**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES**

Marché n°2026-0079-00-00 MPA

Acheteur

Numih France

12 rue Michel Labrousse

CS 93668

31036 Toulouse Cedex 1

Siret n° 18310021300028

Outil de gestion des registres des traitements, des sous-traitants dans le cadre du RGPD

NB : Tout comme l'ensemble des documents de la consultation, le présent document ne peut être modifié à l'initiative du Titulaire.

SOMMAIRE

Article 1.	Introduction.....	4
Article 2.	Objet du marché	4
Article 3.	Présentation de Numih France	4
Article 4.	Réglementations applicables au marché.....	4
4.1	Réglementations applicables au marché.....	4
4.1.1	Règlementation relative à la protection des données à caractère personnel	5
4.1.2	Sécurité des systèmes d'information et confidentialité.....	5
4.1.3	Droit de la commande publique	5
4.1.4	Évolutions réglementaires.....	5
4.2	Réglementations complémentaires applicables au contexte du marché	6
4.2.1	Règlementation relative à la protection des données à caractère personnel	6
4.2.2	Réglementations nationales et européennes relatives à la sécurité numérique	6
4.2.3	Référentiels, normes et bonnes pratiques	6
4.2.4	Réglementations sectorielles spécifiques	6
4.2.5	Évolutions réglementaires.....	6
Article 5.	Description du besoin	6
5.1	Configuration minimale et prérequis techniques.....	7
5.2	Fonctionnalités obligatoires de la solution	7
5.3	Sécurité : traçabilité, sauvegardes, confidentialité et habilitations	9
5.4	Disponibilité, maintenance et assistance	9
Article 6.	Gestion des utilisateurs et des profils	9
Article 7.	Conditions d'exécution des prestations	9
7.1	Hébergement du service dans le data center de Numih France.....	9
7.1.1	Intervention à distance	9
7.1.2	Supervision du service.....	10
7.2	Support.....	11
7.3	Niveau d'engagement en cas d'incident	11
7.4	Réversibilité	12
Article 8.	Audit	Erreur ! Signet non défini.
8.1	Objet et périmètre.....	Erreur ! Signet non défini.
8.2	Fréquence et typologie des audits.....	Erreur ! Signet non défini.
8.3	Préavis et audits inopinés.....	Erreur ! Signet non défini.

- 8.4 Protection du secret des affaires, confidentialité et sécurité **Erreur ! Signet non défini.**
- 8.5 Gestion des sous-traitants et substitués du Titulaire **Erreur ! Signet non défini.**
- 8.6 Coûts **Erreur ! Signet non défini.**
- 8.7 Modalités pratiques d'audit..... **Erreur ! Signet non défini.**
- 8.8 Plan d'actions correctives et délais..... **Erreur ! Signet non défini.**
- 8.9 Ré-audits de vérification **Erreur ! Signet non défini.**
- 8.10 Conservation de la preuve et journaux..... **Erreur ! Signet non défini.**
- 8.11 Manquements, sanctions et résiliation **Erreur ! Signet non défini.**
- 8.12 Articulation avec la commande publique et les documents contractuels
Erreur ! Signet non défini.

Article 9. Sécurité 13

5. Incident de sécurité 13
6. Correction des vulnérabilités techniques 13

Article 1. Introduction

Ce document constitue le cahier des clauses techniques particulières (CCTP) pour l'acquisition d'un outil logiciel de gouvernance des données à caractère personnel. Ce CCTP décrit le projet dans sa globalité.

Le logiciel aura vocation à être utilisé par Numih France ainsi que ses adhérents, dans le cadre de l'offre d'accompagnement RGPD proposée par le GIP.

Article 2. Objet du marché

Le présent marché a pour objet la fourniture, la mise en œuvre et la maintenance d'un outil logiciel de gouvernance des données à caractère personnel, destiné à accompagner Numih France ainsi que ses adhérents et clients dans le pilotage et la mise en conformité des obligations liées à la protection des données, conformément au règlement (UE) 2016/679 (RGPD) et aux textes nationaux applicables.

