Marchés de l'Etat et de ses Etablissements Publics

Ministère de l'Enseignement supérieur, de la Recherche et de l'Espace

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE
DÉLÉGATION PARIS-CENTRE
16 rue Pierre et Marie Curie – 75005 Paris
Tél. : 01.42.34.94.00 – Fax : 01.43.26.87.23

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (C.C.T.P.)

Objet du marché :

Accord-cadre relatif à l'évolution et à la maintenance du système d'information de l'IR* Progédo — Maintien en Condition Opérationnelle (MCO) et Tierce Maintenance Applicative (TMA)

(Annexe technique au Cahier des Clauses Particulières — accord-cadre PROGEDO UAR2506)

Le présent document décrit les caractéristiques techniques du besoin. Il complète le Cahier des Clauses Particulières (CCP) et prévaut sur celui-ci pour toute disposition de nature exclusivement technique.

Nomenclatures :

Code CPV : 72600000-6 (Services de support et de maintenance logicielle) .

72267000-4 (Services de maintenance de logiciels) .

72315000-6 (Gestion de réseaux de données)

Sommaire

1. CONTEXTE ET OBJECTIFS 3

1.1 Présentation de Progédo 3

1.2 Origine du besoin et finalité du projet 3

1.3 Périmètre exclu du marché 4

2. LE MAINTIEN EN CONDITION OPERATIONNELLE (MCO) 4

2.1 Périmètre existant 4

2.2 Fonctionnement souhaité 4

2.3 Exigences contractuelles 5

2.4 Exigences opérationnelles 6

3. LA TIERCE MAINTENANCE APPLICATIVE (TMA) 9

3.1 Modes de fonctionnement 10

3.2 Gouvernance de la TMA 10

3.3 Exigences techniques et qualité 11

3.4 Transfert de connaissances 12

3.5 Utilisation de l'intelligence artificielle générative 12

4. ANNEXES 13

4.1 Catalogue des services existants 13

4.2 Évolutions du système d'information envisagées pour 2027 14

1. Contexte et objectifs

1.1 Présentation de Progédo

Progédo est l'infrastructure nationale pour les données et méthodes en sciences sociales quantitatives. Missionné par le CNRS et le Ministère de l'Enseignement supérieur et de la Recherche, Progédo adhère aux principes d'ouverture, de qualité et de comparaison internationale des données.

L'action de Progédo et de son équipe s'articule autour de trois missions :

a) La diffusion de données de recherche et issues de la statistique publique

Avec son entrepôt Quetelet-Progedo, Progédo favorise la réutilisation, la réplication et la transparence des données en sciences sociales quantitatives.

Progédo œuvre concrètement à la préservation, à la documentation et à la mise à disposition des données pertinentes pour les sciences sociales quantitatives, en lien avec les producteurs de données (Insee, services statistiques ministériels ou chercheurs). L'équipe assure également une veille pour garantir le respect des standards internationaux.

b) La coordination de grandes infrastructures européennes et des communautés liées aux approches quantitatives des données

Autour du CESSDA (Consortium of European Social Science Data Archives) et des grandes enquêtes (ESS, SHARE, GGP), Progédo joue un rôle structurant dans la participation française aux grandes infrastructures européennes. Cette action est complétée par la promotion de la participation aux grands projets comparatifs internationaux dans le domaine des sciences sociales quantitatives, comme les enquêtes ISSP, EVS et CSES. Progédo est à la fois le nœud national et un acteur du développement de ces projets en France.

Progédo participe plus largement à l'animation des communautés liées aux approches quantitatives des données, en renforçant les passerelles entre monde académique, décideurs publics et société. Progédo développe son action auprès des communautés locales en s'appuyant sur le réseau national des dix-sept plateformes universitaires de données.

c) L'innovation et l'amélioration des standards et des méthodes en sciences sociales quantitatives

Avec le ProgéLab, Progédo œuvre à l'amélioration des standards et des méthodes en sciences sociales quantitatives. Le ProgéLab vise, d'une part, à porter des projets de recherche dans le domaine des sciences sociales — à l'image du projet ObHisPop — et, d'autre part, à intégrer de nouvelles méthodes. Il contribue plus largement à l'innovation méthodologique et à l'amélioration continue de la qualité des données.

