Ordonnance Souveraine n° 6.525 du 16 août 2017 portant application des articles 18, 19 et 25 de la loi n° 1.383 du 2 août 2011 sur l'économie numérique, modifiée

ALBERT II
PAR LA GRÂCE DE DIEU
PRINCE SOUVERAIN DE MONACO

Vu la Constitution ;

Vu la loi n° 1.383 du 2 août 2011 sur l'économie numérique, modifiée ;

Vu Notre Ordonnance n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée ;

Vu Notre Ordonnance n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée ;

Vu le Code civil, notamment son article 1163-3 ;

Vu la délibération du Conseil de Gouvernement en date du 26 juillet 2017 qui Nous a été communiquée par Notre Ministre d'État ;

AVONS ORDONNÉ ET ORDONNONS :

ARTICLE PREMIER.

Au sens de la présente ordonnance, on entend par :

« **identification électronique** » : données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale ;

« **schéma d'identification électronique** » : dispositif pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales. Ce dispositif détermine les spécifications des niveaux de garantie des moyens d'identification électronique délivrés dans le cadre dudit schéma ;

« **signature électronique** » : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies au troisième alinéa de l'article 1163-3 du Code civil ;

« **signature électronique avancée** » : une signature électronique qui satisfait, en outre, aux exigences suivantes :

a) être liée au signataire de manière univoque ;
b) permettre d'identifier le signataire ;
c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et
d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ;

« **signataire** » : une personne physique qui crée une signature électronique ;

« **données de création de signature électronique** » : des données uniques qui sont utilisées par le signataire pour créer une signature électronique ;

« **dispositif de création de signature électronique** » : un dispositif logiciel ou matériel servant à créer une signature électronique ;

« **dispositif de création de signature électronique qualifié** » : un dispositif de création de signature électronique qui satisfait aux exigences définies par arrêté ministériel ;

« **cachet électronique** » : une signature électronique pour une personne morale ;

« **données de validation** » : les données qui servent à valider une signature électronique ;

« **validation** » : le processus de vérification et de confirmation de la validité d'une signature ;

« **certificat électronique** » : attestation électronique qui associe les données de validation d'une signature ou d'un cachet électronique à une personne physique ou morale et confirme au moins le nom ou le pseudonyme de cette personne ;

« **certificat électronique qualifié** » : certificat électronique répondant aux exigences définies à l'article 5 ;

« **service de confiance** » : un service de confiance est un service électronique qui consiste :

- - en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, et de certificats électroniques ; ou
- - en la conservation de signatures électroniques, de cachets électroniques ou des certificats électroniques relatifs à ces services ;

« **prestataire de service de confiance** » : un prestataire de services de confiance est une personne physique ou morale qui fournit un ou plusieurs services de confiance ;

« **horodatage électronique** » : acte qui consiste en l'apposition de la date d'expédition résultant d'un procédé fiable lors d'un envoi par courrier électronique ou d'un envoi recommandé électronique.

ART. 2.

L'identification électronique comporte trois niveaux de garantie :

- le niveau de garantie « **faible** », qui renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique accordant un degré limité de fiabilité à l'identité revendiquée ou prétendue d'une personne, et qui est caractérisé par des spécifications techniques, des normes et des procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité ;
- le niveau de garantie « **substantiel** », qui renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique accordant un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne, et qui est caractérisé par des spécifications techniques, des normes et des procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité ;
- le niveau de garantie « **élevé** », qui renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique accordant un niveau de fiabilité à l'identité revendiquée ou prétendue d'une personne plus élevé qu'un moyen d'identification électronique ayant le niveau de garantie substantiel, et qui est caractérisé par des spécifications techniques, des normes et des procédures y afférents, y compris les contrôles techniques, dont l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

Un procédé fiable d'identification doit respecter les spécifications techniques, normes, procédures et contrôles techniques fixés par arrêté ministériel.

ART. 3.

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique avancée, établie grâce à un dispositif de création de signature électronique qualifié et que la validation de cette signature repose sur l'utilisation d'un certificat électronique qualifié. Une telle signature électronique est une signature électronique qualifiée.

La signature électronique comporte trois niveaux de fiabilité : **simple**, **avancé** et **qualifié**.

Les exigences devant être respectées à chacun des trois niveaux ainsi que les normes, procédures et contrôles techniques applicables aux dispositifs de création de signature électronique sont déterminés par arrêté ministériel.

La conformité des dispositifs de création de signature électronique fait l'objet d'une certification du directeur de l'Agence Monégasque de la Sécurité Numérique.

Les modalités de cette certification sont publiées par arrêté ministériel.

ART. 4.

Le cachet électronique comporte trois niveaux de fiabilité : **simple**, **avancé** et **qualifié**.

Les exigences qui doivent être respectées à chacun des trois niveaux ainsi que les normes, procédures et contrôles techniques applicables aux dispositifs de création de cachet électronique sont déterminés par arrêté ministériel.

La conformité des dispositifs de création de cachet électronique fait l'objet d'une certification du directeur de l'Agence Monégasque de Sécurité Numérique. Les modalités de ladite certification sont publiées par arrêté ministériel.

ART. 5.

Un certificat de signature électronique associant les données de validation d'une signature à une personne physique et d'un cachet électronique à une personne morale comporte deux niveaux de fiabilité : **simple** et **qualifié**.

Un certificat de signature électronique peut être révoqué ou temporairement suspendu.

La validité des certificats de signature électronique ainsi que les normes, procédures et contrôles techniques applicables aux certificats de signature électronique sont déterminés par arrêté ministériel.

ART. 6.

L'horodatage électronique comporte deux niveaux de fiabilité : **simple** et **qualifié**.

Les exigences qui doivent être respectées à chacun des deux niveaux ainsi que les normes, procédures et contrôles techniques applicables aux dispositifs de création d'horodatage électronique sont déterminés par arrêté ministériel.

La conformité des dispositifs de création d'horodatage électronique fait l'objet d'une certification du directeur de l'Agence Monégasque de la Sécurité Numérique. Les modalités de la certification sont publiées par arrêté ministériel.

ART. 7.

Les services de confiance comportent trois niveaux de fiabilité : **simple**, **avancé** et **qualifié**, sous réserve des dispositions de l'article 6.

Les exigences qui doivent être respectées à chacun des trois niveaux ainsi que les normes, procédures et contrôles techniques applicables aux services de confiance sont déterminés par arrêté ministériel.

ART. 8.

Les prestataires de services de confiance comportent deux niveaux de fiabilité : **simple** et **qualifié**.

Les exigences qui doivent être respectées à chacun des deux niveaux ainsi que les normes, procédures et contrôles techniques applicables aux prestataires de services de confiance sont déterminés par arrêté ministériel.

ART. 9.

Un Référentiel Général de Sécurité, garantissant l'usage de procédés fiables dans l'utilisation des services électroniques qu'ils proposent, en définissant les exigences, règles techniques et de sécurité, ainsi que les différents niveaux de garantie pour l'identité électronique, la signature électronique, le cachet électronique, le certificat électronique, l'horodatage électronique, les services de confiance et les prestataires de services de confiance, est déterminé par arrêté ministériel.

ART. 10.

Notre Secrétaire d'État, Notre Directeur des Services Judiciaires et Notre Ministre d'État sont chargés, chacun en ce qui le concerne, de l'exécution de la présente ordonnance.

Donné en Notre Palais à Monaco, le seize août deux mille dix-sept.

ALBERT.
Par le Prince,
P/Le Secrétaire d'État :
Le Président du Conseil d'État :
PH. NARMINO.