Loi du Pays n° 2017-30 du 2 novembre 2017 relative à la dématérialisation des actes des autorités administratives et aux téléservices (erratum publié au JOPF n° 89 NC du 7 novembre 2017 à la page 16424)

(NOR : SGG1621556LP)
Paru in extenso au journal officiel n°74 NS du 02/11/2017 à la page 7058 dans la partie Lois du pays

Version en vigueur au 08/11/2017

Après avis du Conseil économique, social et culturel de la Polynésie française,
L'assemblée de la Polynésie française a adopté ;
Vu l'attestation de non-recours du Conseil d'Etat formulée par courrier n° 914 du 24 octobre 2017 ;
Le Président de la Polynésie française promulgue la loi du pays dont la teneur suit :

SECTION I - DISPOSITIONS GÉNÉRALES

Article LP. 1er

Au sens de la présente loi du pays, on entend par :

1° "autorité administrative", la Polynésie française, ses établissements publics, les autorités administratives indépendantes, les organismes de protection sociale et les autres organismes et personnes de droit public et de droit privé chargés d'une mission de service public administratif ;

2° "système d'information", tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives ;

3° "téléservice", tout système d'information permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives et aux agents des autorités administratives d'en assurer le traitement et le suivi ;

4° "usager", toute personne physique ou toute personne morale de droit privé, à l'exception de celles qui sont chargées d'une mission de service public lorsqu'est en cause l'exercice de cette mission ;

5° "partie utilisatrice", une personne physique ou morale qui se fie à un service de confiance ;

6° "signature électronique", 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 ;

7° "signature électronique avancée", une signature électronique qui satisfait aux exigences énoncées à l'article LP. 24 ;

8° "signature électronique qualifiée", une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié, et qui repose sur un certificat qualifié de signature électronique ;

9° "données de création de signature électronique", des données uniques qui sont utilisées par le signataire pour créer une signature électronique ;

10° "certificat de signature électronique", une attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne ;

11° "certificat qualifié de signature électronique", un certificat de signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe 1 ;

12° "dispositif de création de signature électronique", un dispositif logiciel ou matériel configuré servant à créer une signature électronique ;

13° "dispositif de création de signature électronique qualifié", un dispositif de création de signature électronique qui satisfait aux exigences énoncées à l'annexe 2 ;

14 "service de confiance", un service électronique normalement fourni contre rémunération qui consiste :

a) En la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ou

b) En la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services ;

15° "service de confiance qualifié", un service de confiance qui satisfait aux exigences de la présente loi du pays ;

16° "prestataire de services de confiance", une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié ;

17° "prestataire de services de confiance qualifié", un prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et qui figure sur une liste de référence fixée par le conseil des ministres ;

18° "produit de sécurité", un dispositif matériel ou logiciel, ou les composants correspondants du dispositif matériel ou logiciel, qui sont destinés à être utilisés pour la fourniture de services de confiance ;

19° "cachet électronique", 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 ;

20° "cachet électronique avancé", un cachet électronique qui satisfait aux exigences énoncées à l'article LP. 31 ;

21° "cachet électronique qualifié", un cachet électronique avancé qui est créé à l'aide d'un dispositif électronique qualifié et qui repose sur un certificat qualifié de cachet électronique ;

22° "données de création de cachet électronique", des données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique ;

23° "certificat de cachet électronique", une attestation électronique qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne ;

24° "certificat qualifié de cachet électronique", un certificat de cachet électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe 3 ;

25° "dispositif de création de cachet électronique", un dispositif logiciel ou matériel configuré utilisé pour créer un cachet électronique ;

26° "dispositif de création de cachet électronique qualifié", un dispositif de création de cachet électronique qui satisfait aux exigences fixées à l'annexe 2 ;

27° "horodatage électronique", des données sous forme électronique qui associent d'autres données sous forme électronique, à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant ;

28° "horodatage électronique qualifié", un horodatage électronique qui satisfait aux exigences fixées à l'article LP. 37 ;

29° "service d'envoi recommandé électronique", un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée ;

30° "service d'envoi recommandé électronique qualifié", un service d'envoi recommandé électronique qui satisfait aux exigences fixées à l'article LP. 39.