1.2 Origine du besoin et finalité du projet

Hébergé par Huma-Num, le système d'information de Progédo est principalement constitué du catalogue (data.progedo.fr), qui assure la diffusion de données issues de la recherche et de la statistique publique.

L'objectif du présent marché est le Maintien en Condition Opérationnelle (MCO) et la poursuite de la Tierce Maintenance Applicative (TMA) de l'IR* Progédo.

Le schéma ci-dessous présente le fonctionnement général du catalogue :

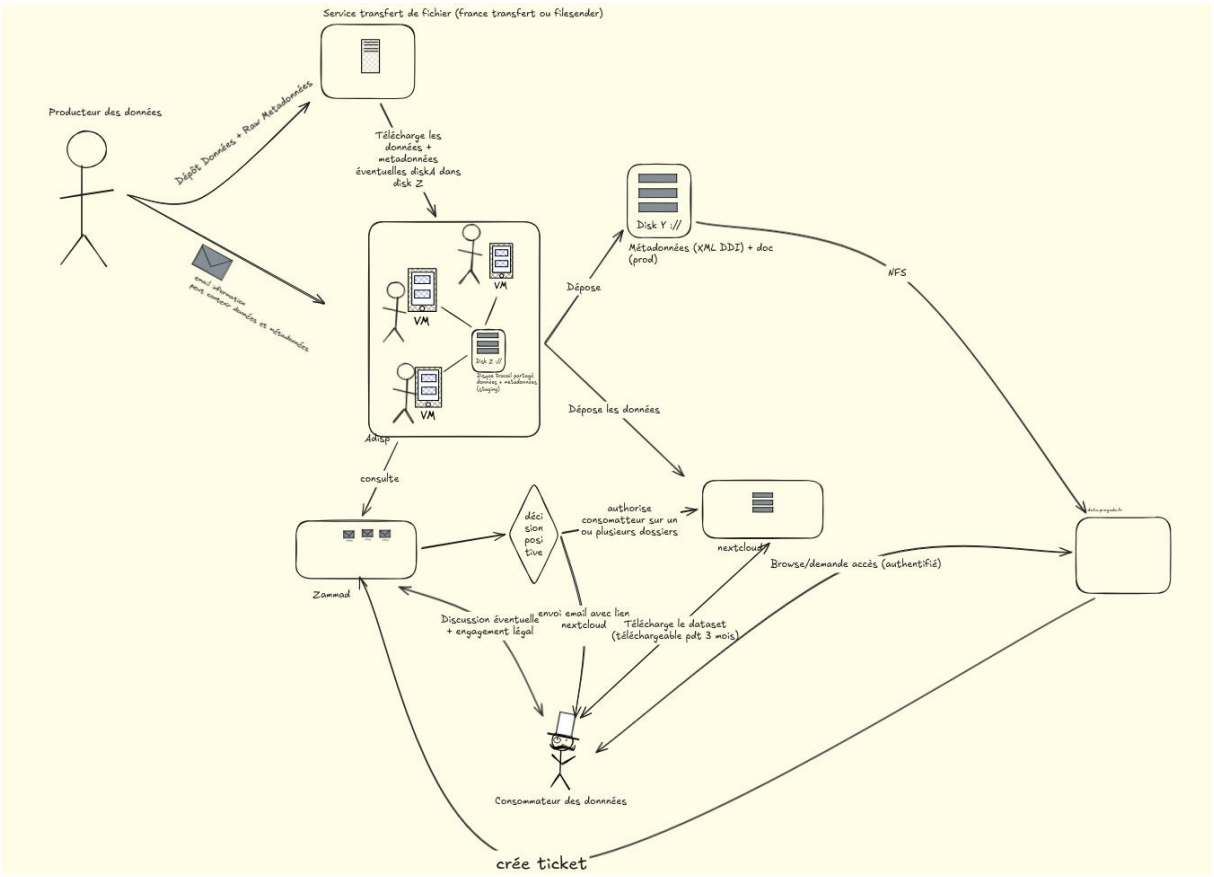


Schéma fonctionnel du catalogue — flux de dépôt, de validation et de mise à disposition des données.

