SunPKI

Sunnystamp Natural Persons CA

Déclaration d'IGC

Version 1.12

Date d'entrée en vigueur : 04/11/2026

Tous droits réservés

Table des matières

1. Objet du document 2
2. Définitions et acronymes 2
3. Conditions générales d'utilisation 6
4. Références 15

9 Av Maréchal Leclerc - 10120 ST ANDRE LES VERGERS - FRANCE
Tél. : +33 (0)3 25 43 90 78 – www.goodflag.com
SAS au capital de 26 739 euros – R.C.S. Troyes 480 622 257 – Code APE 5829C – TVA FR01480622257

1. Objet du document

Au début de l'année 2025, la société Lex Persona a adopté le nom commercial Goodflag. En revanche, toutes les références techniques et organisationnelles, telles que les gabarits des Certificats, les Certificats d'AC, l'organe de gouvernance de l'AC, etc., conservent le nom Lex Persona et sont toujours en vigueur.

Ce document est la Déclaration d'Infrastructure de Gestion de Clés de l'Autorité de Certification intermédiaire « Sunnystamp Natural Persons CA », ci-après dénommée AC dans le reste du document.

Ce document a pour objectif de présenter et résumer les points principaux décrits par la Politique de Certification et la Déclaration des Pratiques de Certification (PC/DPC) de l'AC disponible à l'adresse : https://pki2.sunnystamp.com/repository.

Il est à destination des titulaires de Certificats (appelés Signataires), des personnes morales disposant du Service de signature (appelées Clients) et des Utilisateurs de Certificats (UC).

2. Définitions et acronymes

Autorité de Certification (AC)
Au sein d'un Prestataire de Service de Certification Electronique (PSCE), ici la société Lex Persona, une AC a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une PC/DPC, et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du Certificat).

Autorité d'Enregistrement (AE)
Les missions principales de l'AE consistent à vérifier l'identité des Signataires, authentifier et transmettre à l'AC les demandes de création et de révocation de Certificats et d'archiver les données relatives à l'identification des Signataires. L'AE est gérée et opérée par Lex Persona. L'AE peut déléguer tout ou partie de ses missions à une entité tierce sous contrat avec Lex Persona. Lex Persona, en tant qu'AC, reste toujours responsable des obligations qui lui incombent vis-à-vis des Clients et des Signataires.

Bi-clé
Combinaison d'une Clé Privée et d'une Clé Publique utilisée pour effectuer des opérations cryptographiques.

Certificat
Ensemble d'informations garantissant l'association entre l'identité d'un Signataire et une Clé Publique, grâce à une signature électronique de ces données, effectuée à l'aide de la Clé Privée de l'AC qui délivre le Certificat. Un Certificat contient des informations telles que :

- L'identité du Signataire ;

- La Clé Publique du Signataire ;
- Le(s) usage(s) autorisé(s) de la Clé Publique ;
- La durée de vie du Certificat ;
- L'identité de l'AC ;
- La signature de l'AC.

Clé Privée
Clé d'une Bi-clé d'une entité devant être utilisée exclusivement par cette entité.

Clé Publique
Clé d'une Bi-clé d'une entité pouvant être rendue publique.

Client
Personne morale qui dispose du Service de signature et le met à la disposition de personnes qu'elle habilite, lesquelles créent les Transactions de signature au sein desquelles des documents sont soumis à la signature de Signataires. Le Client, ou la personne qu'il a habilitée, fournit à l'AE les informations d'identité du Signataire. Le Client ne demande pas de Certificat : la demande émane du Signataire lui-même, lors du parcours de consentement de la Transaction de signature.

Déclaration des Pratiques de Certification (DPC)
Ensemble de pratiques qu'une Autorité de Certification met en œuvre pour émettre, gérer, révoquer et renouveler les Certificats qu'elle émet dans le cadre d'une Politique de Certification.

Entité Légale
Terme utilisé dans ce document pour désigner exclusivement la personne morale à laquelle le Signataire est rattaché, le cas échéant, et au nom de laquelle ce dernier utilise son Certificat.