31° "données de validation", des données qui servent à valider une signature électronique ou un cachet électronique ;

32° "validation", le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique.

Art. LP. 2

La présente loi du pays est applicable aux autorités administratives visées à l'article LP. 1er.

Elle n'est pas applicable à la dématérialisation des échanges :

1° Prévus et organisés par la loi organique statutaire n° 2004-192 du 27 février 2004 entre institutions de la Polynésie française ;

2° Relatifs à la gestion des ressources humaines au sein d'une autorité administrative.

Art. LP. 3

Les écrits et documents échangés au sein d'une autorité administrative, entre autorités administratives et entre une autorité administrative et ses usagers peuvent être remplacés par des écrits et documents électroniques dans les conditions fixées par la présente loi du pays.

Art. LP. 4

Les décisions des autorités administratives peuvent faire l'objet d'une signature électronique dans les conditions prévues par la présente loi du pays.

SECTION II - DES ÉCHANGES DE DONNÉES AU SEIN D'UNE AUTORITÉ ADMINISTRATIVE

Art. LP. 5

Sous réserve des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les services d'une autorité administrative peuvent échanger entre eux toutes les informations ou données strictement nécessaires pour traiter une demande présentée par un usager ou une déclaration transmise par celui-ci en application d'un texte législatif ou réglementaire après avoir obtenu l'accord exprès de la personne concernée.

Ces échanges interviennent dans le respect de règles contribuant à la sécurité des informations, y compris par voie électronique.

Un service d'une autorité administrative chargé de traiter une demande ou une déclaration mentionnée à l'alinéa précédent fait connaître à la personne concernée les informations ou données qui sont nécessaires à cette fin et celles qu'elle se procure directement auprès d'autres services, qui en sont à l'origine ou qui les détiennent en vertu de leur mission.

L'usager est informé du droit d'accès et de rectification dont dispose chaque personne intéressée sur les informations et données mentionnées au présent article.

Art. LP. 6

Lorsque les informations ou données nécessaires pour traiter une demande présentée par un usager ou une déclaration transmise par celui-ci, en application d'un texte législatif ou réglementaire, peuvent être obtenues directement auprès d'un autre service, une attestation sur l'honneur de l'usager de l'exactitude des informations déclarées se substitue à la production de pièces justificatives.

Art. LP. 7

Lorsque les informations ou données nécessaires pour traiter la demande ou la déclaration ne peuvent être obtenues directement par un service auprès d'un autre service, il revient à la personne concernée de les communiquer audit service.

Art. LP. 8

Les échanges prévus dans le cadre de la présente section peuvent être mis en œuvre dans le cadre de téléservices dans les conditions fixées par la présente loi du pays.

Art. LP. 9

Un arrêté pris en conseil des ministres détermine :

1° Les domaines et procédures concernés par les échanges d'informations et de données ;

2° Les modalités des échanges d'informations entre services ;

3° La liste des services auprès desquelles la demande de communication s'effectue en fonction du type d'informations ou de données ;

4° Les informations ou données qui ne peuvent faire l'objet de ces échanges ;

5° Le délai de conservation des informations et données applicables à chaque système ;

6° La liste des pièces dont la fourniture n'est plus nécessaire ;

7° Le délai au terme duquel, en l'absence de communication de l'information ou de la donnée nécessaire pour traiter une demande, il appartient à l'usager de communiquer au service ladite information ou donnée.

SECTION III - DES ÉCHANGES DE DONNÉES ENTRE AUTORITÉS ADMINISTRATIVES

Art. LP. 10

Les articles LP. 5 à LP. 9 de la présente loi du pays sont applicables aux échanges de données électroniques entre autorités administratives, lesquels interviennent dans le respect des règles de sécurité et d'interopérabilité prévues aux articles LP. 20 et LP. 46.

SECTION IV - DES ÉCHANGES DE DONNÉES ÉLECTRONIQUES ENTRE UNE AUTORITÉ ADMINISTRATIVE ET SES USAGERS DANS LE CADRE D'UN TÉLÉSERVICE

Art. LP. 11

Les autorités administratives peuvent mettre en place un ou plusieurs téléservices dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et des règles de sécurité, d'accessibilité et d'interopérabilité prévues aux articles LP. 20, LP. 45 et LP. 46.