1.3 Périmètre exclu du marché

Sont exclus du périmètre du présent marché :

- l'hébergement de la plateforme.
- le pôle ProgéLab.

2. Le Maintien en Condition Opérationnelle (MCO)

le MCO vise à garantir le maintien en état opérationnel des services informatiques nécessaires au bon fonctionnement de l'IR* Progédo. Elle inclut la supervision, la sécurisation, et la conformité de ces services aux exigences réglementaires et techniques du CNRS et de l'ANSSI.

2.1 Périmètre existant

L'ensemble des services actuellement maintenus est listé au catalogue des services fourni en annexe (cf. 4.1 — Catalogue des services existants).

2.2 Fonctionnement souhaité

Le marché fonctionne par émission de bons de commande glissants couvrant la durée totale du marché. Un nouveau bon de commande est émis lors de l'épuisement du budget alloué, sans interruption du MCO.

Le prestataire devra proposer une approche modulaire permettant l'ajout de nouveaux services ou périmètres à le MCO via l'émission de bons de commande dédiés par service.

Le prestataire devra intégrer le catalogue initial des services décrit en annexe (cf. 4.1 — Catalogue des services existants).

2.3 Exigences contractuelles

2.3.1 Contrat de service (SLA) et conformité PSSI-CNRS

Un SLA (Service Level Agreement, ou « accord de niveau de service ») est un engagement contractuel par lequel le prestataire s'oblige à fournir un service selon des niveaux de qualité mesurables, appelés indicateurs de niveau de service. Il précise, pour chacun de ces indicateurs, le seuil à respecter et les modalités de mesure et de suivi. Il permet ainsi à Progédo d'objectiver la qualité du MCO et de la piloter sur des critères vérifiables.

Un SLA sera formalisé entre le prestataire et le Progédo dès le début du marché. Il portera sur l'ensemble des services du catalogue (cf. 4.1) et sera révisé à chaque intégration d'un nouveau service ou périmètre au MCO. Compte tenu de la nature des services de Progédo, dont une interruption temporaire n'a pas de conséquence grave, le SLA distingue deux axes indépendants : la disponibilité des services et la sécurité des données.

Disponibilité des services

Ces engagements s'appliquent pendant les heures ouvrées (jours ouvrés, de 9 h à 18 h), sauf exception convenue au bon de commande. Ils comportent :

- des délais de prise en compte et de résolution par niveau de criticité :
    - incident critique (service inaccessible pour l'ensemble des utilisateurs) : prise en compte sous 4 h, résolution ou contournement sous 1 jour ouvré .
    - incident majeur (service dégradé ou fonction importante indisponible) : prise en compte sous 1 jour ouvré, résolution sous 3 jours ouvrés .
    - incident mineur (gêne sans impact sur l'usage) : traitement planifié avec le CNRS .
- une disponibilité mensuelle minimale de 98 %, mesurée sur les heures ouvrées et hors maintenances planifiées, celles-ci étant annoncées au moins 5 jours ouvrés à l'avance .
- un taux de résolution des incidents ≥ 90 % dans les délais contractuels.

Sécurité des données

La gravité d'un incident de sécurité ne dépend pas de la criticité du service concerné, mais de la sensibilité des données exposées. Une suspicion de compromission, de fuite ou d'exfiltration de données est traitée avec la priorité la plus élevée, y compris en dehors des heures ouvrées. Le prestataire s'engage à :

- alerter le CNRS sans délai et au plus tard sous 24 h après la prise de connaissance de l'incident, afin de lui permettre de remplir ses propres obligations, notamment la notification à la CNIL sous 72 h en cas de violation de données personnelles (art. 33 du RGPD) .
- prendre sans délai les mesures de confinement nécessaires (isolement, révocation des accès), en concertation avec le CNRS .
- remettre un rapport préliminaire sous 72 h, puis un rapport final avec post-mortem sous 30 jours.

