Politique d'Enregistrement et Déclaration des Pratiques d'Enregistrement

Identification du document

042017_C1_DEM_v1.0_politique_d_enregistrement_et_declaration_des_pratiques_d_enregistrement

Identification du propriétaire du document

Propriétaire	Coordonnées
David Emo	Email : d.emo@netheos.net Téléphone : +33 9 72 34 11 80

Classification du document

Document public

Révisions

Date	Version	Auteur	Relecture	Commentaires
04/2017	1.0	DEM	ODE, CSO, LMO	

Table des matières

1. Introduction

1.1. Présentation générale

La présente Politique d'Enregistrement et Déclaration de Pratiques d'Enregistrement (ci-après nommée "PE/DPE") décrit les règles, pratiques et principes juridiques, commerciaux et techniques que NETHEOS, ses Clients et les Utilisateurs emploient pour garantir la validité de l'Enregistrement de l'Utilisateur dans le cadre d'une demande de Certificat auprès d'une Autorité de Certification (ci-après nommée "AC") intervenant lors d'un Parcours Client réalisé à distance ou en face à face.

NETHEOS édite et opère le service d'enregistrement Trust and Sign.

La présente PE/DPE a pour objet de décrire la phase d'enregistrement des Utilisateurs.

1.2. Identification du document

La présente PE/DPE appelée " Politique d'Enregistrement et Déclaration des Pratiques d'Enregistrement Trust and Sign" est la propriété de NETHEOS. Elle est identifiée par la référence suivante :
042017_C1_DEM_v1.0_politique_d_enregistrement_et_declaration_des_pratiques_d_enregistrement

1.3. Entités intervenant dans le service de confiance

1.3.1. Autorité de certification

L'Autorité de Certification est l'autorité en charge de l'émission des Certificats.

Elle est contractuellement liée à l'AE.

1.3.2. Autorité d'enregistrement

L'Autorité d'Enregistrement est l'autorité qui a en charge la vérification de l'identité, des droits et de la qualité du demandeur du certificat électronique. Ces éléments seront ensuite transmis au service de génération de certificats et inscrits dans le certificat. Elle gère également les données d'activation telles que le code à usage unique envoyé par SMS au demandeur (dît "code OTP").

L'Autorité d'Enregistrement a également la responsabilité de journaliser et d'auditer les demandes d'enregistrement.

1.3.3. Utilisateur

L'Utilisateur est la personne physique qui réalise le parcours client et qui signe le ou les Documents Métiers.

1.3.4. Tierce parties ou applications utilisatrices

Personne ou application qui valide le Certificat d'un Utilisateur dans le cadre de la validation de signature électronique de Document.

1.3.5. Autres participants

1.3.5.1. Opérateur d'enregistrement

L'Opérateur d'enregistrement est la personne physique qui a la responsabilité de valider l'identité des Utilisateurs grâce aux informations recueillies durant le Parcours client. Les

procédures d'identification sont variables en fonction du niveau de confiance demandé par le Client.

1.3.5.2. Client

Le Client désigne l'entité légale ayant contractualisé avec NETHEOS. Ces responsabilités sont décrites au § 8.5.

1.3.5.3. Autorité d'enregistrement déléguée

L'autorité d'enregistrement déléguée est l'autorité qui a en charge et en délégation de l'AE, la vérification de l'identité, des droits et de la qualité du demandeur du certificat électronique dans le cas où l'enregistrement est réalisé par un Client ou un Partenaire de NETHEOS. L'AED est contractuellement liée à l'AE.

1.4. Gestion de la PE/DPE

1.4.1. Entité gérant la PE/DPE

L'entité en charge de la gestion et de l'administration de la PE/DPE est la Direction de la société NETHEOS. Elle est responsable de la création, du suivi et de la modification de la PE/DPE.

Chaque trimestre, cette entité organise un comité de suivi de la présente PE/DPE afin d'évaluer les modifications devant y être apportées. Ces changements peuvent être motivés par des évolutions techniques, règlementaires ou bien organisationnelles.

1.4.2. Point de contact

Voici les coordonnées de la personne responsable de l'élaboration de la PE/DPE :

- M. David EMO ;
- Poste : Responsable produit ;
- Adresse : NETHEOS, 1025 avenue Henri Becquerel, Bâtiment 18 34000 Montpellier ;
- Email : d.emo@NETHEOS.net ;
- Téléphone : (+33) 9 72 34 11 80.

1.4.3. Entité déterminant la conformité de la Déclaration de Pratiques de ce document

La Direction procède à des audits réguliers des différents éléments constitutifs du service d'enregistrement et autorise ou non les demandes d'enregistrement.

1.4.4. Procédures d'approbation de la conformité de la Déclaration de Pratiques

La Direction évalue selon ses propres critères la conformité du présent document. Elle approuve les résultats des audits de conformité réalisés par les experts mandatés par elle.

1.5. Définitions et acronymes

1.5.1. Définitions

Audit : contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures.

Certificat : clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis**.**

Confidentialité : propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus.

Déclaration de pratiques d'enregistrement : désigne les pratiques et principes juridiques, commerciaux et techniques que NETHEOS, ses Clients et les Utilisateurs emploient pour garantir la validité de l'Enregistrement de l'Utilisateur dans le cadre d'une demande de Certificat auprès d'une Autorité de Certification intervenant lors d'un Parcours Client réalisé à distance ou en face à face.

Document métier : désigne un document électronique créé par le Client sous un format PDF et devant être signé par l'Utilisateur.

Données d'activation : valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un PIN, une phrase secrète, …).

Dossier de preuve : désigne les fichiers créés lors de la signature du Document électronique par l'Utilisateur désigné permettant d'assurer la validité de l'acte signé, l'identification de l'Utilisateur ainsi que l'ensemble des opérations réalisées sur le Document. Ce dossier permet d'assurer la traçabilité et la preuve de la réalisation de la signature en ligne en cas de procès.

Parcours client : désigne l'ensemble des étapes que suit un Utilisateur dans sa relation et ses interactions avec le Client.

Partenaire : un partenaire désigne une entité légale ayant contractualisé avec NETHEOS afin de revendre les services de NETHEOS sous son propre nom de marque.

Plan de continuité d'activité : le plan de continuité d'activité, a pour but de garantir la continuité du service de l'entreprise après un sinistre important touchant le système informatique. Il s'agit ici de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données.

Plan de reprise d'activité : le plan de reprise d'activité permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation. Le plan de reprise d'activité peut supposer une perte de données.

Politique d'enregistrement : désigne les procédures et les règles définies et mises en œuvre par l'Autorité d'Enregistrement pour identifier, authentifier les Utilisateurs et enregistrer les demandes d'émission, de renouvellement et de révocation des Certificats.