Art. LP. 12

Lorsqu'elle met en place un ou plusieurs téléservices, l'autorité administrative rend accessibles leurs modalités d'utilisation, notamment les modes de communication possibles. Ces modalités s'imposent aux usagers.

Art. LP. 13

Tout usager peut, adresser à une autorité administrative, dans le cadre d'un téléservice, une demande, une déclaration, un document ou une information, ou lui répondre par la même voie.

Cette autorité administrative est régulièrement saisie et traite la demande, la déclaration, le document ou l'information sans lui demander la confirmation ou la répétition de son envoi sous une autre forme.

Art. LP. 14

Tout envoi à une autorité administrative par voie électronique dans le cadre d'un téléservice au sens de la présente loi du pays fait l'objet d'un accusé de réception électronique et, lorsque celui-ci n'est pas instantané, d'un accusé d'enregistrement électronique.

Ils sont émis selon un procédé conforme aux règles fixées par le référentiel général de sécurité mentionné à l'article LP. 20.

Les conditions et délais d'émission de l'accusé de réception et de l'accusé d'enregistrement ainsi que les indications devant y figurer sont déterminés par arrêté pris en conseil des ministres.

L'autorité administrative n'est pas tenue de respecter l'obligation prévue à l'alinéa premier pour les envois abusifs, notamment par leur nombre ou leur caractère répétitif ou systématique, ou les envois susceptibles de porter atteinte à la sécurité de son système d'information.

Après en avoir, si possible, informé la source des envois en cause, un système d'information peut être configuré pour bloquer la réception des envois provenant de sources identifiées comme ayant émis un nombre significatif d'envois abusifs ou émis des envois susceptibles de porter atteinte à la sécurité du système d'information.

Art. LP. 15

Toute personne tenue de respecter une date limite ou un délai pour présenter une demande, déposer une déclaration ou produire un document auprès d'une autorité administrative peut, lorsqu'il existe un téléservice, satisfaire à cette obligation au plus tard à la date prescrite par l'utilisation de ce téléservice. Dans ce cas, fait foi la date figurant sur l'accusé de réception ou, le cas échéant, sur l'accusé d'enregistrement adressé à l'usager par ce téléservice conformément aux dispositions de l'article LP. 14.

Ces dispositions ne sont pas applicables aux procédures pour lesquelles la présence personnelle du demandeur est exigée en application d'une disposition particulière.

Art. LP. 16

Lorsqu'un usager doit adresser un document à l'autorité administrative par lettre recommandée, cette formalité peut, lorsqu'il existe un téléservice, être accomplie par l'utilisation de ce téléservice.

Lorsque l'autorité administrative doit notifier un document à une personne par lettre recommandée, cette formalité peut être accomplie par l'utilisation d'un téléservice, permettant de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si le document a été remis. L'accord exprès de l'intéressé doit être préalablement recueilli.

Art. LP. 17

Le conseil des ministres peut écarter l'usage d'un téléservice pour certaines démarches administratives pour des motifs de bonne administration ou lorsque la présence personnelle du demandeur apparaît nécessaire.

Art. LP. 18

I. Sauf dans les cas où un régime de décision implicite est institué par une autre réglementation, le silence gardé par l'autorité administrative sur une demande pendant plus de deux mois à compter de la date de réception par l'usager de l'accusé de réception ou de l'accusé d'enregistrement prévu à l'article LP. 14 vaut décision de rejet.

II. Cet article n'est pas applicable aux organismes de protection sociale.

Art. LP. 19

Par dérogation à l'article LP. 4 de la présente loi du pays, sont dispensées de la signature de leur auteur, dès lors qu'ils comportent ses prénom, nom et qualité ainsi que la mention du service de l'autorité administrative auquel celui-ci appartient, les décisions émanant des autorités administratives qui sont notifiées aux usagers par l'intermédiaire d'un téléservice ainsi que les actes préparatoires à ces actes ou décisions.