Le suivi de ces indicateurs est assuré dans le tableau de bord du MCO (cf. 2.4.4) et examiné lors des comités de pilotage (COPIL et COSEC le cas échéant).

Conformité à la PSSI-CNRS

La PSSI-CNRS (Politique de Sécurité des Systèmes d'Information du CNRS) fixe le cadre de sécurité applicable aux systèmes d'information de l'organisme. Le prestataire s'engage à s'y conformer de manière stricte, ce qui implique :

- l'application des règles de sécurité, de confidentialité et de protection des données .
- l'alignement sur les recommandations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et sur le RGPD (Règlement général sur la protection des données).

2.3.2 Matrice RACI

Une matrice RACI (matrice de responsabilité) sera établie et validée en début de marché pour clarifier les rôles et responsabilités de chaque partie prenante. Cette matrice couvrira l'ensemble des processus clés, incluant la gestion des incidents et des problèmes, la gestion des évolutions, ainsi que les audits et contrôles de réversibilité.

2.3.3 Clause de réversibilité / sortie

La réversibilité désigne l'ensemble des opérations permettant à Progédo, à la fin du marché ou en cas de résiliation, de reprendre lui-même le MCO et la TMA ou de les confier à un autre prestataire, sans interruption des services, sans perte de données et sans perte de connaissances.

Toute sortie du marché, quelle qu'en soit la cause, est précédée d'un préavis de trois mois minimum, porté à six mois pour les services critiques. Pendant cette période, le prestataire remet un plan de réversibilité que Progédo valide, précisant le calendrier, les livrables et les interlocuteurs de chaque étape. Ce plan de réversibilité sera sanctionné par l'émission d'un dernier bon de commande qui couvrira la période.

Le prestataire remet une documentation technique et fonctionnelle complète et à jour, comprenant notamment l'architecture, les procédures d'exploitation, l'historique des incidents et le backlog en cours. Il l'accompagne de sessions de formation, ou de pairing, auprès des équipes internes de Progédo ou du prestataire entrant.

Il transmet également à Progédo les configurations, scripts, définitions d'infrastructure et pipelines nécessaires à la continuité du service, ainsi que les données, dans des formats ouverts et réutilisables. À l'issue du transfert, il révoque ses accès, restitue ou renouvelle les secrets qu'il détient et atteste de la suppression des données de Progédo qu'il conserve.

Pendant toute la période de transfert, le prestataire maintient les services en état de fonctionnement opérationnel, dans le respect du SLA (cf. 2.3.1).

2.3.4 Droit d'audit

Le droit d'audit est le droit reconnu à Progédo de vérifier, par lui-même ou par un tiers qu'il mandate, que le prestataire respecte ses engagements contractuels : niveaux de service, sécurité, conformité à la PSSI-CNRS et au RGPD, qualité de la documentation et préparation de la réversibilité.

Progédo peut réaliser un audit une fois par an, ainsi qu'après tout incident de sécurité majeur. L'audit peut être conduit par Progédo, par le RSSI du CNRS, par l'ANSSI ou par un tiers mandaté, à condition que celui-ci soit tenu à la confidentialité et ne soit pas un concurrent du prestataire.

Il porte sur le périmètre confié au prestataire. Il peut couvrir les procédures d'exploitation, les configurations et le code, les journaux, les sauvegardes, la gestion des accès et des secrets, les revues de droits, les indicateurs du SLA et la documentation. Il peut aussi inclure un test de restitution de la documentation et des configurations, afin de contrôler la réversibilité.

Progédo notifie l'audit au prestataire avec un préavis de quinze jours ouvrés, ramené à quarante-huit heures en cas d'incident de sécurité. Le prestataire donne accès aux documents, aux systèmes concernés et aux personnes compétentes, et répond aux demandes dans un délai raisonnable.