Le marché porte notamment sur :

- la mise à disposition d'une solution logicielle de gouvernance RGPD, accessible en mode SaaS ou hébergé chez Numih France ;
- les prestations de paramétrage, de déploiement et d'accompagnement à la prise en main de la solution, avec reprise des données existantes sur SmartGlobal ;
- la maintenance évolutive et corrective ainsi que l'assistance technique et fonctionnelle associées.

La solution devra permettre de centraliser, structurer, documenter et piloter l'ensemble des éléments constitutifs de la conformité RGPD, notamment :

- la gestion des registres de traitements de données à caractère personnel ;
- la documentation des obligations réglementaires ;
- le suivi des actions de conformité et de gouvernance des données ;
- Registre des violations de données ;
- Registre d'exercice des droits des personnes concernées
- La réalisation d'analyse d'impact...

Ce marché s'inscrit dans une démarche de conformité durable, outillée et évolutive, visant à sécuriser les traitements de données personnelles mis en œuvre par le GIP ainsi que ses adhérents accompagnés dans leur mise en conformité RGPD.

Article 3. Présentation de Numih France

Numih France est une structure publique de coopération spécialisée dans l'informatique, travaillant avec des établissements de santé, collectivités territoriales et services déconcentrés de l'État répartis sur l'ensemble du territoire

Éditeur de progiciels hospitaliers et de santé sur des domaines complémentaires s'appuyant sur des dizaines d'années d'expérience, et hébergeur de données de santé certifié depuis 2018, Numih France accompagne les établissements de santé dans la construction et le développement de leur système d'information.

Article 4. Réglementations applicables au marché

4.1 Réglementations applicables au marché

Dans le cadre de l'exécution du présent marché, le titulaire s'engage à respecter l'ensemble des dispositions législatives et réglementaires applicables, en vigueur à la date de notification du marché et pendant toute sa durée d'exécution.

Les obligations listées ci-après ne sont pas exhaustives et n'exonèrent pas le titulaire de son devoir général de conformité.

4.1.1 Règlementation relative à la protection des données à caractère personnel

Le titulaire devra se conformer strictement aux dispositions suivantes :

- **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016** relatif à la protection des données à caractère personnel (RGPD) ;
- **Loi n° 78-17 du 6 janvier 1978 modifiée** relative à l'informatique, aux fichiers et aux libertés ;
- textes réglementaires nationaux et européens pris pour l'application du RGPD ;
- recommandations, lignes directrices et référentiels publiés par la CNIL et, le cas échéant, par le Comité européen de la protection des données (CEPD), lorsqu'ils sont pertinents au regard de l'objet du marché.

Dans le cadre de la fourniture de la solution, le titulaire interviendra en qualité de sous-traitant au sens de l'article 28 du RGPD, pour le compte de Numih France et, le cas échéant, des structures adhérentes bénéficiant de l'offre RGPD portée par le GIP. À ce titre, une annexe RGPD devra être signée entre les parties.

4.1.2 Sécurité des systèmes d'information et confidentialité

Le titulaire devra respecter les règles applicables en matière de sécurité des systèmes d'information, notamment :

- les principes généraux de sécurité définis par l'ANSSI, lorsqu'ils sont pertinents au regard de la nature de la solution proposée ;
- les exigences relatives à la confidentialité, à l'intégrité, à la disponibilité et à la traçabilité des données ;
- les obligations de sécurité applicables aux prestataires manipulant des données sensibles ou confidentielles.

Lorsque la solution est hébergée, le titulaire devra respecter les réglementations applicables à l'hébergement des données, notamment en matière de localisation des données et de maîtrise de la chaîne de sous-traitance.

4.1.3 Droit de la commande publique

Le titulaire est tenu de respecter les dispositions applicables en matière de commande publique, notamment :

- le Code de la commande publique ;
- les principes de liberté d'accès à la commande publique, d'égalité de traitement des candidats et de transparence des procédures.