SECTION V - DE LA SÉCURITÉ DES ÉCHANGES ÉLECTRONIQUES ENTRE LES AUTORITÉS ADMINISTRATIVES ET ENTRE UNE AUTORITÉ ADMINISTRATIVE ET SES USAGERS

Art. LP. 20

Un référentiel général de sécurité, approuvé par le conseil des ministres, fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique telles que les fonctions d'identification, de signature électronique, de confidentialité, d'intégrité et d'horodatage.

Art. LP. 21

Lorsqu'une autorité administrative met en place un système d'information, elle détermine les fonctions de sécurité nécessaires pour protéger ce système. Pour les fonctions de sécurité traitées par le référentiel général de sécurité, elle fixe le niveau de sécurité requis parmi les niveaux prévus et respecte les règles correspondantes.

L'autorité administrative procède à l'homologation de son système d'information conformément aux objectifs de sécurité fixés par le référentiel général de sécurité.

Art. LP. 22

Les produits de sécurité et les prestataires de services de confiance peuvent obtenir une qualification qui atteste de leur conformité à un niveau de sécurité du référentiel général de sécurité.

Cette qualification correspond à la qualification délivrée par les autorités de métropole en application de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Un arrêté pris en conseil des ministres précise les modalités d'application de la présente section et fixe la liste de référence des produits et prestataires de service de confiance qualifiés par référence à la liste dressée par les autorités nationales dans le cadre de la mise en œuvre du référentiel général de sécurité métropolitain.

SECTION VI - EFFETS JURIDIQUES

PARAGRAPHE I - SIGNATURES ÉLECTRONIQUES

Art. LP. 23

L'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.

L'effet juridique d'une signature électronique qualifiée est équivalent à celui d'une signature manuscrite.

L'écrit électronique a la même force probante que l'écrit sur support papier dès lors qu'il remplit les conditions prévues aux articles LP. 25 et LP. 26 de la présente loi du pays.

Art. LP. 24

Une signature électronique avancée satisfait aux exigences suivantes :

1° Etre liée au signataire de manière univoque ;

2° Permettre d'identifier le signataire ;

3° 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 ;

4° Etre liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Art. LP. 25

1° Les certificats qualifiés de signature électronique satisfont aux exigences fixées à l'annexe 1 ;

2° Si un certificat qualifié de signature électronique a été révoqué après la première activation, il perd sa validité à compter du moment de sa révocation et il ne peut en aucun cas recouvrer son statut antérieur.

Art. LP. 26

Les dispositifs de création de signature électronique qualifiés respectent les exigences fixées à l'annexe 2.

Art. LP. 27

Le processus de validation d'une signature électronique qualifiée confirme la validité d'une signature électronique qualifiée à condition que :

1° Le certificat sur lequel repose la signature ait été, au moment de la signature, un certificat qualifié de signature électronique conforme à l'annexe 1 ;

2° Le certificat qualifié ait été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ;

3° Les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice ;

4° L'ensemble unique de données représentant le signataire dans le certificat soit correctement fourni à la partie utilisatrice ;

5° La signature électronique ait été créée par un dispositif de création de signature électronique qualifié ;

6° L'intégrité des données signées n'ait pas été compromise ;

7° Les exigences prévues à l'article LP. 24 aient été satisfaites au moment de la signature.

Le système utilisé pour valider la signature électronique qualifiée fournit à la partie utilisatrice le résultat correct du processus de validation et permet à celle-ci de détecter tout problème pertinent relatif à la sécurité.

Art. LP. 28

Un service de validation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui :

1° Fournit une validation en conformité avec l'article LP. 27 à l'exception du dernier alinéa ;

2° Permet aux parties utilisatrices de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire qui fournit le service de validation qualifié.

Art. LP. 29

Un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

PARAGRAPHE II - CACHETS ÉLECTRONIQUES

Art. LP. 30

L'effet juridique et la recevabilité d'un cachet électronique comme preuve en justice ne peuvent être refusés au seul motif que ce cachet se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du cachet électronique qualifié.

Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles le cachet électronique qualifié est lié.