Protocole de consentement : désigne l'ensemble des règles de recueil de consentement pour un Parcours Client donné utilisant le Service à savoir (i) la définition des actions à réaliser par l'Utilisateur sur le Terminal d'affichage pour signer le Document métier proposé par l'Application Client, (ii) les informations utilisées pour la création de l'identité Utilisateur, (iii) les modalités de contrôle par le Service des informations saisies par l'Utilisateur par comparaison aux informations fournies par le Client pour chaque Transaction, (iv) le type de fichier soumis par le Client à signature (XML/PDF…), (v) les modalités de visualisation du Document métier présenté et du message d'acceptation (ou de refus) associé.

Service ("Trust and Sign") : désigne le service tel que défini dans la présente PE et fournit en mode SaaS. Le service permet aux Utilisateurs de signer des Documents métiers au sein d'un Parcours Client. Le service constitue et archive les dossiers d'enregistrement relatifs à l'identification et à l'authentification des Utilisateurs.

1.5.2. Acronymes

AC : Autorité de Certification.

AE : Autorité d'Enregistrement.

AED : Autorité d'Enregistrement Déléguée.

CGU : Conditions Générales d'Utilisation.

DPE : Déclaration de Pratiques d'Enregistrement.

IGC : Infrastructure de Gestion de Clés.

IP : Internet Protocol.

OID : Object Identifier.

PC : Politique de Certification.

PE : Politique d'Enregistrement.

PIN : Personal Identification Number.

PSGP : Politique de Signature et Gestion de Preuves.

2. Responsabilités concernant la mise à disposition des informations devant être publiées

2.1. Entités chargées de la mise à disposition des informations

NETHEOS est en charge de la publication des informations mentionnées au § 2.2 ci-dessous.

2.2. Informations devant être publiées

La direction de NETHEOS assure la publication des informations suivantes :

- La PE/DPE ;
- Les Conditions Générales d'Utilisation ("CGU") : les CGU sont rendues disponibles en fonction des acteurs selon les modalités suivantes :
    - Client : elles sont annexées au contrat signé entre le Client et NETHEOS ;
    - Utilisateur : la communication des CGU aux Utilisateurs est gérée au sein du Parcours Client ;

2.3. Délais et fréquences de publication

La PE/DPE est disponible en permanence et mise à jour selon les besoins.

2.4. Contrôle d'accès aux informations publiées

La direction de NETHEOS garantit l'intégrité des informations publiées et la traçabilité des modifications apportée à ces informations. L'accès aux informations dont la diffusion n'est pas prévue au § 2.2 est protégé.

L'ensemble des informations mentionnées au § 2.2 est disponible en lecture seule et en téléchargement sur Internet.

3. Identification et authentification

3.1. Validation initiale de l'identité

3.1.1. Méthode pour prouver la possession de la clé privée

La preuve de la possession de la clé privée par l'Utilisateur est réalisée par les procédures de génération de la clé privée (se reporter au § 6.1.1 ci-dessous) correspondant à la clé publique à certifier et par le mode d'activation et de gestion de la clé privée Utilisateur (se reporter au § 6.2 ci-dessous).

3.1.2. Validation de l'identité d'un Client

L'enregistrement du Client nécessite l'identification de l'entité légale, de la personne physique représentant cette entité et la preuve du rattachement de la personne physique à l'entité.

3.1.2.1. Identification de l'entité

L'enregistrement du Client nécessite un document en cours de validité au moment de la demande de certificat attestant de l'existence de l'entité et mentionnant le numéro SIREN de celle-ci (extrait Kbis ou certificat d'identification au répertoire national des entreprises ou inscription au répertoire des métiers, etc).

3.1.2.2. Identification de la personne physique représentant de l'entité

L'enregistrement du Client nécessite une copie d'au moins un document d'identité en cours de validité (passeport, carte nationale d'identité ou titre de séjour) de la personne physique représentant l'entité. Ce document doit mentionner l'identité complète de la personne physique incluant le prénom et le nom, la date et le lieu de naissance et un numéro national d'identité reconnu.

L'adresse électronique est également requise afin de permettre la communication avec la personne physique.

3.1.2.3. Preuve du rattachement de la personne physique à l'entité

L'enregistrement du Client nécessite un document, signé par le mandataire social ou un de ses délégataires, attestant du rattachement de cette personne à l'entité et de son habilitation à engager la responsabilité de l'entité.

3.1.3. Validation de l'identité d'un Utilisateur

3.1.3.1. A distance

Si l'Utilisateur n'a pas fait l'objet d'une vérification d'identité préalable par le Client, le dossier d'enregistrement comprend :

- Une copie d'au moins un document d'identité en cours de validité (passeport, carte nationale d'identité ou titre de séjour) de l'Utilisateur ou l'utilisation d'un moyen d'authentification issue d'une base de connaissance ou qui s'appuie sur un tiers ayant déjà authentifié l'Utilisateur ;
- L'identité complète de l'Utilisateur incluant le prénom et le nom, la date et le lieu de naissance et un numéro national d'identité reconnu.

La validation des informations d'identification de l'Utilisateur sont réalisées soit par l'Opérateur d'AE soit par un processus automatique équivalent ou soit par l'Opérateur d'AED.

Si l'Utilisateur a déjà fait l'objet d'une vérification d'identité préalable par l'AE ou par un tiers reconnu par l'AE, le Client doit utiliser un moyen d'authentification permettant de s'assurer que l'Utilisateur est bien la personne ayant fait l'objet de la vérification initiale (exemple : utilisation d'un compte protégé par un mot de passe, envoi d'un code unique aléatoire par SMS sur un numéro de téléphone mobile vérifié comme étant celui de l'Utilisateur, certificat, etc…). NETHEOS validera que l'identification préalable et les authentifications suivantes sont conformes à la présent PE/DPE ;

3.1.3.2. En face à face

Le Client devra s'assurer du respect des obligations suivantes :

- Identifier et authentifier les Utilisateurs lors d'un face-à-face avec l'Opérateur d'AED en demandant à l'Utilisateur de présenter au moins un document officiel d'identité en cours de validité (passeport, carte nationale d'identité ou titre de séjour) ;
- Documenter ses règles de vérification des informations de l'Utilisateur portées sur sa pièce d'identité officielle présentée à l'Opérateur d'AE et, pour les professionnels seulement, les informations portées dans les justificatifs d'appartenance à une entité légale le cas échéant sa fonction au sein de l'entité légale ;
- Collecter une copie des pièces justificatives de l'identité de l'Utilisateur ainsi que les données d'authentification ;
- Respecter la présente PE/DPE ;
- Informer l'Utilisateur de la gestion de ses données personnelles et des conditions générales d'utilisation ;
- Enfin, le Client devra avertir immédiatement NETHEOS pour tout incident de sécurité survenant lors de l'enregistrement.

3.1.4. Validation de l'identité d'une entité légale

Si l'Utilisateur appartient à une entité légale alors le Service vérifie l'existence de l'entité légale et que l'Utilisateur appartient effectivement à celle-ci.

Le dossier d'enregistrement comprend un document en cours de validité au moment de la demande de certificat attestant de l'existence de l'entité et mentionnant le numéro SIREN de celle-ci (extrait Kbis ou certificat d'identification au répertoire national des entreprises ou inscription au répertoire des métiers, etc) ou bien le résultat de l'interrogation automatique d'un référentiel officiel attestant de l'existence de l'organisation.