4.1.4 Évolutions réglementaires

Le titulaire s'engage à prendre en compte, pendant toute la durée du marché, les évolutions législatives et réglementaires impactant l'objet du marché, notamment en matière de protection des données à caractère personnel, et à proposer les adaptations nécessaires de la solution, sans remise en cause de l'équilibre économique du marché.

4.2 Réglementations complémentaires applicables au contexte du marché

Le Titulaire est tenu de respecter l'ensemble des réglementations complémentaires, normes et référentiels applicables, en vigueur à la date de notification du marché ou entrant en vigueur au cours de son exécution, dès lors qu'ils couvrent le champ fonctionnel du présent marché.

Cette obligation inclut notamment, sans que cette liste soit exhaustive :

4.2.1 Règlementation relative à la protection des données à caractère personnel

Le titulaire devra se conformer strictement aux dispositions suivantes :

- **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016** relatif à la protection des données à caractère personnel (RGPD) ;
- **Loi n° 78-17 du 6 janvier 1978 modifiée** relative à l'informatique, aux fichiers et aux libertés ;
- textes réglementaires nationaux et européens pris pour l'application du RGPD ;
- recommandations, lignes directrices et référentiels publiés par la CNIL et, le cas échéant, par le Comité européen de la protection des données (CEPD), lorsqu'ils sont pertinents au regard de l'objet du marché.

4.2.2 Réglementations nationales et européennes relatives à la sécurité numérique

- dispositions législatives et réglementaires relatives à la **sécurité des systèmes d'information** ;
- **directive (UE) 2022/2555 dite "NIS 2"**, transposée en droit national, lorsque le périmètre du marché ou les entités concernées entrent dans son champ d'application ;
- textes nationaux relatifs à la résilience, à la continuité et à la sécurité des services numériques.

4.2.3 Référentiels, normes et bonnes pratiques

- référentiels, guides et recommandations publiés par la CNIL ;
- référentiels et bonnes pratiques publiées par l'ANSSI ;
- normes et standards internationaux pertinents (notamment ISO/IEC 27001, ISO/IEC 27701, ou équivalents), lorsqu'ils sont applicables aux prestations fournies.

4.2.4 Réglementations sectorielles spécifiques

Lorsque les adhérents du GIP relèvent de secteurs soumis à des obligations spécifiques, le titulaire devra se conformer aux réglementations applicables, notamment :

- réglementations relatives aux données de santé, le cas échéant ;
- réglementations applicables aux organismes publics ou parapublics ;
- obligations spécifiques liées à la nature des missions exercées par les structures adhérentes.

4.2.5 Évolutions réglementaires

Le titulaire s'engage à assurer une veille réglementaire sur les textes applicables au champ fonctionnel du marché et à adapter la solution, le cas échéant, afin de garantir la conformité continue des prestations fournies, sans interruption du service.

Article 5. Description du besoin

Le titulaire devra proposer une solution conforme aux spécifications techniques minimales définies ci-après. Ces exigences constituent des conditions de conformité de l'offre.

La solution attendue devra permettre d'accompagner à la fois Numih France et ses adhérents, dans le cadre de l'offre d'accompagnement RGPD proposée par le GIP.

Compte tenu de la diversité des structures adhérentes (nature juridique, taille, maturité RGPD, types de traitements mis en œuvre), la présente description n'a pas vocation à être exhaustive. Les candidats sont invités à présenter les besoins auxquels ils peuvent répondre, en mentionnant expressément ceux auxquels ils ne pourront pas répondre.

5.1 Configuration minimale et prérequis techniques

La solution devra :

- Être accessible via un navigateur web standard, sans installation lourde côté poste utilisateur ;
- Être compatible à minima avec les navigateurs récents (Chrome, Edge, Firefox ou équivalent) ;
- Permettre un accès sécurisé depuis le réseau du GIP ainsi que, le cas échéant, depuis les environnements des structures adhérentes ;
- Ne pas imposer de configuration matérielle spécifique autre qu'un poste bureautique standard connecté à Internet.

Le candidat précisera :

- L'architecture générale de la solution ;
- Les prérequis techniques éventuels côté utilisateurs (GIP et adhérents) ;
- Les modalités d'administration centralisée et de supervision.