Art. LP. 31

Un cachet électronique avancé satisfait aux exigences suivantes :

1° Etre lié au créateur du cachet de manière univoque ;

2° Permettre d'identifier le créateur du cachet ;

3° Avoir été créé à l'aide de données de création de cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer un cachet électronique ;

4° Etre lié aux données auxquelles il est associé de telle sorte que toute modification ultérieure des données soit détectable.

Art. LP. 32

1° Les certificats qualifiés de cachet électronique satisfont aux exigences fixées à l'annexe 3 ;

2° Si un certificat qualifié de cachet électronique a été révoqué après la première activation, il perd sa validité à compter du moment de sa révocation et il ne peut en aucun cas recouvrer son statut antérieur.

Art. LP. 33

Les dispositifs de création de cachet électronique respectent les exigences fixées à l'annexe 2.

Art. LP. 34

Les articles LP. 27, LP. 28 et LP. 29 s'appliquent à la validation et à la conservation des cachets électroniques.

PARAGRAPHE III - EXIGENCES APPLICABLES AUX PRESTATAIRES DE SERVICES DE CONFIANCE QUALIFIÉS ET NON QUALIFIÉS

Art. LP. 35

I - Exigences communes applicables aux prestataires de services de confiance qualifiés et non qualifiés :

Un prestataire de services de confiance qualifié et non qualifié :

1° Prend les mesures techniques et organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents ;

2° Notifie, dans les meilleurs délais et en tout état de cause dans un délai de vingt-quatre heures après en avoir eu connaissance, à l'autorité nationale de contrôle, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de confiance a été fourni, le prestataire de services de confiance notifie aussi, dans les meilleurs délais, à la personne physique ou morale l'atteinte à la sécurité ou la perte d'intégrité.

II - Exigences spécifiques applicables aux prestataires de services de confiance qualifiés :

Un prestataire de services de confiance qualifié qui fournit des services de confiance qualifiés doit :

1° Lorsqu'il délivre un certificat qualifié pour un service de confiance, vérifier, par des moyens appropriés, l'identité et, le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié ;

2° Lorsqu'il délivre des certificats qualifiés et décide de révoquer un certificat, enregistrer cette révocation dans sa base de données relative aux certificats et publie le statut de révocation du certificat en temps utile, et en tout état de cause dans les vingt-quatre heures suivant la réception de la demande. Cette révocation devient effective immédiatement dès sa publication ;

3° En ce qui concerne le point 2°, lorsqu'il délivre des certificats qualifiés fournir à toute partie utilisatrice des

informations sur la validité ou le statut de révocation des certificats qualifiés qu'il a délivrés. Ces informations sont disponibles, au moins par certificat, à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée qui est fiable, gratuite et efficace ;

4° Employer du personnel et, le cas échéant, des sous-traitants qui possèdent l'expertise, la fiabilité, l'expérience et les qualifications nécessaires, qui ont reçu une formation appropriée en ce qui concerne les règles en matière de sécurité et de protection des données à caractère personnel ;

5° En ce qui concerne le risque de responsabilité pour dommages conformément à l'article LP. 44, maintenir des ressources financières suffisantes et/ou contracter une assurance responsabilité appropriée, conformément au droit en vigueur ;

6° Avant d'établir une relation contractuelle, informer, de manière claire et exhaustive, toute personne désireuse d'utiliser un service de confiance qualifié des conditions précises relatives à l'utilisation de ce service, y compris toute limite quant à son utilisation ;

7° Utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et assurer la sécurité technique et la fiabilité des processus qu'il prend en charge ;

8° Utiliser des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière que :

a) Les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données ;

b) Seules des personnes autorisées puissent introduire des données et modifier les données conservées ;

c) L'authenticité des données puisse être vérifiée ;

9° Prendre des mesures appropriées contre la falsification et le vol de données ;

10° Enregistrer et maintenir accessibles pour une durée appropriée, y compris après que les activités du prestataire de services de confiance qualifié ont cessé, toutes les informations pertinentes concernant les données délivrées et reçues par le prestataire de services de confiance qualifié, aux fins notamment de pouvoir fournir des preuves en justice et aux fins d'assurer la continuité du service. Ces enregistrements peuvent être effectués par voie électronique ;

11° Avoir un plan actualisé d'arrêt d'activité afin d'assurer la continuité du service conformément aux dispositions vérifiées par l'autorité nationale de contrôle ;

12° Assurer le traitement licite de données à caractère personnel conformément à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

13° Au cas où il délivre des certificats qualifiés, établir et tenir à jour une base de données relative aux certificats.