Fournisseur d'Identité
Entité tierce chargée par l'AE d'identifier et d'authentifier les Signataires. Le Fournisseur d'Identité, après avoir vérifié l'identité du Signataire, produit un Jeton d'identité attestant de cette identité. Ce Jeton est validé et exploité par l'AE de sorte que l'AC délivre le Certificat du Signataire sur la base des informations d'identité qu'il contient.

Infrastructure de Gestion de Clés (IGC)
Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs Certificats utilisés par des services de confiance. Une IGC peut être composée d'une Autorité de Certification, d'un Opérateur de Certification, d'une Autorité d'Enregistrement centralisée et/ou locale, de Mandataires de Certification, d'une entité d'archivage, d'une entité de publication, etc.

Jeton d'identité

Ensemble de données produites par un Fournisseur d'Identité à la suite de l'authentification d'une personne physique et contenant notamment les informations d'identité de cette personne (nom, prénom, etc.).

Liste des Certificats Révoqués (LCR) : liste signée, publiée par l'AC et contenant à un instant donné la liste des Certificats révoqués par l'AC.

Object Identifier (OID)
Identifiant universel, représenté sous la forme d'une suite d'entiers. Les OID sont organisés sous une forme hiérarchique avec des nœuds visant à faciliter l'interopérabilité entre différents logiciels.

Politique de Certification (PC)
Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une Autorité de Certification se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC/DPC peut également, si nécessaire, identifier les obligations et les exigences portant sur les autres intervenants, notamment les Signataires et les UC.

Prestataire de Contrôle d'Identité à Distance (PCID)
Prestataire fournissant un service de contrôle à distance de la pièce d'identité des personnes physiques, certifié a minima au niveau ETSI LCP. Dans le cadre de la présente PC/DPC, l'AE recourt à un tel prestataire pour le seul contrôle de la concordance entre les nom et prénom(s) gérés par l'AE avec ceux figurant sur la pièce d'identité recueillie lors de l'authentification du Signataire, à l'exclusion du rapprochement entre le Signataire et cette pièce d'identité, lequel est assuré par l'AE elle-même.

Service de Fédération d'Identité Reconnu (SFIR)
Service d'identification et d'authentification de personnes physiques, reconnu par l'AC selon les critères et la procédure définis au chapitre 3.2.7 de la PC/DPC, auquel l'AE délègue la validation de l'identité du Signataire pour les Certificats ETSI LCP SFIR. Un SFIR agit en qualité de Fournisseur d'Identité ou fédère plusieurs Fournisseurs d'Identité. La liste des SFIR reconnus par l'AC figure au chapitre 3.2.7 de la PC/DPC.

Service de signature
Service de confiance de création de signatures et de délivrance de Certificats de signature générés « à la volée », mis à disposition par Lex Persona à ses clients pour leur permettre de faire signer des documents à des personnes physiques. Dans le cadre de la PC/DPC, le Service de signature est une composante de l'AE. Il identifie et authentifie les Signataires afin de leur délivrer un Certificat « à la volée » dédié à une Transaction de signature particulière. La Clé Privée du Signataire, associée au Certificat, est générée et utilisée de manière sécurisée par le Service de signature pour signer les documents de la Transaction de signature et est immédiatement détruite une fois les documents signés.

Signataire
Personne physique, rattachée ou non à une Entité Légale, identifiée dans le Certificat comme étant le porteur de la Clé Privée associée à la Clé Publique contenue dans le Certificat et utilisant cette Clé Privée pour signer des documents électroniques. Le Signataire est à l'origine de la demande de Certificat, qu'il formule et accepte lors de la Transaction de signature.

Transaction de signature
Opération de courte durée, gérée par le Service de signature, durant laquelle un Signataire doit s'authentifier auprès de l'AE pour obtenir un Certificat et pouvoir signer électroniquement les documents de cette transaction avec sa Clé Privée « distante » associée à son Certificat et opérée par le Service de signature.