5.2 Fonctionnalités obligatoires de la solution

La solution devra permettre la gestion mutualisée et cloisonnée de la conformité RGPD, au bénéfice du GIP et de ses adhérents, selon une logique multi-entités.

1. Gouvernance RGPD multi-entités

La solution devra permettre :

- La gestion distincte de plusieurs entités (GIP et adhérents), avec cloisonnement strict des données des entités,
- La possibilité pour le GIP d'exercer un rôle d'administration, de supervision ou d'accompagnement aux données des adhérents ;
- L'adaptation des droits et périmètres selon le rôle du GIP auprès de chaque adhérent (accompagnement, conseil, pilotage)
- la possibilité pour le DPO de piloter la mise en conformité en communiquant avec les utilisateurs (par exemple : un espace tchat ; l'envoi de notifications par mail ; une fonctionnalité de fil de commentaires pour envoyer une question à une personne par mail avec lien) ;
- la possibilité d'extraire les indicateurs issus des différents plans d'actions par entité (fiches registres, registres des violations de données, registre des droits) ;
- Le paramétrage de rappels et notifications aux référents métiers.

2. Registre et documentation des traitements

La solution devra permettre :

- tenue et mise à jour d'un registre des activités de traitement, conforme à l'article 30 du RGPD, pour chaque entité, les champs registres devant être entièrement paramétrables (possibilité d'ajouter ou moduler les champs) ;
- La documentation des finalités, bases légales, catégories de données, durées de conservation (par catégories de données) et mesures de sécurité par des champs prédéfinis ;
- La mutualisation possible de modèles, référentiels ou trames entre le GIP et les adhérents avec la possibilité de disposer d'une base de fiches registres, et de pouvoir dupliquer une fiche sur plusieurs entités en même temps ;
- La possibilité d'impliquer et donner accès à plusieurs utilisateurs sur une fiche registre ;
- La possibilité de filtrer les traitements par grandes catégories (par exemple : RH ; dossier médical etc.) ;
- La gestion des responsables de traitement avec une distinction du registre responsable de traitement / sous-traitant par un filtre ou un espace dédié ;

- La gestion des sous-traitants et acteurs impliqués par l'import de sous-traitants ;
- La gestion des logiciels par import (Excel) ;
- La possibilité d'extraire le registre des traitements en format CNIL (fichier Excel) ;
- La possibilité d'extraire le plan d'actions saisi dans la fiche registre (sous format Excel) ;
- La possibilité d'ajouter des pièces jointes sur une fiche registre.

3. Analyses d'impact et gestion des risques

La solution devra permettre :

- La réalisation et suivi des analyses d'impact relatives à la protection des données (AIPD) sur la base du modèle CNIL : avec possibilité d'import de l'AIPD sur le logiciel CNIL et d'export à partir du logiciel CNIL.
- La possibilité de reprendre une fiche registre pour débiter une AIPD sans ressaisie ;
- La possibilité de générer un questionnaire envoyé au référent métier concerné pour faciliter le remplissage de l'AIPD (optionnel) ;
- La possibilité de différents rédacteurs sur l'AIPD ;
- La possibilité d'export Word de l'AIPD (selon les droits du profil) ;
- La possibilité de suivre le plan d'action associé : suivi des risques, des mesures de réduction et des décisions associées ;
- historisation et traçabilité des validations.

4. Gestion des violations de données

La solution devra permettre :

- L'enregistrement et suivi des violations de données sous forme de registre pour chaque entité (avec champs paramétrables) ;
- La gestion des délais réglementaires et alertes associées ;
- La possibilité de suivre le plan d'action associé (actions préventives, actions immédiates, actions de remédiation) ;
- L'historisation et traçabilité des actions ;
- La possibilité de générer et d'exporter une synthèse PDF de chaque enregistrement ;
- La possibilité d'extraire le registre des violations sous format Excel.

5. Veille réglementaire et espace documentaire

La solution devra permettre :

- La mise à disposition d'un flux de veille réglementaire (CNIL ; Dalloz ; Légifrance...) ;
- La présence d'un espace documentaire permettant de partager des documents juridiques, ou procédures...