Le dossier d'enregistrement comprend également un document attestant du rattachement de cette personne à l'entité et de son habilitation à engager la responsabilité de l'entité ou bien le résultat de l'interrogation automatique d'un référentiel officiel attestant de l'habilitation de l'Utilisateur à représenter l'organisation.

3.1.5. Informations non vérifiées du signataire

La présente PE/DPE ne formule pas d'exigence particulière sur ce sujet.

3.1.6. Validation de l'autorité du demandeur

Les appels au Service ne pouvant s'effectuer qu'au sein d'un Parcours client et ceux-ci étant authentifiés techniquement, l'autorité de l'Utilisateur en lien avec le Client est reconnue comme valide.

3.2. Identification et validation d'une demande de renouvellement de clés

3.2.1. Identification et validation pour un renouvellement courant

Sans objet.

3.2.2. Identification et validation pour un renouvellement après révocation

Sans objet.

3.3. Identification et validation d'une demande de révocation

La demande de révocation devra être effectué par l'Utilisateur auprès du Client. Le Client transmettra alors la demande de révocation par email à NETHEOS.

La validation de la révocation sera alors confirmée via un appel téléphonique sur le téléphone de l'Utilisateur.

La révocation interviendra au plus tard 24 HEURES après la réception par l'AE de la demande de révocation de l'utilisateur.

4. Exigences opérationnelles sur le cycle de vie des certificats

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

La demande peut être réalisée par l'Utilisateur ou bien par le responsable de l'organisation rattachée à l'Utilisateur.

4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificats

Le Service recueille les informations suivantes afin de constituer la demande de certificat :

- Le nom d'usage, nom de naissance, prénom, la date et le lieu de naissance de l'Utilisateur ;
- Le SIREN, la raison sociale et l'adresse de l'organisation.

Afin de pouvoir contacter l'Utilisateur ou bien le responsable de l'organisation rattachée à l'Utilisateur, le Service recueille également l'adresse électronique et le numéro de téléphone.

4.2. Traitement d'une demande de certificat

4.2.1. Exécution des processus d'identification et de validation de la demande

Les identités sont vérifiées conformément aux exigences mentionnées au § 3.1.

Le Service vérifie donc :

- L'identité de l'Utilisateur ;
- Que l'Utilisateur a pris connaissance des CGU du Service.

Une fois ces vérifications effectuées, le Service émet la demande de certificat.

Le Service conserve une copie des éléments d'identification présentés sous forme électronique et procède à leur horodatage et à leur archivage.

4.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, le Service en informe l'Utilisateur en le justifiant.

4.2.3. Durée d'établissement du certificat

L'AE s'efforce de traiter la demande de certificat dans un délai raisonnable. Néanmoins, il n'y a aucune restriction concernant la durée maximale de traitement.

4.3. Délivrance du certificat

4.3.1. Actions de l'AC concernant la délivrance du certificat

Se référer à la politique de certification de l'AC.

4.3.2. Durée de vie du certificat

Se référer à la politique de certification de l'AC.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

Se référer à la politique de certification de l'AC.

4.4.2. Publication du certificat

Se référer à la politique de certification de l'AC.

4.5. Fonction d'information sur l'état des certificats

4.5.1. Caractéristiques opérationnelles

Sans objet.

4.5.2. Disponibilité de la fonction

Sans objet.

4.5.3. Dispositifs optionnels

Sans objet.

4.6. Fin d'abonnement

Sans objet.

5. Mesures de sécurité non techniques

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

Le site d'exploitation de l'OSC hébergeant l'AE respecte les règlements et normes en vigueur (Tier III) et son installation tient compte des résultats de l'analyse de risques, par exemple certaines exigences spécifiques de type inondation, explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques...). Le site d'exploitation (protégé par gardes et des détecteurs d'intrusion, ...) fournit une protection robuste contre les accès non autorisés aux équipements et données de l'AE.

5.1.2. Accès physique

Les équipements de l'AC et de l'AE sont protégés contre les accès non autorisés et les tentatives d'endommagement. La protection physique permet de s'assurer au minimum que :

- La surveillance, manuelle ou électronique, des accès autorisés et non autorisés est assurée ;
- Aucun accès non autorisé ne soit possible sur les équipements;
- Les supports d'informations papiers et informatiques qui contiennent des informations sensibles en clairs sont stockés dans des endroits sûrs ;
- Les personnes non autorisées soient toujours accompagnées par des personnes autorisées dans les locaux ;
- Un journal des accès soit maintenu ;
- Au moins deux (2) niveaux de barrières de sécurité sont mises en œuvres pour les accès aux équipements ;
- Les systèmes de sécurité physiques (par exemple, des serrures de porte, radars, caméras, ...) sont mis en oeuvre ;
- Les locaux sont protégés contre les accès non autorisés.

5.1.3. Alimentation électrique et climatisation

Le site de type "Tiers III" garantit une redondance de l'alimentation électrique et du système de climatisation.

5.1.4. Exposition aux dégâts des eaux

Les systèmes sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

5.1.5. Prévention et protection incendie

Le site de type "Tiers III" garantit une protection optimale contre les risques d'incendie.

5.1.6. Conservation des supports

Les supports (papier et numériques) sont conservés conformément aux procédures définies dans le cadre de l'exploitation de l'AE.

5.1.7. Mise hors service des supports

En fin de vie, les supports seront soit détruits soit réinitialisés en vue d'une réutilisation soit stockés dans un coffre-fort sécurisé.

5.1.8. Sauvegarde hors site

Des sauvegardes hors site sont réalisées permettant une reprise rapide des services de l'AE suite à la survenance d'un sinistre ou d'un événement conduisant à la corruption des données.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

Les rôles de confiance de l'AE sont classés avec les types de rôles de suivants :

- Les personnels d'exploitation, dont la responsabilité est le maintien des systèmes en conditions opérationnelles de fonctionnement et les sauvegardes ;
- Les personnels d'administration des services en ligne, dont la responsabilité est l'administration technique des composantes de l'AE ;
- Les personnels d'opération des services en ligne dont la responsabilité est de mettre en œuvre les fonctions de l'AE. On distingue ici deux profils d'opérateurs d'AE :
  - L'opérateur d'enregistrement, en charge de valider les dossiers d'enregistrement ;
  - L'opérateur de révocation, en charge de valider les demandes de révocation ;
- Les personnels d'audit système, dont la responsabilité est d'auditer les archives et les logs applicatifs ;
- Les personnels de « sécurité », dont la responsabilité est de réaliser les opérations de vérification de de la bonne application des mesures et de la cohérence de fonctionnement de la composante de l'AE.

5.2.2. Nombre de personnes requises par tâche

Les tâches dévolues aux différents rôles sont réalisées par au moins une personne. Les rôles sont répartis et gérés (gestion des congés et des arrêts maladie notamment) de manière à assurer une disponibilité constante pour chaque fonction de l'AE.