Utilisateur de Certificats (UC)
Toute personne physique ou morale qui utilise un Certificat délivré par l'AC, pour ses propres besoins, et qui doit pour cela le vérifier préalablement.

3. Conditions générales d'utilisation

Contact de l'AC	LEX PERSONA 9 AVENUE MARECHAL LECLERC 10120 ST ANDRE LES VERGERS FRANCE Adresse email : pki@sunnystamp.com Téléphone : +33 (0)3 25 43 90 78
Site de publication	Les informations, énumérées dans la section 2.2 de la PC/DPC, sont publiées sur le site de publication de l'AC : https://pki2.sunnystamp.com/repository. Le site de publication est disponible 24h/24 et 7j/7 en conditions normales de fonctionnement. L'adresse https://pki2.sunnystamp.com/repository est redirigée vers https://goodflag.com/services-de-confiance.
Types de Certificats émis	L'AC délivre des Certificats à des personnes physiques pouvant être rattachées ou non à une Entité Légale. Ces Certificats ont une durée de validité maximale d'une (1) heure et ne peuvent être utilisés que pour signer les documents de la Transaction de signature pour laquelle ils ont été spécialement créés. L'AC délivre six types de Certificats : 1. Les certificats utilisés par ses répondeurs OCSP pour signer les réponses OCSP ; 2. Les certificats « ETSI LCP avec possibilité de révocation » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.2, conformes à la norme [EN 319 411-1] pour le niveau LCP ; ces Certificats ne sont plus émis par l'AC, la présente Déclaration étant maintenue à leur égard pour les seuls besoins de la validation des signatures électroniques déjà produites ; 3. Les certificats « OPEN REG » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.3, pour lesquels la présente PC/DPC laisse l'Autorité d'Enregistrement libre de définir le processus d'enregistrement appliqué pour authentifier et vérifier l'identité des Signataires ; 4. Les certificats « ETSI LCP SFIR » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.4, conformes à la norme [EN 319 411-1] pour le niveau LCP, délivrés à la suite

Copyright Goodflag 2026

	d'une authentification du Signataire auprès d'un Service de Fédération d'Identité Reconnu (SFIR) au sens de la section 3.2.7 de la PC/DPC. Les Certificats émis sous cet OID antérieurement à la date d'entrée en vigueur de la version 1.15 de la PC/DPC, alors dénommés « FranceConnect », ne comportent pas l'identifiant de politique 0.4.0.2042.1.3 et ne relèvent d'aucune conformité ETSI revendiquée ; 5. Les certificats « MIE eIDAS » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.5, conformes à la norme [EN 319 411-2] pour le niveau QCP-n-qscd, délivrés à la suite d'une vérification de l'identité du Signataire réalisée conformément à l'article 24, paragraphe 1 bis, du règlement eIDAS, au moyen : - du portefeuille européen d'identité numérique, ou d'un moyen d'identification électronique notifié satisfaisant aux exigences énoncées à l'article 8 du règlement eIDAS en ce qui concerne le niveau de garantie « élevé » ; ou - d'un moyen d'identification électronique certifié par l'ANSSI au titre de l'article L.102 du code des postes et des communications électroniques, selon un niveau de certification substantiel ou élevé, et figurant à ce titre au catalogue publié par l'ANSSI ; ou - d'une autre méthode d'identification garantissant l'identification de la personne physique avec un degré de confiance élevé, et dont la conformité est confirmée par un organisme d'évaluation de la conformité. L'AE s'assure que la notification ou la certification du moyen d'identification électronique utilisé est en cours de validité à la date de la Transaction de signature. Les normes de référence applicables à la vérification de l'identité et des attributs prévue à l'article 24, paragraphes 1, 1 bis et 1 ter, du règlement eIDAS sont fixées par le [UE_2025_1566], pris en application du paragraphe 1 quater du même article ; 6. Les certificats « ETSI LCP PCID » avec l'OID 1.3.6.1.4.1.22542.100.1.1.1.6, conformes à la norme [EN 319 411-1] pour le niveau LCP, délivrés à la suite du contrôle de la pièce d'identité du Signataire au moyen d'un service fourni par un Prestataire de