5. Gestion des droits des personnes

La solution devra permettre :

- L'enregistrement et suivi des demandes d'exercice de droits sous forme de registre pour chaque entité (avec champs paramétrables) ;
- La gestion des délais réglementaires et alertes associées ;
- La traçabilité des actions et réponses apportées ;
- La possibilité de générer et d'exporter une synthèse PDF de chaque enregistrement ;
- La possibilité d'extraire le registre des droits sous format Excel.

6. Pilotage, reporting, exports

La solution devra permettre et faciliter le pilotage de la conformité par :

- Des tableaux de bord de suivi de la conformité, différenciés par entité ;
- La génération d'indicateurs consolidés permettant au GIP d'avoir une vision globale de la conformité RGPD par entité ;
- La génération de rapports et d'exports (formats standards).

5.3 Sécurité : traçabilité, sauvegardes, confidentialité et habilitations

La solution devra garantir :

- La totale reprise des données antérieures présentes sur la solution Smart Global via une procédure de migration de données (Registre, violation, exercice des droits, horodatage, documents associés)
- Une phase de test permettant de valider l'exactitude des données importées ;
- La possibilité d'un hébergement HDS (optionnel) ;
- Des sauvegardes en temps réel, avec possibilité de récupérer des données en cas d'erreur ou de suppression involontaire ;
- Droit administrateur pour le GIP donnant un droit de suppression sur toutes les actions effectuées (exemple : supprimer une violation de données créée par erreur) ;
- une gestion fine des habilitations, fondée sur des profils utilisateurs paramétrés différenciés (ci-dessous détaillés) ;
- un cloisonnement strict des données entre le GIP et chaque adhérent ;
- Accès à un module de traçabilité : permettant traçabilité des accès et des actions ;
- la conformité aux principes de protection des données dès la conception et par défaut.

5.4 Disponibilité, maintenance et assistance

La solution devra garantir :

- un taux de disponibilité minimal de 99,5% hors plages de maintenance planifiées ;
- des plages de maintenance communiquées à l'avance, compatibles avec l'activité du GIP et de ses adhérents ;
- une maintenance corrective et évolutive incluant les évolutions réglementaires ;
- un dispositif d'assistance technique et fonctionnelle, adapté à un usage multi-entités, accessible a minima aux heures ouvrées ;
- une adresse mail dédiée support ;
- accès limité du support sous validation du GIP.

Article 6. Gestion des utilisateurs et des profils

La solution devra permettre :

- la création de profils utilisateurs sur mesure (en fonction des tâches affectées) distincts, notamment :
 - administrateurs du GIP ;
 - DPO ou référents RGPD du GIP ;
 - référents RGPD des adhérents ;
 - utilisateurs métiers ou contributeurs ;
 - utilisateurs en consultation ;
- un nombre d'utilisateurs évolutif, compatible avec l'adhésion progressive de nouvelles structures ;
- l'ajout, la modification et la suppression d'utilisateurs et d'entités tout au long de l'exécution du marché, sans remise en cause de l'architecture globale.

Article 7. Conditions d'exécution des prestations

7.1 Hébergement du service dans le data center de Numih France

L'hébergement de la solution dans les data center de Numih France est à privilégier.

Dans ce cas le déploiement devra suivre les procédures de déploiement de Numih France et suivre les prérequis ci-après

7.1.1 Intervention à distance

Un Plan d'Assurance Sécurité (PAS) est exigé. Il devra être fourni au plus tard au démarrage de la prestation.

Ces interventions se feront au travers du bastion authentifiant de Numih France.

Le PAS peut être un sous-ensemble du plan d'assurance qualité (PAQ).

À la signature du contrat, Numih France doit pouvoir indiquer s'il accepte le PAS type du Titulaire ou si un cycle de validation du PAS est nécessaire.

