

Délibération n° 2021-114 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

« *Délivrance de certificats de signature et cachet électroniques destinés aux personnes morales* »

exploité par la Direction de l'Expansion Economique

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 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° 1.144 du 26 juillet 1991 concernant l'exercice de certaines activités économiques et juridiques ;

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 n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et les administrés ;

Vu l'Ordonnance Souveraine n° 11.986 du 2 juillet 1996 portant création de la Direction de l'Expansion Economique, 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 demande d'avis déposée par le Ministre d'Etat, le 25 mars 2021, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité le « *Délivrance de certificats de signature et cachet électroniques destinés aux personnes morales* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 21 mai 2021, 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 2 juin 2021 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.

Les signatures électroniques sont définies comme « *des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer* » et les cachets électroniques comme « *des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières* ».

A cet égard, le responsable de traitement précise dans la demande d'avis que « *la signature et le cachet électronique sont, à un document numérique, ce que la signature manuscrite et le tampon d'entreprise sont à un document papier* ».

Afin de répondre à la nécessité de proposer ces solutions aux entreprises monégasques, l'Ordonnance Souveraine n° 8.450 du 24 décembre 2020 a modifiée l'Ordonnance Souveraine n° 11.986 portant création de la Direction de l'Expansion Economique (DEE) afin d'étendre les missions de cette dernière et de lui attribuer le statut de tiers de confiance chargé de concevoir, de délivrer et de gérer des certificats électroniques qualifiés.

Il est indiqué par le responsable de traitement que la DEE pourra délivrer trois types de certificats aux personnes physiques représentant une personne morale : ceux permettant la signature électronique ; ceux qui pourront faire office de cachet ; ceux permettant l'authentification et qui permettront dans de futurs usages d'accéder aux téléservices de l'Administration.

Conformément aux dispositions de l'article 7 de la Loi n° 1.165 du 23 décembre 1993 modifiée, le Ministre d'Etat soumet ainsi, à l'avis de la Commission, le traitement ayant pour finalité « *Délivrance de certificats de signature et cachet électroniques destinés aux personnes morales* ».

I. Sur la finalité et les fonctionnalités du traitement

Le présent traitement a pour finalité « *Délivrance de certificats de signature et cachet électroniques destinés aux personnes morales* ».

Il concerne les personnes physiques représentant des personnes morales situées en Principauté (le représentant légal de la société, le porteur du certificat qui peut être un salarié comme un tiers, le mandataire de certification qui peut être un salarié de la société comme un tiers) et les personnels « *opérateurs d'enregistrement* » de la DEE dans le cadre de leurs missions de délivrance des certificats.

Les fonctionnalités sont :

- Traitement d'une demande de certificat par l'opérateur d'enregistrement :
 - Saisie de la demande : enregistrement des informations du dossier du demandeur dans l'outil de guichet en ligne par l'agent de la DEE ;
 - Validation : vérification des documents d'identité et de l'immatriculation sur les répertoires et registres gérés par la DEE et validation de la demande par l'agent ;
 - Paiement : acquittement des droits ;
 - Emission du certificat : la demande de génération de certificat est opérée par l'agent de la DEE avec l'outil de guichet en ligne. Cet outil génère et envoie un flux de demande de certificat auprès de l'Autorité de certification de la DEE. Celle-ci produit le certificat et le renvoie à l'outil guichet en ligne ;
 - Impression : production de la carte à puce contenant ledit certificat ;
 - Contrôle qualité des certificats : vérification du certificat contenu dans la puce de la carte ;
 - Remise : remise en main propre au porteur ou au mandataire de certification ;
 - Fourniture du code d'activation et du code de révocation ;
- 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, radiation de la société des répertoires et registres gérés par la Direction de l'Expansion Economique, sortie d'un porteur des effectifs de la société, décès d'un porteur, renouvellement d'un certificat (encore en cours de validité) entraînant la révocation du précédent).

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 le respect d'une obligation légale à laquelle il est soumis et par la réalisation d'un intérêt légitime qu'il poursuit et qui ne méconnaît ni l'intérêt, ni les droits et libertés fondamentaux des personnes concernées.

A cet égard, il précise que la section signature et cachet électroniques du Pôle Administration Générale de la DEE est chargée, en application de l'article 2 l'Ordonnance Souveraine n° 11.986 portant création de la Direction de l'Expansion Economique, modifiée par l'Ordonnance Souveraine n° 8.450 du 24 décembre 2020, « *de la délivrance des certificats*

qualifiés de signature et de cachet électroniques en tant que prestataire de services de confiance au sens de la réglementation monégasque en vigueur en la matière ».

En outre, la Loi n° 1.383 pour une Principauté Numérique, 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, le Référentiel Général de Sécurité pour la Principauté de Monaco annexé à l'Arrêté Ministériel n° 2020-461 du 6 juillet 2020 fixant les conditions d'application de la Loi n° 1.383 relative aux services de confiance, viennent encadrer les conditions de délivrances de cachets électroniques qualifiés et la sécurité y afférente.