	Contrôle d'Identité à Distance (PCID) certifié a minima au niveau ETSI LCP, complétée par le rapprochement du Signataire avec cette pièce d'identité au moyen d'un OTP transmis par SMS. À l'exception des Certificats « ETSI LCP avec possibilité de révocation », qui ne sont plus émis, les Certificats de Signataire délivrés par l'AC ne peuvent pas être révoqués. Un tel Certificat n'est en effet généré qu'au moment où la signature électronique a lieu, pour une durée d'une heure et pour les seuls besoins d'une unique Transaction de signature : il n'existe donc aucune période pendant laquelle sa révocation aurait un effet utile. Les Certificats des composantes de l'IGC, et notamment les Certificats de répondeur OCSP, ne sont pas concernés par ce qui précède : leurs conditions de révocation sont décrites à la section 4.9 de la PC/DPC. Les Certificats sont émis par l'AC « Sunnystamp Natural Persons CA », qui est elle-même émise par l'AC racine « Sunnystamp Root CA G2 ». Les certificats de ces AC sont disponibles à l'adresse suivante : https://pki2.sunnystamp.com/repository. L'AC peut délivrer des certificats de test, lesquels sont identifiés par le préfixe « `TEST-` » dans les attributs SN et GN du sujet.
Objet des Certificats	Les Certificats émis par l'AC sont des certificats de signature à destination de personnes physiques, et qui, dans le cas des Certificats OPEN REG et MIE eIDAS, peuvent être rattachées à une personne morale.
Modalités d'obtention	La demande d'un Certificat provient du besoin par le Signataire de signer, au sein d'une Transaction de signature, les documents que lui a soumis le Client. La validation de l'identité du Signataire s'effectue de la manière suivante. <u>Pour les Certificats ETSI LCP PCID</u> : Le Client doit fournir à l'AE les nom, prénom(s) et numéro de téléphone portable du Signataire devant signer les documents.

	Le Signataire doit ensuite saisir l'OTP SMS que lui a envoyé l'AE et transmettre à l'AE un document officiel d'identité (carte nationale d'identité, passeport ou titre de séjour) en cours de validité avec photographie comportant ses nom, prénom(s), date et lieu de naissance. La vérification de la validité et de l'authenticité de ce document est réalisée au moyen d'un service fourni par un Prestataire de Contrôle d'Identité à Distance (PCID) certifié a minima au niveau ETSI LCP. L'AE ne recourt à ce service que pour le contrôle de la concordance des nom et prénom(s) du Signataire définis par l'AE avec ceux figurant sur la pièce d'identité ; le rapprochement entre le Signataire et le document ainsi contrôlé est assuré par l'AE elle-même, au moyen de l'OTP SMS qui permet de vérifier que le Signataire est bien le propriétaire du numéro de téléphone portable communiqué par le Client. <u>Pour les Certificats OPEN REG</u> : Le Client doit fournir a minima à l'AE les nom et prénom(s) du Signataire devant signer les documents. L'AE délègue au Client les procédures d'identification et d'authentification du Signataire. Le Client doit documenter ces procédures et en conserver la traçabilité. Le cas échéant, l'AE délègue également au Client les procédures d'identification et de vérification de l'Entité Légale et du rattachement du Signataire à ladite Entité Légale, que le Client doit documenter de manière appropriée et dont il doit conserver la traçabilité. <u>Pour les Certificats ETSI LCP SFIR :</u> L'AE délègue la validation de l'identité du Signataire à un SFIR reconnu au sens de la section 3.2.7 de la PC/DPC et récupère du Jeton d'identité au moins les informations d'identité suivantes du Signataire : Pour comparaison avec les informations définies par le Client : • Nom de naissance ; • Prénom(s) ; À des fins probatoires : • Date de naissance ;