Le PAS doit traiter au minimum les thèmes suivants :

- Identification de l'interlocuteur en charge de la sécurité des interventions chez le Titulaire
- Critères de sécurité utilisés dans la désignation des personnes chargées de l'intervention à distance, engagement de sécurité, information de ces personnes sur la sécurité de la prestation et sensibilisation ;
- Règles de protection des informations relatives au SIS ou à l'intervention et détenues par le Titulaire (copie, diffusion, conservation, destruction, transmission) ;
- Désignation des sites d'exécution de la prestation, protection et accès physiques des locaux utilisés, séparation vis-à-vis d'autres prestations ;
- Architecture générale de la plateforme utilisée pour l'intervention à distance, cloisonnement technique vis-à-vis d'autres prestations, fonctions de sécurité activées dans la plateforme ;
- Accès logique des intervenants à la plateforme, identification et authentification, mise en veille et déconnexion automatiques, séparation des tâches, gestion des droits, traçabilité des actions ;
- Dispositions prises pour continuer à assurer les activités de la prestation à la suite d'un sinistre majeur ;
- Assurance et contrôle de la sécurité des services d'intervention fournis.

7.1.2 Supervision du service

Le Titulaire met à disposition toutes les informations nécessaires permettant d'assurer la supervision fonctionnelle et techniques des services.

La supervision comprend à minima les périmètres suivants :

- Supervision des briques applicatives
- Supervision des web services et API
- Supervision des environnements techniques hébergés par Numih France

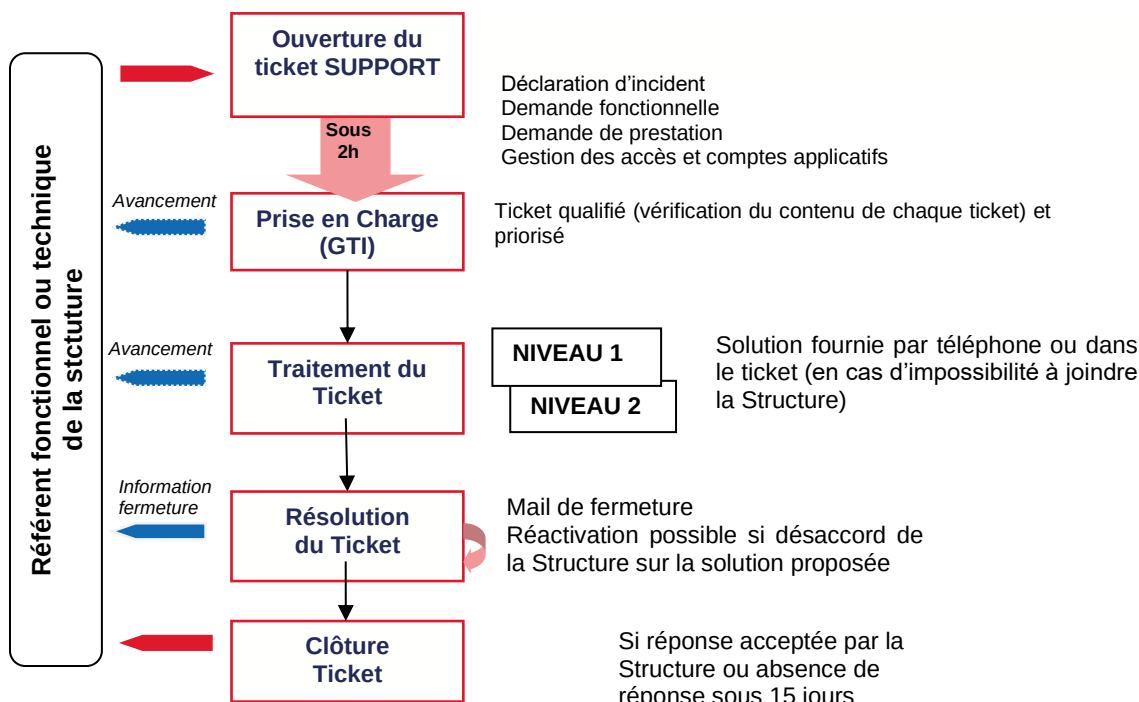
Le système de supervision doit notamment permettre de gérer par exemple la disponibilité de l'url, l'espace disque, la présence d'un fichier témoin, la disponibilité d'une base ou d'un annuaire... Aucune information nominative n'est accessible par ce service.