5.2.3. Identification et authentification pour chaque rôle

Pour chacun des membres du personnel ayant accès à l'AE (opération ou administration), l'identité et les autorisations sont vérifiées avant l'attribution d'un rôle ou des droits correspondants :

- Vérification du membre et ajout à la liste des rôles ;
- Ouverture d'un compte dans les systèmes concernés.

5.2.4. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles.

5.3. Mesures de sécurité vis à vis du personnel

5.3.1. Qualifications, compétences, et habilitations requises

Chaque personne amenée à travailler au sein de l'IGC est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles. Les personnels doivent être formés pour les rôles qu'ils occupent. Les rôles et leurs missions sont documentés afin de bien gérer la séparation des rôles et l'affectation de personne en fonction de la sensibilité des rôles et de leurs compétences, du contrôle des antécédents et de leurs formations.

5.3.2. Procédures de vérification des antécédents

La société NETHEOS met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

5.3.3. Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondants à la composante au sein de laquelle il opère. Cette formation couvre les aspects suivants :

- Règles de sécurité ;
- Logiciels d'AE en fonction de leur version ;
- Procédures applicables pour les services de l'AE ;
- Responsabilités du rôle ;
- Procédures pour la résolution des incidents et des litiges ;
- Connaissance minimale du système informatique de l'AE ;
- Procédure du plan de continuité.

Le personnel a eu connaissance et compris les implications des opérations dont il a la responsabilité.

5.3.4. Exigences en matière de formation continue et fréquences des formations

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5. Fréquence et séquence de rotations entre différentes attributions

La direction de NETHEOS s'assure que les changements de rôles n'affectent pas la sécurité des services de l'AE.

5.3.6. Sanctions en cas d'actions non autorisées

Les sanctions adéquates sont appliquées pour les personnels de l'AE ne respectant pas les règles de sécurité de la PE/DPE.

5.3.7. Exigences vis à vis du personnel des prestataires externes

Il est recommandé que les prestataires et les visiteurs soient accompagnés par un personnel de l'entité pour avoir accès aux locaux sensibles.

Les contrats passés avec des prestataires externes identifient les périmètres d'intervention, les responsabilités, les délais de dépannage, les garanties de qualité et les procédures de traitement d'un incident.

5.3.8. Documentation fournie au personnel

NETHEOS fournit au personnel en charge du service de l'AE les documentations nécessaires en fonction de leur attribution.

5.4. Procédures de constitution des données d'audit

5.4.1. Type d'événement à enregistrer

Les traces des événements suivants sont supposées être directement auditables, sans besoin de rapprochement avec d'autres. Pour cette raison, ils ne sont pas mentionnés dans le présent document. Ces traces sont alors consultables directement sur les équipements concernés. Le responsable de l'AE peut y avoir accès rapidement au travers d'une demande auprès des administrateurs de la plateforme.

Les évènements non concernés par le rapprochement des traces sont :

- Démarrage et arrêt des systèmes informatiques et des applications ;
- Événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion et déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes ;
- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel.

À l'inverse, les scénarios couvrent les évènements suivants :

- Réception de demande de création de dossier ;
- Visualisation d'un contrat ;
- Validation / rejet d'une demande de certificat ;
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Contrôle automatique d'une pièce justificative ;
- Archivage légal d'un dossier ;
- Acceptation ou rejet d'un dossier client.

5.4.2. Fréquence de traitement des journaux d'événements

Les journaux d'audits des composantes de l'AE sont revus sur une base trimestrielle par le responsable de l'audit qui conduit une recherche de preuves d'éventuelles activités malicieuses et de suivi des opérations sensibles.

Le responsable d'audit explique les évènements significatifs dans un rapport d'audit. Une telle revue implique de vérifier que les journaux n'ont pas été altérés, qu'il n'y a pas de discontinuité ou de perte dans les journaux, et par une revue rapide et synthétique de rechercher des incohérences dans les journaux d'audits.

5.4.3. Période de conservation des journaux d'événements

Les journaux sont accessibles 1 an avant d'être supprimés.

5.4.4. Protection des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

5.4.5. Procédure de sauvegarde des journaux d'événements

Le responsable sécurité met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements, conformément aux exigences de la politique de sécurité. Les sauvegardes des journaux sont protégées avec le même niveau de sécurité que les originaux.

5.4.6. Système de collecte des journaux d'événements

Les journaux d'évènement sont créés dès la mise en route d'un système et ne s'arrêtent que lorsque le système s'arrête. Le système de collecte des journaux permet de rassembler et de garantir l'intégrité et la disponibilité des journaux d'évènement. Si besoin est, le système de collecte des journaux protège les données en intégrité. Si un problème apparaît pendant la collecte des journaux, l'exploitant système détermine s'il est nécessaire de suspendre les opérations de la ou des composantes impactées avant d'avoir résolu le problème.

5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement

Chacun des événements enregistrés dans le système de collecte des journaux est associé à un serveur ou à un service.

5.4.8. Évaluation des vulnérabilités

Conformément à nos procédures d'audit, le responsable d'audit est chargé d'analyser les journaux pour détecter toute tentatives frauduleuses. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

5.5. Archivage des données

5.5.1. Types de données à archiver

L'archivage des données permet d'assurer la pérennité des journaux constitués par l'AE.

Les données archivées au niveau de chaque composante, sont les suivantes :

- Journaux :

- Accès physique (un an) ;
- Vidéo pour la protection des locaux (un mois) ;
- Gestion des rôles de confiance (10 ans) ;
- Accès aux systèmes d'information (5 ans) ;
- Logs des systèmes d'information et des réseaux (5 ans) ;
- Documentations de l'AE (5 ans) ;
- Incident de sécurité et rapports d'audit (10 ans) ;

- Documentation relative à l'audit gardé par l'entité gérant la PE/DPE (5 ans) ;
- Document PE/DPE (5 ans) ;
- Contrat entre NETHEOS et les Clients (5 ans) ;
- Type d'équipement, logiciel et configuration pour l'AC (5 ans) ;
- Autres données et applications utilisés pour la vérification des archives (5 ans) ;
- Tous les journaux relatifs au fonctionnement de l'entité gérant la PE/DPE et des audits (5 ans) ;
- Les dossiers d'enregistrement (7 ans).

5.5.2. Période de conservation des archives

La période de conservation des archives est donnée au § 5.5.1 ci-dessus.

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :

- Seront protégées en intégrité, confidentialité et authenticité ;
- Seront accessibles aux seules personnes autorisées ;
- Pourront être consultées et exploitées par les personnes autorisées.

5.5.4. Procédure de sauvegarde des archives

Si les supports utilisés pour le stockage des archives ne peuvent permettre de conserver les données conformément au délai de rétention défini au § 5.5.1, alors un mécanisme de transfert régulier d'archives sur un nouveau support sera mis en œuvre.

5.5.5. Exigences d'horodatage des données

Les éléments mentionnés au § 5.5.1 ne nécessitent pas d'horodatage fourni par un tiers horodateur. Tous les éléments disposent néanmoins d'un horodatage fourni par le composant sur lequel l'élément a été généré. Tous les composants sont synchronisés sur une même source de temps.