	• Lieu de naissance. L'AE vérifie que le Jeton d'identité est valide, qu'il émane du SFIR sollicité et qu'il porte une revendication de niveau de garantie au moins équivalente au niveau « faible » au sens de l'annexe du règlement d'exécution (UE) 2015/1502. À défaut, ou en l'absence de toute revendication de niveau de garantie, le Certificat n'est pas émis et la Transaction de signature ne peut aboutir. L'AE compare les nom et prénom(s) déclarés lors de l'identification du Signataire par le créateur de la Transaction de signature avec ceux portés par le Jeton d'identité, après normalisation des valeurs selon les règles définies à la section 3.1.1.3 de la PC/DPC. En cas de discordance, le Certificat n'est pas émis et la Transaction de signature ne peut aboutir ; les date et lieu de naissance portés par le Jeton d'identité ne font pas l'objet de cette comparaison et sont conservés avec celui-ci dans le dossier d'enregistrement (cf. section 3.2.4 de la PC/DPC). Les informations portées par le Jeton d'identité prévalent sur les informations déclarées lors de l'identification pour la constitution du champ subject du Certificat. L'AE rejette toute demande de Certificat fondée sur un service ne figurant pas dans la liste des SFIR reconnus par l'AC (section 3.2.7 de la PC/DPC). <u>Pour les Certificats MIE eIDAS</u> : L'AE délègue la validation de l'identité du Signataire au moyen d'identification électronique, et récupère les informations d'identité suivantes du Signataire : Pour comparaison avec les informations définies par le Client : • Nom de naissance ; • Prénom(s) ; À des fins probatoires : • Date de naissance ; • Lieu de naissance. L'AE s'assure que les moyens d'identification électronique auxquels elle délègue la validation d'identité répondent bien aux exigences de l'article 24, paragraphe 1 bis, point a) ou

	point c), du règlement eIDAS. L'AE compare les nom et prénom(s) déclarés lors de l'identification du Signataire par le créateur de la Transaction de signature avec ceux restitués par le moyen d'identification électronique. En cas de discordance, le Certificat n'est pas émis et la Transaction de signature ne peut aboutir. Les informations restituées par le moyen d'identification électronique prévalent pour la constitution du champ subject du Certificat. Le Signataire peut être rattaché à une Entité Légale si le moyen d'identification électronique le permet et que l'identité qu'il porte contient les informations relatives à ce rattachement ; ce rattachement est alors automatiquement validé par le moyen d'identification électronique. <u>Pour tous les Certificats</u> : Le Signataire doit approuver explicitement les CGU. Les informations du Signataire qui sont ou seront contenues dans le champ subject du Certificat sont portées à sa connaissance afin qu'il puisse les accepter explicitement avant de déclencher la création ou l'utilisation de la Clé Privée associée à son Certificat pour signer les documents de la Transaction de signature. L'acceptation du Certificat par le Signataire emporte son consentement à la publication du Certificat, laquelle s'opère via les documents signés au cours de la Transaction de signature.
Utilisation de la clé privée et du Certificat par le Signataire pour signer	La Clé Privée d'un Signataire est protégée par le Service de signature qui met en œuvre des moyens techniques et organisationnels pour garantir que seul le propriétaire de cette Clé Privée puisse l'utiliser pour signer. L'utilisation par le Signataire de sa Clé Privée et de son Certificat associé est strictement limitée au Service de signature. La Clé Privée du Signataire est gérée exclusivement par le Service de signature, qui la crée, l'utilise et la détruit dans le cadre d'une Transaction de signature spécifique. Pour tous les Certificats délivrés par l'AC, la clé privée du Signataire est générée et stockée sur un HSM certifié *FIPS 140-2 level 3*, certifié QSCD et présent sur la liste publiée par la Commission européenne.
Modalités de renouvellement	Il n'y a pas de processus de renouvellement.