Numih France utilise la solution de supervision Centreon. La supervision devra être compatible avec cet outil.

Le dossier d'exploitation devra notamment contenir l'identification des services critiques dont la surveillance sera assurée au cours de l'astreinte, ainsi que les prérequis des sondes à mettre en œuvre et les procédures de niveau 1.

Le cas échéant, le système de supervision doit permettre la création de tableaux de bord à destination des adhérents finaux.

7.2 Support



7.3 Niveau d'engagement en cas d'incident

Les actions correctives sont engagées selon les délais d'intervention suivants, en fonction de la sévérité de l'incident ou de la demande.

Classification		Délai de prise en compte	Garantie de Temps de Rétablissement (GTR)
Sévérité de l'incident ou de la demande	Critique (Sévérité 1)	15 minutes	04h00 - 7j/7 24H24
	Haute / urgente (Sévérité 2)	30 minutes	24h00 (J+1)
	Normal (Sévérité 3)	01h00	48h00 (J+2)
Demande de service		04h00	48h00 (J+2)

- Durée maximale d'arrêt acceptable (DMIA) : 4h
- Taux de disponibilité minimum : en 99%

Le Titulaire s'engage à garantir une disponibilité mensuelle de la plateforme de signature électronique de 99 %, hors périodes de maintenance planifiées et communiquées à l'Acheteur au moins 5 jours ouvrés à l'avance.

7.3.1 Définition de l'indisponibilité

Est considérée comme une indisponibilité toute période durant laquelle la plateforme est inaccessible ou ne permet pas l'exécution normale et sécurisée des opérations, objet du marché, pour une part significative des utilisateurs.

Garanties de continuité de service

- GTI-Garantie de Temps d'Intervention : le Titulaire s'engage à intervenir dans un délai maximal de 1 heure ouvrée après détection ou notification de l'incident

- GTR-Garantie de Temps de Rétablissement : la remise en service complète de la plateforme doit être assurée dans un délai maximal de 2 heures ouvrées après détection de l'incident.
- PRM-Point de reprise maximal : en cas de perte de données, le Titulaire garantit que les données créées ou modifiées dans les 15 minutes précédant l'incident pourront être restaurées.

7.3.2 Survenance d'incident majeur

Notification d'incident majeur

Tout incident majeur (indisponibilité, faille de sécurité, perte de données) devra être signalé à l'Acheteur dans un délai maximal de 1 heure suivant sa détection. Le Titulaire fournira une première évaluation des impacts, des causes probables et des mesures immédiates prises.

Rapport d'incident

- Un rapport d'incident détaillé sera transmis à l'Acheteur dans un délai de 5 jours ouvrés après la résolution complète de l'incident. Ce rapport devra inclure, a minima :
 - La nature de l'incident, sa durée et son périmètre ;
 - L'analyse des causes (post-mortem) ;
 - Les impacts constatés ; Les mesures correctives mises en œuvre ;
 - Les actions préventives prévues pour éviter la récurrence.

L'acheteur pourra solliciter une réunion de retour d'expérience avec les représentants du Titulaire.

7.4 Réversibilité

Le Titulaire s'engage à réaliser l'ensemble des actions de préparation et d'exécution de la réversibilité (y compris la fourniture des éléments nécessaires à la reprise du service par le tiers désigné), dans un délai maximal de 2 mois à compter de la réception de la demande de d'exécution de la réversibilité.

Une fois la réversibilité exécutée et le nouveau système mis en production par le tiers assurant la reprise du service, le Titulaire fournit une assistance aux équipes du tiers pendant une période de 2 mois. Cette assistance comprendra également le transfert, de savoir-faire nécessaire à la continuité de service ainsi que toutes les données contenues dans l'outil. Durant cette période, la gestion du fonctionnement des systèmes est sous la responsabilité de ce tiers.