5.5.6. Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (Se reporter au § 5.4.6).

5.5.7. Procédure de récupération et de vérification des archives

Les archives sont régulièrement testées afin de s'assurer de leur contenu et de leur lisibilité. Seules les personnes autorisées et l'entité gérant la PE/DPE peuvent accéder aux archives.

5.6. Fin de vie des services de confiance

5.6.1. Transfert d'activité ou cessation d'activité affectant l'OSE

En cas de fin d'activité, l'AE effectue les actions suivantes :

- Notifier les Clients affectés ;
- Notifier l'AC ;
- Transférer les archives à une entité désignée par l'AE dont l'identité est communiquée à l'AC.

5.6.2. Cessation d'activité affectant l'activité AE

Afin de permettre au client d'assurer la continuité de ses activités, NETHEOS ainsi que ses prestataires assurent la réversibilité des données en fin de contrat.

Les actions et procédures décrites ci-dessous permettent de garantir la réversibilité :

- Maintien à jour des documentations techniques ou non techniques ;
- Possibilité d'exporter toutes les données du client (base de données, configurations, documents, archives) ;
- Purge des bases de données de NETHEOS ;
- Séquestre du code source à l'agence pour la protection des programmes (APP) ;
- Mise à disposition d'une assistance technique.

6. Mesures de sécurité techniques

6.1. Données d'activation

6.1.1. Génération et installation des données d'activation

6.1.1.1. Clé privée des porteurs

Se référer à la politique de certification de l'AC.

6.1.2. Protection des données d'activation

6.1.2.1. Clé privée des porteurs

Se référer à la politique de certification de l'AC.

6.1.3. Autres aspects liés aux données d'activation

6.1.3.1. Clé privée des porteurs

Se référer à la politique de certification de l'AC.

6.2. Mesures de sécurité des systèmes informatiques

6.2.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les exigences de sécurité technique spécifiques aux systèmes informatiques sont décrites dans la politique de sécurité des systèmes d'informations (PSSI) de NETHEOS. Cette politique aborde les objectifs de sécurité suivants :

- Identification et authentification ;
- Contrôle d'accès ;
- Intégrité des composants ;
- Sécurité des flux :
- Journalisation et audits ;
- Supervision et contrôle ;
- Sensibilisation.

6.2.2. Niveau d'évaluation de la sécurité des systèmes informatiques

Des audits sont planifiés par le responsable des audits internes en collaboration avec le responsable de la sécurité.

La fréquence des audits s'établit comme suit :

- Audits tous les ans minimum, diligentés par le responsable de la sécurité du système d'information ;
- Audits ponctuels : en cas de doute, de suspicion, sur le niveau de qualité de la gestion de l'infrastructure interne ou de l'AE.

6.3. Mesures de sécurité liées au développement des systèmes

6.3.1. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système ou d'une composante du Service « Trust and Sign » est documentée.

6.3.2. Niveau d'évaluation sécurité du cycle de vie des systèmes

L'implémentation du système permettant de mettre en œuvre les composantes du Service « Trust & Sign » est documentée. La configuration du système des composantes du Service « Trust & Sign » ainsi que toute modification et mise à niveau est documentée.

6.4. Mesures de sécurité réseau

Les mesures de sécurité réseau sont décrites dans la politique de sécurité des systèmes d'informations (PSSI) de NETHEOS.

6.5. Horodatage / système de datation

Sans objet.

7. Audit de conformité et autres évaluations

Pour s'assurer du niveau de sécurité de son infrastructure interne et de l'autorité d'enregistrement, NETHEOS a mis en place un processus d'audit.

7.1. Fréquences et / ou circonstances des évaluations

La fréquence des audits s'établit comme suit :

- Audits tous les ans minimum, diligentés par le responsable de la sécurité du système d'information ;
- Audits ponctuels : en cas de doute, de suspicion, sur le niveau de qualité de la gestion de l'infrastructure interne ou de l'AE.

7.2. Identités : qualification des évaluateurs

L'équipe d'audit système est constituée d'experts internes à la société NETHEOS spécialistes du domaine de la sécurité.

Cette équipe d'audit est constituée de personnes n'ayant pas de fonctions opérationnelles au sein de la société (cf. document des rôles).

Ces personnes sont soumises à des obligations de confidentialité, compte tenu des informations qui seront mises à leur disposition lors de ces audits.

Les auditeurs intervenant sont choisis parmi des personnes jugées compétentes en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée. Ils ont un rôle neutre au sein du système d'information.

7.3. Relations entre évaluateurs et entités évaluées

L'équipe d'auditeur est composée de personnes neutres. Celles-ci n'ont aucune fonction opérationnelle ou fonction de sécurité.

7.4. Actions prises suite aux conclusions des évaluations

Suite à un audit, s'il y a lieu, un plan de correctifs est mis en place. Celui-ci décrit les remarques faites par l'équipe d'audit ou par l'auditeur externe. Pour chacune de ces remarques, une priorité ainsi qu'une date de correction sont attribuées.

7.5. Communication des résultats

Les résultats des audits sont mis à la disposition du Client sur demande expresse de ce dernier.

8. Autres problématiques métiers et légales

8.1. Responsabilité financière

8.1.1. Couverture par les assurances

L'AE a souscrit une assurance responsabilité civile couvrant les risques liés à son activité professionnelle.

8.1.2. Autres ressources

Sans objet.

8.1.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

8.2. Confidentialité des données professionnelles

8.2.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- La partie non-publique de la DPE de l'AE,
- Les journaux d'événements des composantes de l'IGC,
- Les dossiers d'enregistrement des porteurs.

8.2.2. Informations hors du périmètre des informations confidentielles

Sans objet.

8.2.3. Responsabilités en termes de protection des informations confidentielles

NETHEOS applique des procédures de sécurité pour garantir la confidentialité des informations confidentielles. NETHEOS s'engage à respecter la législation et la réglementation en vigueur sur le territoire français.

8.3. Protection des données personnelles

8.3.1. Politique de protection des données personnelles

NETHEOS respecte la législation et la réglementation en vigueur sur le territoire français.

Les traitements réalisés sur les données par le Service font l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés ("CNIL").

Le respect de ces obligations est contrôlé par un Correspondant Informatique et Liberté.

8.3.2. Informations à caractère personnel

Les données personnelles sont l'ensemble des informations présentes dans le dossier d'enregistrement.

8.3.3. Informations à caractère non personnel

Sans objet.

8.3.4. Responsabilité en termes de protection des données personnelles

Se reporter à la législation et la réglementation en vigueur sur le territoire français.

8.3.5. Notification et consentement d'utilisation des données personnelles

Conformément à la législation et la réglementation en vigueur sur le territoire français, les informations personnelles de l'Utilisateur ne sont pas transmises ou communiquées à des tiers sauf dans les cas d'une procédure judiciaire ou d'une demande émanant de l'Utilisateur.