PARAGRAPHE IV - HORODATAGE ÉLECTRONIQUE

Art. LP. 36

L'effet juridique et la recevabilité d'un horodatage électronique comme preuve en justice ne peuvent être refusés au seul motif que cet horodatage se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences de l'horodatage électronique qualifié.

Un horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent cette date et cette heure.

Art. LP. 37 *Rédaction issue de Erratum à la loi du pays n° 2017-30 du 2 novembre 2017*

Un horodatage électronique qualifié satisfait aux exigences suivantes :

1° Il lie la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données ;

2° Il est fondé sur une horloge exacte liée au temps universel coordonné ;

3° Il est signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié ou par une méthode équivalente.

PARAGRAPHE V - SERVICES D'ENVOI RECOMMANDÉ ÉLECTRONIQUE

Art. LP. 38

L'effet juridique et la recevabilité des données envoyées et reçues à l'aide d'un service d'envoi recommandé électronique comme preuves en justice ne peuvent être refusés au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du service d'envoi recommandé électronique qualifié.

Les données envoyées et reçues au moyen d'un service d'envoi recommandé électronique qualifié bénéficient

d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié et à leur réception par le destinataire identifié, et à l'exactitude de la date et de l'heure de l'envoi et de la réception indiquées par le service d'envoi recommandé électronique qualifié.

Art. LP. 39

Les services d'envoi recommandé électronique qualifiés satisfont aux exigences suivantes :

1° Ils sont fournis par un ou plusieurs prestataires de services de confiance qualifiés ;

2° Ils garantissent l'identification de l'expéditeur avec un degré de confiance élevé ;

3° Ils garantissent l'identification du destinataire avant la fourniture des données ;

4° L'envoi et la réception de données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié, de manière à exclure toute possibilité de modification indétectable des données ;

5° Toute modification des données nécessaire pour l'envoi ou la réception de celles-ci est clairement signalée à l'expéditeur et au destinataire des données ;

6° La date et l'heure d'envoi, de réception et toute modification des données sont indiquées par un horodatage électronique qualifié.

Dans le cas où les données sont transférées entre deux prestataires de services de confiance qualifiés ou plus, les exigences fixées aux points 1° à 6° s'appliquent à tous les prestataires de services de confiance qualifiés.

PARAGRAPHE VI - LISTE DES PRESTATAIRES DE SERVICES DE CONFIANCE QUALIFIÉS

Art. LP. 40

Les prestataires de service de confiance visés par la présente section sont ceux ayant obtenu la qualification délivrée par le règlement eIDAS n° 910-2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

La certification des dispositifs de création de signature électronique et de cachet électronique qualifiés atteste de leur conformité aux exigences fixées à l'annexe 2 de la présente loi du pays.

Cette certification correspond à celle délivrée par le règlement eIDAS n° 910-2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

Un arrêté pris en conseil des ministres fixe les dispositions d'application du présent article.

PARAGRAPHE VII - EQUIVALENCE ET TRANSITION ENTRE SERVICES DE CONFIANCE QUALIFIÉS

Art. LP. 41

Le conseil des ministres approuve le référentiel d'exigences. Ce dernier fixe les normes relatives aux services de confiance qualifiés prévus aux paragraphes I à V de la présente section, ainsi que les équivalences entre les services de confiance qualifiés au sens du référentiel général de sécurité et les services de confiance prévus aux paragraphes I à V de la présente section.

PARAGRAPHE VIII - ARCHIVES ÉLECTRONIQUES

Art. LP. 42

L'effet juridique et la recevabilité des archives électroniques comme preuves en justice ne peuvent être refusés au seul motif que ces documents se présentent sous une forme électronique.