Les principaux livrables attendus sont :

- Les outils ou procédures permettant l'extraction des données ou les données extraites des briques numériques concernées par le présent marché
- La documentation de livraison ainsi que les contraintes d'utilisation et de rechargement des données

Les données sont exportées et fournies au format CSV ou JSON.

Les données de reprises doivent échangées par les parties avec des outils permettant de garantir :

- Le chiffrement des échanges (à minima les flux)
- La traçabilité des échanges

A l'issue de la période d'assistance, le Titulaire s'engage à supprimer les données propriété de Numih France ou de ses clients. Toute donnée conservée devra être anonymisée.

Un PV de fin de réversibilité intégrant un engagement de destruction et/ou d'anonymisation devra être fourni.

Article 8. Sécurité

Pour Rappel : la charte sécurité du système d'information de Numih France, énonce les exigences relatives à la sécurité de ses systèmes d'information. Elle est applicable et à signer dans les contextes ci-dessous :

- Pour les prestataires externes, ayant accès dans le cadre de leur mission à tout ou partie des Systèmes d'Information de Numih France.
- Pour les Titulaires de marché associés aux technologies de l'information et de la communication (ordinateurs, logiciels, développements ou hébergement d'application via le web) ainsi qu'aux fournitures et services annexes

Lorsque le candidat a obtenu une certification de sécurité (HDS, 27001, RGS, ...) sur le périmètre de la prestation visée par le présent marché, un certificat en cours de validité est à fournir.

Dans le cadre de la réalisation de la prestation, le Titulaire s'engage à mettre en application les exigences de sécurité de l'annexe Outil RGPD_Exigences sécurité.xlsx.

Les tableaux de cette annexe doivent être complétés par la description de la mise en œuvre et des éventuels écarts. Il revient à Numih France d'apprécier ces réponses, d'exiger si nécessaires des compléments et in fine d'accepter les risques résiduels liés aux éventuels écarts (voir page de garde de l'annexe).

Certaines exigences peuvent être sous responsabilité partagée.

5. Incident de sécurité

Toute partie qui a connaissance d'un incident de sécurité impactant ou pouvant impacter le Services et ses données doit en informer l'ensemble des parties prenantes.

Pour tout incident impactant les Données à Caractère Personnel, les Délégués à la Protection des Données (DPD) des parties doivent en être informés.

Les contacts Numih France sont rssi@numihfrance.fr et dpo@numihfrance.fr.

6. Correction des vulnérabilités techniques

L'échelle ci-après suit le Common Vulnerability Scoring System ([CVSS](#)) pour la classification des vulnérabilités techniques d'un système d'information.

Les délais de correction sont adaptés pour un service en production.

Elle doit servir de base de référence pour définir les priorités de correction. Les délais de correction indiqués sont standards et peuvent ajuster en fonction du contexte (exposition du système concerné, facilité d'exploitation, existence de moyen de contournement, etc.)

Criticité	Définition	Délai de correction
Négligeable	Non considéré comme une vulnérabilité ou dont le score est inférieur à 1,9 Point que l'auditeur a souhaité relever, ou risque négligeable	À intégrer dans la prochaine évolution du périmètre concerné (soumis à validation de l'éditeur)
Faible	Concerne tous les scores compris entre 2 et 3.9 Tous les risques de sécurité représentant une menace faible pour le système audité	À intégrer dans la prochaine évolution du périmètre concerné
Moyen	Concerne tous les scores compris entre 4 et 6.9 Tous les risques de sécurité représentant une menace pouvant conduire à la récolte d'informations sensibles.	Selon analyse effectuée, dans les 3 mois en moyenne
Élevée	Concerne tous les scores compris entre 7 et 8.9 Tous les risques de sécurité représentant une menace significative pour la sécurité. L'attaquant ne possède pas les accès complets sur le système audité. Des informations très sensibles sont compromises.	10 à 30 jours

Criticité	Définition	Délai de correction
Critique	Concerne tous les scores supérieurs à 9 Risque critique pour le système d'information et nécessitant une correction immédiate ou imposant en arrêt immédiat du service.	5 à 10 jours