8.3.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Se reporter à la législation et la réglementation en vigueur sur le territoire français.

8.3.7. Autres circonstances de divulgation d'informations personnelles

Sans objet.

8.4. Droits sur la propriété intellectuelle et industrielle

NETHEOS détient tous les droits, titres et intérêts relatifs au Service, y compris tous les droits de propriété intellectuelle qui subsistent dans le Service ou qui sont associés aux systèmes ou aux logiciels mis en place pour opérer le Service.

L'utilisation du Service ne confère au Client ou à l'Utilisateur aucun droit de propriété intellectuelle sur le Service ni sur les contenus auxquels il peut accéder (marques, logos, images, sources informatiques, documentations, etc.).

L'Utilisateur détient tous les droits de propriété intellectuelle sur ses données personnelles présentes dans le dossier d'enregistrement.

8.5. Interprétations contractuelles et garanties

L'AE, les Clients et les Utilisateurs sont responsables des dommages occasionnés suite à un manquement à leurs obligations respectives telles que définis dans la présente PE/DPE et dans les CGU.

8.5.1. Les obligations de l'AE

- L'AE s'engage à respecter la présente PE/DPE et les CGU ;
- L'AE s'engage à respecter la PC et la DPC de l'AC ;
- L'AE s'engage à rendre disponible les CGU à l'Utilisateur avant la signature des Documents Métier ;
- L'AE s'engage à protéger les données d'activation ;
- L'AE s'engage à collecter les données et pièces justificatives permettant de valider l'identité de l'Utilisateur ;
- L'AE s'engage à alerter l'AC en cas d'incident de sécurité ayant des conséquences sur le processus d'enregistrement et de signature;
- L'AE s'engage à alerter les Clients et les AED en cas d'incident de sécurité ayant des conséquences sur le processus d'enregistrement et de signature ;
- L'AE s'engage à protéger les données personnelles des Utilisateurs.
- L'AE s'engage à être audité par l'AC sur les pratiques mises en œuvre et pour s'assurer des exigences respectées par l'AE.

8.5.2. Les obligations du Client en tant qu'AED

- L'AED s'engage à respecter la présente PE/DPE et les CGU ;
- L'AED s'engage à respecter la PC et la DPC de l'AC ;
- L'AED s'engage à rendre disponible les CGU à l'Utilisateur avant la signature du Document ;
- L'AED s'engage à collecter les données et pièces justificatives permettant de valider l'identité de l'Utilisateur ;
- L'AED s'engage à signer le contrat qui la lie à NETHEOS et l'engage en qualité d'AED et à en respecter les termes ;
- L'AED s'engage à documenter ses procédures internes de fonctionnement à l'attention de son personnel dans le cadre des fonctions qui lui sont dévolues en qualité d'AED ;
- L'AED s'engage à accepter les audits de conformité à la présente PE/DPE et à remédier aux non-conformités qui pourraient être révélées. Ces audits peuvent être menés par l'AE ou l'AC ;
- L'AED s'engage à alerter l'AE en cas d'incident de sécurité ayant des conséquences sur le processus d'enregistrement et de signature.

8.5.3. Les obligations du Client

- Le Client s'engage à respecter la présente PE/DPE et les CGU ;
- Le Client s'engage à mettre en œuvre les moyens techniques et humains adéquats nécessaires à la réalisation des prestations auxquelles il s'engage ;
- Le Client s'engage à accepter les audits de conformité à la présente PE/DPE et à remédier aux non-conformités qui pourraient être révélées. Ces audits peuvent être menés par l'AE ou l'AC ;
- Le Client s'engage à alerter l'AE en cas d'incident de sécurité sur le processus d'enregistrement et de signature ;
- Le Client s'engage à alerter les Utilisateurs concernés en cas d'incident de sécurité sur le processus d'enregistrement et de signature ;
- Le Client s'engage à protéger les données personnelles des Utilisateurs.
- Le Client s'engage à choisir et à définir le Protocole de consentement et le type de donnée d'activation associées.

8.5.4. Les obligations de l'Utilisateur

- L'Utilisateur s'engage à protéger la confidentialité des données d'activation afin d'en éviter un usage non autorisé ;
- L'Utilisateur s'engage à respecter les CGU ;
- L'Utilisateur s'engage à fournir des informations complètes et correctes à l'AE ou le cas échéant à l'AED ;
- L'Utilisateur s'engage à alerter le Client en cas d'incident de sécurité sur le processus d'enregistrement et de signature ;

• L'Utilisateur s'engage à avertir immédiatement l'AE ou le cas échéant à l'AED en cas de non-conformité détectée sur son identité inscrite dans le certificat émis.

8.6. Limite de garantie

Sans objet.

8.7. Limite de responsabilité

L'offre du service est soumise à une obligation de moyens, dans les limites de ce qui est commercialement raisonnable et fait cependant l'objet d'une limitation de garantie.

Sauf tel qu'expressément prévu par la présente PE/DPE ou par les conditions d'utilisation générales, ni NETHEOS, ni ses fournisseurs ou distributeurs, ne font aucune promesse spécifique concernant les services. Par exemple, NETHEOS ne s'engage aucunement concernant le contenu des services, les fonctionnalités spécifiques disponibles par le biais des services, leur fiabilité, leur disponibilité ou leur adéquation à répondre aux besoins du client. NETHEOS fournit le service « en l'état ».

Certaines juridictions n'autorisent pas l'exclusion de certaines garanties, telles que la garantie implicite de qualité marchande, d'adéquation à répondre à un usage particulier et de conformité. Dans les limites permises par la loi, NETHEOS exclut toute garantie.

Dans les limites permises par la loi, NETHEOS, ses fournisseurs et distributeurs, déclinent toute responsabilité pour les pertes de bénéfices, de revenus ou de données, ou les dommages et intérêts indirects, spéciaux, consécutifs, exemplaires ou punitifs.

Dans les limites permises par la loi, la responsabilité totale de NETHEOS, de ses fournisseurs et distributeurs, pour toute réclamation dans le cadre des présentes conditions d'utilisation, y compris pour toute garantie implicite, est limitée au montant que le Client a payé pour utiliser le service.

En aucun cas, NETHEOS, ses fournisseurs et distributeurs ne seront tenus responsables pour toute perte ou dommage qui n'aurait pas été raisonnablement prévisible.

8.8. Indemnités

Sans objet.

8.9. Durée et fin anticipée de validité de la Politique d'Enregistrement et Déclaration de Pratiques d'Enregistrement

8.9.1. Durée de validité

Cette PE/DPE reste en application jusqu'à la publication d'une nouvelle version.

8.9.2. Fin anticipée de validité

Cette PE/DPE reste en application jusqu'à la publication d'une nouvelle version.

8.9.3. Effets de la fin de validité et clauses restant applicables

Sans objet.

8.10. Notifications individuelles et communications entre les participants

La Direction de NETHEOS met à disposition la nouvelle version de la PE/DPE dès qu'elle est disponible.

