur de la DRHFFP ou du Référent de Signature Electronique du Département.

- l'Autorité du Département et son Référent de Signature Electronique qui ont pour responsabilité d'habiliter les personnes physiques représentant les Organismes du Secteur Public autorisés à bénéficier de certificats électroniques : en lecture et écriture.

En ce qui concerne les 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 doivent être limités à ce qui est strictement nécessaire à l'exécution de leur contrat 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.

Elle considère que ces accès sont justifiés.

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

Le présent traitement fait l'objet de rapprochements avec les traitements légalement mis en œuvre suivants :

- « *Répertoire du Commerce et de l'Industrie* », l'Organisme du Secteur Public concerné devant être répertorié au RCI ;
- « *Gestion de la messagerie professionnelle* » ;
- « *Gestion d'un outil de partage de documents sécurisés avec des partenaires internes et externes à l'Administration Monégasque* » ;
- « *Gestion des dossiers des fonctionnaires et agents relevant de la Fonction Publique et de statuts particuliers* ».

La Commission considère que ces rapprochements 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'observations particulières.

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.

Elle rappelle néanmoins que, conformément à l'article 17 de la Loi n° 1.165, modifiée, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par ce traitement 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.

En outre Commission relève à nouveau que (les entités) de la Principauté (sont) est en cours d'obtention à l'international de la reconnaissance de (leur) sa qualité d'autorité de certification racine de confiance, ce qui peut conduire jusqu'à ladite obtention à des avertissements portés à l'attention des parties utilisatrices. L'utilisation du certificat est alors conditionnée à la volonté des parties utilisatrices de les autoriser.

## VIII. Sur la durée de conservation

Les informations sont conservées 10 ans (durée de vue du Certificat de 3 ans + 7 ans de conservation légale), excepté les Certificats dont la durée de vie ne peut dépasser 3 ans et les informations temporelles qui sont supprimées au bout d'un an.

Ce délai de conservation est justifié par l'Annexe de l'Arrêté Ministériel n° 2020-894 du 18 décembre 2020 portant application des articles 20, 29 et 34 de l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la Loi n° 1.383 du 2 août 2011 pour une Principauté Numérique, modifiée, relative aux services de confiance qui prévoit que « *les dossiers d'enregistrement doivent être conservés pendant sept (7) ans après la fin de validité du certificat faisant l'objet d'une demande* ».

Si la Commission considère que ces durées de conservation sont conformes aux exigences légales, elle regrette de ne pas avoir été consultée pour avis relativement à ces durées de conservation, à l'instar de la CNIL sur les référentiels de l'ANSSI.

## Après en avoir délibéré, la Commission

**Demande** qu'en cas de renouvellement des certificats, les anciennes copies des documents d'identité soient supprimées.

**Rappelle que :**

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switch, routeurs, pares-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 ;

- les personnels de l'Administration doivent également être informés de leurs droits ;

- la capacité à engager l'Administration doit être effective, prévue par des bases textuelles claires prévoyant la fonction éligible à en disposer et les délégations de signatures possibles.

**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.

**Estime** que le périmètre des Lois n° 1.483 et 1.383 doit être précisé afin que les acteurs concernés puissent de manière certaine connaitre l'étendue de leurs obligations.

**Constate** que la Principauté est en cours d'obtention à l'international de la reconnaissance de sa qualité d'autorité de certification racine de confiance, ce qui peut conduire, jusqu'à ladite obtention, à des alertes de sécurité portées à l'attention des parties utilisatrices des certificats. Leur utilisation est alors conditionnée à la volonté des parties utilisatrices de les autoriser, ce qui est de nature à brouiller le message de confiance dans le numérique et à en affecter ainsi l'utilisation effective.

**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, par le Ministre d'Etat, du traitement automatisé d'informations nominatives ayant pour finalité la *« Délivrance de Certificats qualifiés de signature et cachet électroniques aux personnes dûment habilitées des Organismes du Secteur Public »***.

Le Président

Guy MAGNAN