PARAGRAPHE IX - COPIE NUMÉRIQUE

Art. LP. 43

L'effet juridique et la recevabilité d'une copie numérique comme preuves en justice ne peuvent être refusés au seul motif que ces documents se présentent sous une forme électronique.

La copie fiable a la même force probante que l'original. La fiabilité est laissée à l'appréciation du juge.

Est présumée fiable jusqu'à preuve du contraire toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par un arrêté pris en conseil des ministres.

Si l'original subsiste, sa présentation peut toujours être exigée.

PARAGRAPHE X - RESPONSABILITÉ

Art. LP. 44

Sans préjudice du dernier alinéa du présent article, les prestataires de services de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par la présente loi du pays.

Il incombe à la personne physique ou morale qui invoque les dommages visés au premier alinéa de prouver que le prestataire de services de confiance non qualifié a agi intentionnellement ou par négligence.

Un prestataire de services de confiance qualifié est présumé avoir agi intentionnellement ou par négligence, à moins qu'il ne prouve que les dommages visés au premier alinéa ont été causés sans intention ni négligence de sa part.

Lorsque les prestataires de services de confiance informent dûment leurs clients au préalable des limites qui existent à l'utilisation des services qu'ils fournissent et que ces limites peuvent être reconnues par des tiers, les prestataires de services de confiance ne peuvent être tenus responsables des dommages découlant de l'utilisation des services au-delà des limites indiquées.

SECTION VII - RÉFÉRENTIEL GÉNÉRAL D'ACCESSIBILITÉ

Art. LP. 45

Un référentiel général d'accessibilité, approuvé par un arrêté pris en conseil des ministres, fixe les orientations techniques, sémantiques, organisationnelles et d'ergonomie vers lesquelles les téléservices doivent tendre afin d'assurer aux personnes handicapées la réception et la compréhension de tout type d'information diffusée sous forme numérique, de leur permettre d'utiliser ces services et, le cas échéant, d'interagir avec ces derniers.

SECTION VIII - RÉFÉRENTIEL GÉNÉRAL D'INTEROPÉRABILITÉ DES SYSTÈMES D'INFORMATION

Art. LP. 46

Un référentiel général d'interopérabilité, approuvé par le conseil des ministres, fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives.

SECTION IX - DISPOSITIONS FINALES ET TRANSITOIRES

Art. LP. 47

A l'article 1er de la délibération n° 83-81 du 28 avril 1983 portant sur la réglementation archivistique en Polynésie française, après les mots : "support matériel", il est inséré les mots : "ou numérique".

Art. LP. 48

Les systèmes d'information existant à la date de publication du référentiel général de sécurité mentionné à l'article LP. 20 de la présente loi du pays sont mis en conformité avec ce référentiel dans un délai de cinq ans à compter de sa publication. Les applications créées dans les six mois suivant la date de publication du référentiel sont mises en conformité avec celui-ci au plus tard vingt-quatre mois après cette date.

Les systèmes d'information existant à la date de publication du référentiel général d'interopérabilité mentionné à l'article LP. 46 sont mis en conformité avec ce référentiel dans un délai de cinq ans à compter de sa publication. Les applications créées dans les six mois suivant la date de publication du référentiel sont mises en conformité avec celui-ci au plus tard vingt-quatre mois après cette date.

Le présent acte sera exécuté comme loi du pays.

Fait à Papeete, le 2 novembre 2017.

Par le Président de la Polynésie française :
Edouard FRITCH.

Le ministre du logement,
de l'aménagement et de l'urbanisme,
Jean-Christophe BOUISSOU.

Travaux préparatoires :
- avis n° 72 CESC du 22 décembre 2016 du conseil économique, social et culturel de la Polynésie française ;
- arrêté n° 82 CM du 27 janvier 2017 soumettant un projet de loi du pays à l'assemblée de la Polynésie française ;
- examen par la commission des institutions, des affaires internationales et européennes et des relations avec les

communes le 7 août 2017 ;
- rapport n° 90-2017 du 10 août 2017 de M. Jules Ienfa, rapporteur du projet de loi du pays ;
- adoption en date du 14 septembre 2017 ; texte adopté n° 2017-26 LP/APF du 14 septembre 2017 ;
- publication à titre d'information au JOPF n° 76 du 22 septembre 2017.