Modalités de révocation	Les Certificats de Signataire délivrés par l'AC ne peuvent pas être révoqués, pour les raisons exposées à la rubrique « Types de Certificats émis » ci-dessus. Les Certificats « ETSI LCP avec possibilité de révocation » ont cessé d'être émis. Les Certificats des composantes de l'IGC, et notamment les Certificats de répondeur OCSP, peuvent quant à eux être révoqués dans les conditions décrites à la section 4.9 de la PC/DPC.
Limites d'usage	Les Certificats délivrés par l'AC ont une durée de validité maximale de 1 heure et sont utilisés par les Signataires pour signer exclusivement les documents de la transaction de signature pour laquelle ils ont été spécialement créés. L'AC ne peut être tenue responsable de l'utilisation du Certificat d'une manière non conforme à la PC/DPC. Les usages autres que ceux décrits à la section 1.4.1 de la PC/DPC sont interdits. De plus, les Certificats doivent être utilisés dans la limite des lois et réglementations en vigueur. Un Certificat délivré par l'AC est utilisé par un UC pour valider les signatures électroniques créées par une personne physique qui est le propriétaire du Certificat. Les certificats de test ne sont produits qu'à des fins de test technique ou de démonstration et n'engagent ni l'AC ni la personne qui les utilise. Les informations du dossier d'enregistrement ainsi que les traces des événements liés au cycle de vie des Certificats sont conservées par l'AC pendant 7 ans. Le dossier d'enregistrement comprend notamment la preuve de l'acceptation des CGU par le Signataire ainsi que, selon le type de Certificat, une copie du rapport du contrôle de la pièce d'identité (Certificats ETSI LCP PCID et ETSI LCP avec possibilité de révocation), le Jeton d'identité signé restitué par le SFIR (Certificats ETSI LCP SFIR) ou le jeton OpenID Connect d'authentification du Signataire au MIE eIDAS (Certificats MIE eIDAS).
Obligations des Signataires	Le Signataire a l'obligation de : • Respecter les exigences de la PC/DPC qui concernent le Signataire ;

	• Respecter les modalités d'usages précisées dans le chapitre 4.5 de la PC ; • Fournir des informations correctes à l'AE lors de la phase d'enregistrement ; • Confirmer l'exactitude des informations contenues, ou qui seront contenues, dans son Certificat ; • Informer l'AE de toute modification des informations contenues dans son Certificat ; • Accepter les CGU ; • Protéger ses moyens d'authentification ; • Accepter l'accord relatif à l'utilisation d'un dispositif cryptographique satisfaisant aux exigences de la section 6.2.11 de la PC/DPC.
Obligations des Clients	Le Client a l'obligation de : • Respecter les obligations qui lui incombent et qui sont décrites dans l'accord de souscription ; • Respecter les modalités d'usages précisées dans le chapitre 1.4 de la PC ; • Fournir des informations correctes à l'AE lors de la phase d'enregistrement ; • Informer l'AE de toute modification des informations contenues dans le Certificat.
Obligations de vérification des certificats par les UC	Les UC ont l'obligation de : • Respecter les obligations décrites dans l'accord d'utilisation des Certificats ; • Vérifier et respecter l'usage pour lequel le Certificat a été émis ; • Utiliser le logiciel et le matériel adéquat pour la vérification de la validité du Certificat ; • Vérifier que l'extension « KeyUsage » contenue dans le Certificat est conforme à l'utilisation du Certificat ; • Vérifier que l'OID de la PC/DPC est contenu dans l'extension « Certificate Policies » du Certificat ; • Vérifier, avant son utilisation, la validité de la chaîne de certification (dates de validité, signature des Certificats, statut de révocation) en partant du Certificat du Signataire et en remontant au moins jusqu'au Certificat de l'AC. Il est rappelé aux UC que les certificats de test ne sont produits qu'à des fins de test technique ou de démonstration et n'engagent ni l'AC ni la personne qui les utilise.