La Commission relève toutefois, comme elle a pu le développer dans son avis sur les projets d'Ordonnances Souveraines portant application de la Loi n° 1.483 relative à l'identité numérique, 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 DEE correspondent à la définition de l'article 2 de la Loi sur l'identité numérique qui dispose que « *l'identité numérique d'une personne est constituée de données d'identification personnelle sous la forme d'un identifiant numérique représentant de manière univoque une personne physique ou une personne morale* ». Lesdits certificats contiennent notamment le nom, prénom, nom de l'entreprise sous la forme d'un identifiant numérique représentant de manière univoque une personne physique. Ils sont délivrés à des personnes morales (leurs représentants) sur la base d'informations disponibles sur un « *registre* » public, et le périmètre de la demande d'avis expose que la DEE délivre « *les certificats d'authentification d'une personne physique représentant une personne morale qui permettront dans les futurs usages à la personne physique de s'authentifier sur les téléservices de l'Administration* », c'est-à-dire les moyens d'identification au sens de la Loi relative à l'identité numérique. La Commission relève toutefois qu'aucune information n'est fournie dans le traitement concernant le certificat d'authentification.

La Commission estime qu'il serait nécessaire de lever cette ambiguïté en ce qu'elle emporte de nombreuses conséquences : si la Loi relative à l'identité numérique s'applique, les personnes doivent dès lors être inscrites sur le Registre National de l'Identité Numérique par le Fournisseur d'identité, le certificat d'authentification doit être défini selon les niveaux de garantie définis à l'article 3 de la Loi n° 1.483 relative à l'identité numérique, etc.

Sous cette réserve, la Commission considère que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 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 du code de révocation : réponses personnelles permettant d'identifier une personne à l'origine d'une demande de révocation ;
- adresses et coordonnées : adresse e-mail professionnelle, numéro de téléphone professionnel (fixe ou mobile) ;
- vie professionnelle : dénomination sociale de l'entreprise, numéro de RCI, rôle au sein de ou pour le compte de l'entreprise, adresse du siège social ;
- données d'identification électronique : données certificats : Cn = Prénom NOM ; SerialNumber (numéro de certificat) ; givenName=Prénom ; sn = NOM ; ou =

organization unit : numéro de RCI ; Title : rôle au sein de ou pour le compte de l'entreprise ; O : Organization : nom de l'entreprise ; C=MC (pays) ; adresse email professionnelle ;

- informations temporelles : horodatages, etc. : logs de connexion du personnel de l'Administration ;
- documents papier fournis par le demandeur : formulaires signés, copie des pièces d'identité transmises (carte d'identité, passeport ou carte de séjour).

Les informations ont pour origine le représentant légal, le porteur ou le mandataire de certification, excepté les informations temporelles et les données d'identification électronique qui sont générées par le système.

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 préalable des personnes concernées est réalisée par le biais d'une mention particulière intégrée dans un document d'ordre général accessible en ligne sur le site du Gouvernement, à savoir les conditions générales d'utilisation de la démarche que les personnes doivent attester avoir pris connaissance et accepter 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. Il est également explicité que le représentant légal et le futur porteur doivent en avoir pris connaissance, couvrant l'ensemble des personnes concernées en lien avec l'Administration.

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

➤ *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 voie électronique suite à un renvoi par lien électronique, auprès de la Direction de l'Expansion Economique.

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 ainsi 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 Direction de l'Expansion Economique : lecture, validation, traitement ;
- Officier de Sécurité de l'AMSN : en lecture, paramétrage, en modification et en suppression ;
- Les personnels de la Direction des Systèmes d'Information ou tiers intervenant pour son compte : en lecture dans le cas d'une intervention support technique à la demande de l'opérateur de la DEE ou de l'Officier de Sécurité de l'AMSN ;
- Administrateur technique du prestataire : en lecture et en configuration. Le prestataire n'intervient qu'en cas de problème technique à résoudre ou d'une configuration à modifier.

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 les 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* », afin de comparer et corréler les informations renseignées par les demandeurs et les informations connues de la DEE, et si ces derniers sont donc éligibles à la délivrance de certificats ;
- « *Gestion de la messagerie professionnelle* » afin de recevoir les notifications de l'applicatif et correspondre avec les demandeurs.

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'observation.

La Commission relève que le prestataire a été qualifié par l'AMSN et figure sur la liste des produits qualifiés.

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 relève 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.

Elle 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

Les informations sont conservées 10 ans (durée de vie de 3 ans du certificat + 7 ans), 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 de la 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 :

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

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 connaître 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. La Commission estime que cela 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 « Délivrance de certificats de signature et cachet électroniques destinés aux personnes morales ».**

Le Président

Guy MAGNAN