Annexe 1 – Exigences applicables aux certificats qualifiés de signature électronique
Annexe 2 – Exigences applicables aux dispositifs de création de signature électronique qualifiés
Annexe 3 – Exigences applicables aux certificats qualifiés de cachet électronique

Voir toutes les modifications dans le temps :

- Loi du Pays n° 2017-30 du 2 novembre 2017, JOPF n° 74 NS du 02/11/2017 à la page 7058
- Erratum à l'intitulé de la loi du Pays n° 2017-30 du 2 novembre 2017, JOPF n° 89 NC du 07/11/2017 à la page 16424
- Erratum à la loi du pays n° 2017-30 du 2 novembre 2017, JOPF n° 126 N du 05/11/2024 à la page 20460

Annexe 1 – Exigences applicables aux certificats qualifiés de signature électronique

Les certificats qualifiés de signature électronique contiennent :

a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de signature électronique ;

b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés, et :

- pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels,

- pour une personne physique: le nom de la personne ;

c) au moins le nom du signataire ou un pseudonyme ; si un pseudonyme est utilisé, cela est clairement indiqué ;

d) des données de validation de la signature électronique qui correspondent aux données de création de la signature électronique ;

e) des précisions sur le début et la fin de la période de validité du certificat ;

f) le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié ;

g) la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat ;

h) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé mentionnés au point g) ;

i) l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié ;

j) lorsque les données de création de la signature électronique associées aux données de validation de la signature électronique se trouvent dans un dispositif de création de signature électronique qualifié, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.

Annexe 2 – Exigences applicables aux dispositifs de création de signature électronique qualifiés

1. Les dispositifs de création de signature électronique qualifiés garantissent au moins, par des moyens techniques et des procédures appropriés, que :

a) la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ;

b) les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois ;

c) l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques actuellement disponibles ;

d) les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2. Les dispositifs de création de signature électronique qualifiés ne modifient pas les données à signer et n'empêchent pas la présentation de ces données au signataire avant la signature.

3. La génération ou la gestion de données de création de signature électronique pour le compte du signataire peut être seulement confiée à un prestataire de services de confiance qualifié.

4. Sans préjudice du paragraphe 1, point d), un prestataire de services de confiance qualifié gérant des données de création de signature électronique pour le compte d'un signataire ne peut reproduire les données de création de signature électronique qu'à des fins de sauvegarde, sous réserve du respect des exigences suivantes :

a) le niveau de sécurité des ensembles de données reproduits doit être équivalent à celui des ensembles de données d'origine ;

b) le nombre d'ensembles de données reproduits n'excède pas le minimum nécessaire pour assurer la continuité du service.

Annexe 3 – Exigences applicables aux certificats qualifiés de cachet électronique

Les certificats qualifiés de cachet électronique contiennent :

a) une mention indiquant, au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié de cachet électronique ;

b) un ensemble de données représentant sans ambiguïté le prestataire de services de confiance qualifié délivrant les certificats qualifiés et :

- pour une personne morale: le nom et, le cas échéant, le numéro d'immatriculation tels qu'ils figurent dans les registres officiels,

- pour une personne physique: le nom de la personne ;

c) au moins le nom du créateur du cachet et, le cas échéant, son numéro d'immatriculation tels qu'ils figurent dans les registres officiels ;

d) des données de validation du cachet électronique, qui correspondent aux données de création du cachet électronique ;

e) des précisions sur le début et la fin de la période de validité du certificat ;

f) le code d'identité du certificat, qui doit être unique pour le prestataire de services de confiance qualifié ;

g) la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat ;

h) l'endroit où peut être obtenu gratuitement le certificat sur lequel reposent la signature électronique avancée ou le cachet électronique avancé mentionnés au point g) ;

i) l'emplacement des services qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié ;

j) lorsque les données de création du cachet électronique associées aux données de validation du cachet électronique se trouvent dans un dispositif de création de cachet électronique qualifié, une mention l'indiquant, au moins sous une forme adaptée au traitement automatisé.