8.11. Amendements à la Politique d'Enregistrement et Déclaration de pratiques d'Enregistrement

8.11.1. Procédures d'amendements

La Direction de NETHEOS révise cette PE/DPE au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion de la Direction de NETHEOS.

8.11.2. Mécanisme et période d'information sur les amendements

Lors de tout changement important de cette PE/DPE, NETHEOS informera les différents acteurs de son intention de modifier sa PE/DPE avant de procéder aux changements et en fonction de l'objet de la modification. Cette communication sera réalisée par voie électronique.

8.11.3. Circonstances selon lesquelles l'OID doit être changé

Si les modifications apportées à la présente PE/DPE sont assez importantes, son OID sera modifié de manière à permettre d'identifier les exigences associées à une procédure d'enregistrement.

8.12. Dispositions concernant la résolution de conflits

En cas de contestation sur l'interprétation ou l'exécution de l'une quelconque des dispositions de la présente PE/DPE et au cas où les parties ne parviendraient pas à un accord amiable dans les quarante-cinq (45) jours suivant la survenance du différend sauf à ce que ce délai soit prolongé expressément entre elles, les tribunaux situés dans le ressort de la Cour de Grande Instance de Montpellier seront seuls compétents pour connaître de tout différend, nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence ou les procédures conservatoires par voie de référé ou requête ou encore opposition sur injonction de payer.

8.13. Juridictions compétentes

Se reporter au § 8.12.

8.14. Conformité aux législations et réglementations

Cette PE/DPE est sujette à la législation et la réglementation en vigueur sur le territoire français.

8.15. Dispositions diverses

8.15.1. Accord global

Sans objet.

8.15.2. Transfert d'activités

Sans objet.

8.15.3. Conséquences d'une clause non valide

Sans objet.

8.15.4. Application et renonciation

Sans objet.

8.15.5. Force majeure

NETHEOS ne pourra être tenu pour responsable, ou considéré comme ayant failli aux conditions de la présente PE/DPE, pour tout retard ou inexécution, lorsque la cause du retard ou de l'inexécution est liée à un cas de force majeure.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuits, ceux habituellement retenus par la jurisprudence des cours et tribunaux français, en application de l'article 1148 du Code civil, ainsi que les événements suivants : la guerre, l'émeute, l'incendie, les grèves internes ou externes à l'entreprise, occupation des locaux, intempéries, tremblement de terre, tempête, inondation, dégât des eaux, restrictions légales ou gouvernementales, modifications légales ou réglementaires des formes de commercialisation, épidémie, pandémie, l'absence de fourniture d'énergie, pannes d'électricité, du réseau ou des installations ou réseaux de télécommunications, l'arrêt partiel ou total du réseau Internet et, de manière plus générale, des réseaux de télécommunications privés ou publics, tout incident survenant sur le réseau d'un opérateur tiers les blocages de routes et les impossibilités d'approvisionnement en fournitures et tout autre cas indépendant de la volonté expresse de NETHEOS empêchant l'exécution normale du Service.

8.16. Autres dispositions

Sans objet.

8.17. Conditions générales d'utilisation de l'AE

Présentation du service

Le Service Trust and Sign (ci-après « Trust and Sign » ou « Service ») est une solution de contractualisation numérique et de validation de dossiers numériques éditée et opérée par NETHEOS.

Toute utilisation du Service est soumise aux Conditions Générales d'Utilisation du service Trust and Sign qui constituent l'intégralité de l'accord entre l'Utilisateur et NETHEOS, à l'exclusion de toutes autres dispositions.

L'Utilisateur reconnaît et accepte que NETHEOS (ou les concédants de NETHEOS) détienne tous les droits, titres et intérêts relatifs au Service, y compris tous droits de propriété intellectuelle qui subsistent dans le Service ou qui sont associés aux systèmes ou aux logiciels mis en place pour opérer le Service.

L'Utilisateur reconnaît également que le Service peut contenir des informations désignées comme confidentielles par NETHEOS et que l'Utilisateur ne doit pas divulguer ces informations sans le consentement préalable écrit de NETHEOS.

Utilisation du Service

L'Utilisateur doit respecter les règles applicables au Service.

L'Utilisateur s'engage à ne pas utiliser le Service de manière impropre qui dégrade le Service ou les serveurs et réseaux connectés au Service.

L'Utilisateur s'engage à utiliser le Service dans le respect des lois en vigueur y compris les lois et réglementations applicables concernant le contrôle des exportations et ré-exportations. NETHEOS pourra suspendre ou cesser la fourniture du Service si l'Utilisateur ne respecte pas les Conditions Générales d'Utilisation.

L'utilisation du Service ne confère à l'Utilisateur aucun droit de propriété intellectuelle sur le Service ni sur les contenus auxquels il peut accéder (images, sources informatiques, documentations, etc). Ces Conditions Générales d'Utilisation ne confèrent pas à l'Utilisateur le droit d'utiliser une quelconque marque ou un quelconque logo présent dans le Service.

L'Utilisateur n'est pas autorisé à supprimer, masquer ou modifier les notices juridiques affichées dans ou avec le Service.

L'Utilisateur est seul responsable (et NETHEOS n'a aucune responsabilité envers l'Utilisateur ou envers toute tierce partie) pour tout manquement à ses obligations en vertu des Conditions Générales d'Utilisation, et pour les conséquences de toute violation (y compris toute perte ou dommage que pourrait subir NETHEOS).

Information de contact

Voici les coordonnées de la personne à contacter pour toutes questions relatives à ces conditions générales d'utilisation :

- M. David EMO ;
- Poste : Responsable produit ;
- Adresse : Netheos, 1025 avenue Henri Becquerel, Bâtiment 18 34000 Montpellier ;
- Email : hello@netheos.com ;
- Téléphone : (+33) 9 72 34 11 80.

Description du processus d'enregistrement

L'enregistrement de l'Utilisateur nécessite la constitution d'un dossier d'enregistrement.

A distance, si l'Utilisateur n'a pas fait l'objet d'une vérification d'identité préalable, le dossier d'enregistrement comprend :

- Une copie d'au moins un document d'identité en cours de validité (passeport, carte nationale d'identité ou titre de séjour) de l'Utilisateur ou l'utilisation d'un moyen d'authentification issue d'une base de connaissance ou qui s'appuie sur un tiers ayant déjà authentifié l'Utilisateur ;
- L'identité complète de l'Utilisateur incluant le prénom et le nom, la date et le lieu de naissance et un numéro national d'identité reconnu.

La validation des informations d'identification de l'Utilisateur sont réalisées soit par l'Opérateur d'AE soit par un processus automatique équivalent.