	La méthode utilisée (LCR ou OCSP) pour vérifier le statut de révocation des Certificats est laissée à l'appréciation de l'UC. Les Certificats de Signataire n'étant ni révocables ni publiés par l'AC, le répondeur OCSP retourne pour ceux-ci un statut « good ». Il en va de même pour tout numéro de série non révoqué relevant de l'AC : une réponse « good » ne permet donc pas d'établir qu'un Certificat portant ce numéro de série a effectivement été émis par l'AC.
Limite de responsabilité	Lex Persona ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme à la PC/DPC des Clés Privées, des Certificats associés, des informations de révocation, ainsi que de tout autre équipement ou logiciel mis à disposition. Lex Persona décline sa responsabilité pour tout dommage résultant des erreurs, inexactitudes ou omissions entachant les informations contenues dans les certificats, dès lors que ces erreurs, inexactitudes ou omissions résultent du caractère erroné des informations communiquées par le Client. Enfin, Lex Persona ne pourra être tenue responsable, dans la limite de la loi française, de perte financière, de perte de données ou de dommage indirect lié à l'utilisation d'un Certificat. La responsabilité de Lex Persona est strictement limitée, quelles que soient les causes, quels que soient les faits générateurs et quels que soient les préjudices causés, au montant payé par le Client sur les 3 derniers mois, et ce dans le respect et les limites de la loi applicable. Sauf prescription légale contraire, toute action du Client devra intervenir au plus tard dans un délai de 3 mois à compter de la survenance du fait générateur fondant l'action.
Références documentaires	La PC/DPC de l'AC est disponible à l'adresse suivante : https://pki2.sunnystamp.com/repository La version de la PC/DPC applicable à un Certificat est celle qui était en vigueur à la date d'émission de ce Certificat, telle qu'attestée par le champ notBefore dudit Certificat. Toutes les versions successives de la PC/DPC sont conservées par Lex Persona, sans limitation de durée, et demeurent accessibles sur le site de publication de l'AC.

Condition d'indemnisation	Sans objet.
Loi applicable et gestion des litiges	La présente PC/DPC est soumise au droit français. En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée au tribunal de commerce de Troyes. L'AC dispose d'une procédure de gestion des plaintes et réclamations qui consiste pour le demandeur à ouvrir un ticket sur le site de support de l'AC : https://support.lex-persona.com
Gestion des données à caractère personnel	L'AC prend toutes les mesures nécessaires pour que les données personnelles soient protégées et stockées de manière à garantir leur intégrité et leur confidentialité conformément à la loi française N°78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés et modifications à venir ainsi que le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.
Audits et références applicables	L'AC est certifiée conforme : ▪ pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.4, à la norme [EN 319 411-1] pour le niveau LCP ; ▪ pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.6, à la norme [EN 319 411-1] pour le niveau LCP ; ▪ pour les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.5, à la norme [EN 319 411-2] pour le niveau QCP-n-qscd et au référentiel d'exigences [ANSSI_QCP]. Les certificats émis selon la politique 1.3.6.1.4.1.22542.100.1.1.1.3 (OPEN REG) ne relèvent d'aucune conformité revendiquée. Le certificat de conformité est valable 2 ans et est délivré à la suite d'un audit réalisé par un organisme accrédité selon la norme [EN 319 403-1].

4. Références

[EN 319 403-1]

ETSI EN 319 403-1 V2.3.1 (2020-06)

Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

[EN 319 411-1]
ETSI EN 319 411-1 V1.5.1 (2025-04)
Policy and security requirements for Trust Service Providers issuing certificates
Part 1: General requirements

[EN 319 411-2]
ETSI EN 319 411-2 V2.6.1 (2025-06)
Policy and security requirements for Trust Service Providers issuing certificates
Part 2: Requirements for trust service providers issuing EU qualified certificates

[ANSSI_QCP]
Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site Internet, Critères d'évaluation de la conformité au règlement eIDAS
ANSSI, version 1.2 du 25 mars 2021

[UE_2025_1566]
Règlement d'exécution (UE) 2025/1566 de la Commission du 29 juillet 2025 établissant des règles d'application du règlement (UE) no 910/2014 en ce qui concerne les normes de référence pour la vérification de l'identité et des attributs de la personne à laquelle le certificat qualifié ou l'attestation électronique d'attributs qualifiée doit être délivré
Applicable à compter du 19 août 2027.