Si l'Utilisateur a déjà fait l'objet d'une vérification d'identité préalable par l'AE ou par un tiers reconnu par l'AE, l'Utilisateur doit utiliser un moyen d'authentification permettant de s'assurer qu'il est bien la personne ayant fait l'objet de la vérification initiale (exemple : utilisation d'un compte protégé par un mot de passe, envoi d'un code unique aléatoire par SMS sur un numéro de téléphone mobile vérifié comme étant celui de l'Utilisateur, certificat, etc…)

En face à face, le Client devra s'assurer du respect des obligations suivantes :

- Identifier et authentifier les Utilisateurs lors d'un face-à-face avec l'Opérateur d'AED en demandant à l'Utilisateur de présenter au moins un document officiel d'identité en cours de validité (passeport, carte nationale d'identité ou titre de séjour) ;
- Documenter ses règles de vérification des informations de l'Utilisateur portées sur sa pièce d'identité officielle présentée à l'Opérateur d'AE et, pour les professionnels seulement, les informations portées dans les justificatifs d'appartenance à une entité légale le cas échéant sa fonction au sein de l'entité légale ;

- Collecter une copie des pièces justificatives de l'identité de l'Utilisateur ainsi que les données d'authentification ;

- Respecter la Politique d'Enregistrement et Déclaration de Pratiques d'Enregistrement du Service ;

- Informer l'Utilisateur de la gestion de ses données personnelles et des conditions générales d'utilisation.

Enfin, le Client devra avertir immédiatement NETHEOS pour tout incident de sécurité survenant lors de l'enregistrement.

Si l'Utilisateur appartient à une entité légale alors le Service vérifie l'existence de l'entité légale et que l'Utilisateur appartient effectivement à celle-ci.

Le dossier d'enregistrement comprend un document en cours de validité au moment de la demande de certificat attestant de l'existence de l'entité et mentionnant le numéro SIREN de celle-ci (extrait Kbis ou certificat d'identification au répertoire national des entreprises ou inscription au répertoire des métiers, etc) ou bien le résultat de l'interrogation automatique d'un référentiel officiel attestant de l'existence de l'organisation.

Le dossier d'enregistrement comprend également un document attestant du rattachement de cette personne à l'entité et de son habilitation à engager la responsabilité de l'entité ou bien le résultat de l'interrogation automatique d'un référentiel officiel attestant de l'habilitation de l'Utilisateur à représenter l'organisation.

Limites de responsabilité

L'offre du service est soumise à une obligation de moyens, dans les limites de ce qui est commercialement raisonnable et fait cependant l'objet d'une limitation de garantie.

Sauf tel qu'expressément prévu par la Politique d'Enregistrement et Déclaration de pratiques d'Enregistrement ou par les Conditions d'Utilisation Générales, ni NETHEOS, ni ses fournisseurs ou distributeurs, ne font aucune promesse spécifique concernant les services. Par exemple, NETHEOS ne s'engage aucunement concernant le contenu des services, les fonctionnalités spécifiques disponibles par le biais des services, leur fiabilité, leur disponibilité ou leur adéquation à répondre aux besoins du client. NETHEOS fournit le service « en l'état ».

Certaines juridictions n'autorisent pas l'exclusion de certaines garanties, telles que la garantie implicite de qualité marchande, d'adéquation à répondre à un usage particulier et de conformité. Dans les limites permises par la loi, NETHEOS exclut toute garantie.

Dans les limites permises par la loi, NETHEOS, ses fournisseurs et distributeurs, déclinent toute responsabilité pour les pertes de bénéfices, de revenus ou de données, ou les dommages et intérêts indirects, spéciaux, consécutifs, exemplaires ou punitifs.

Dans les limites permises par la loi, la responsabilité totale de NETHEOS, de ses fournisseurs et distributeurs, pour toute réclamation dans le cadre des présentes conditions d'utilisation, y compris pour toute garantie implicite, est limitée au montant que le Client a payé pour utiliser le service.

En aucun cas, NETHEOS, ses fournisseurs et distributeurs ne seront tenus responsables pour toute perte ou dommage qui n'aurait pas été raisonnablement prévisible.

Références des documents applicables

042017_C1_DEM_v1.0_politique_d_enregistrement_et_declaration_des_pratiques_d_enregistrement

Protection des données personnelles

NETHEOS respecte la législation et la réglementation en vigueur sur le territoire français.

Les traitements réalisés sur les données par le Service font l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés ("CNIL").

Le respect de ces obligations est contrôlé par un Correspondant Informatique et Liberté.

Les données personnelles sont l'ensemble des informations présentes dans le dossier d'enregistrement.

Pour connaître les responsabilités en termes de protection des données personnelles, se reporter à la législation et la réglementation en vigueur sur le territoire français.

Conformément à la législation et la réglementation en vigueur sur le territoire français, les informations personnelles de l'Utilisateur ne sont pas transmises ou communiquées à des tiers sauf dans les cas d'une procédure judiciaire ou d'une demande émanant de l'Utilisateur.

Pour connaître les conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives, se reporter à la législation et la réglementation en vigueur sur le territoire français.

Loi applicable et tribunal compétent

Ces conditions générales d'utilisation sont sujettes à la législation et la réglementation en vigueur sur le territoire français.

En cas de contestation sur l'interprétation ou l'exécution de l'une quelconque des dispositions des présentes CGU et au cas où les parties ne parviendraient pas à un accord amiable dans les quarante-cinq (45) jours suivant la survenance du différend sauf à ce que ce délai soit prolongé expressément entre elles, les tribunaux situés dans le ressort de la Cour de Grande Instance de Montpellier seront seuls compétents pour connaître de tout différend, nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence ou les procédures conservatoires par voie de référé ou requête ou encore opposition sur injonction de payer.

Liste des certificats et audits externes réalisés

À propos de ces conditions

NETHEOS peut apporter des modifications aux Conditions Générales d'Utilisation de temps en temps par exemple, pour refléter des modifications de la loi ou du Service. Lorsque ces modifications sont apportées, NETHEOS publiera une nouvelle version des Conditions Générales d'Utilisation à l'adresse http://www.netheos.com/cgu.

Si l'Utilisateur n'accepte pas les modifications apportées aux Conditions Générales d'Utilisation d'un Service donné, il doit cesser toute utilisation de ce Service.

L'Utilisateur reconnaît et accepte que s'il utilise le Service après la date à laquelle les Conditions Générales d'Utilisation sont applicables, NETHEOS traitera son utilisation comme l'acceptation des Conditions Générales d'Utilisation mises à jour.

Ces Conditions Générales d'Utilisation constituent la totalité du contrat juridique entre l'Utilisateur et NETHEOS et régissent l'utilisation du Service par l'Utilisateur.

L'Utilisateur convient que si NETHEOS n'exerce pas ou n'applique pas tout droit ou recours qui est contenu dans les Conditions Générales d'Utilisation (ou dont NETHEOS a l'avantage en vertu de toute loi applicable), cela ne peut pas être considéré comme une renonciation formelle des droits de NETHEOS et ces droits ou recours seront toujours disponibles pour NETHEOS.

Mentions légales

NETHEOS

Siège Social : 1025 Avenue Henri Becquerel, Parc Club du Millénaire, Bâtiment 18 - 34 000 Montpellier - France - Tel : 09 72 34 11 80

SAS au capital de 181 023,856 € - Siren : 45302368100043 - Code APE : 5829C - RCS Montpellier - France