À l'issue de l'audit, Progédo remet au prestataire un rapport. Celui-ci propose, dans un délai de quinze jours ouvrés, un plan d'action correctif daté, dont le suivi est assuré en COSEC. Les constats sont traités comme confidentiels.

2.4 Exigences opérationnelles

2.4.1 Supervision et monitoring

La supervision consiste à observer en continu l'état des services (disponibilité, performances, ressources, journaux) afin de détecter les anomalies avant qu'elles n'affectent les utilisateurs, et de déclencher le traitement approprié. Elle s'accompagne de la gestion des incidents et des problèmes, ainsi que des sauvegardes et des plans de reprise, qui garantissent la continuité de l'activité de Progédo.

Le prestataire exploite et fait évoluer les outils de supervision existants : Icinga2 pour la disponibilité des services, Telegraf, InfluxDB et Grafana pour les métriques système et applicatives, Alloy et Loki pour les journaux (cf. 4.1). Il définit avec Progédo les seuils d'alerte, les règles de notification et les tableaux de bord, et les met à jour à chaque intégration d'un nouveau service. Les alertes sont qualifiées, dédoublonnées et rattachées au service concerné. Les alertes de sécurité (cf. 2.4.2) sont traitées y compris en dehors des heures ouvrées, conformément à l'axe 2 du SLA (cf. 2.3.1).

Les indicateurs du SLA sont calculés à partir de ces mesures et publiés dans le tableau de bord.

Gestion des incidents

Un incident est une interruption ou une dégradation d'un service. Tout incident est enregistré dans l'outil de ticketing de Progédo ou du prestataire, avec sa criticité, son historique et les actions menées, ce qui garantit la traçabilité et l'accès de Progédo à l'ensemble des échanges. Ces tickets seront archivés dans le tableau de bord SSI de Progédo.

Le prestataire qualifie l'incident, le traite dans les délais du SLA et informe Progédo de son avancement. Lorsque le délai risque d'être dépassé, ou que l'incident nécessite une décision ou une compétence extérieure, il escalade selon les rôles définis dans la matrice RACI (cf. 2.3.2). Toute suspicion d'incident de sécurité suit la procédure d'alerte et de confinement de l'axe 2.

Un post-mortem est réalisé après chaque incident critique, incident de sécurité ou incident récurrent. Il décrit la chronologie, la cause racine, l'impact et les actions correctives et préventives, qui sont ensuite suivies en tant que problèmes jusqu'à leur clôture. Il est remis à Progédo sous dix jours ouvrés, ou sous trente jours dans le cas d'un incident de sécurité (cf. 2.3.1), et présenté en COPIL ou en COSEC.

Sauvegardes, reprise et continuité d'activité

Le prestataire assure la sauvegarde des configurations, des bases de données (catalogue, Zammad) et des données des applications, en s'appuyant sur les dispositifs existants (BackupPC, sauvegardes TSM chez Huma-Num, NAS). Il propose, si nécessaire, l'évolution de ces dispositifs. Les sauvegardes sont chiffrées, stockées hors du serveur d'origine et conservées selon une durée définie avec Progédo.

Le prestataire élabore et tient à jour un plan de reprise d'activité (PRA), précisant pour chaque service la perte de données maximale admissible et le délai de rétablissement visé, ainsi que les procédures de restauration et les responsabilités. Ces objectifs sont cohérents avec le SLA et proportionnés à la criticité de chaque service. Le prestataire vérifie l'intégrité des sauvegardes et réalise au moins une fois par an un test de restauration, dont les résultats sont communiqués à Progédo. Le PRA est intégré à la documentation remise en fin de marché (cf. 2.3.3).

2.4.2 Volet sécurité

Le volet sécurité regroupe les mesures préventives qui réduisent la probabilité et l'impact d'un incident de sécurité : correction des vulnérabilités, maîtrise des accès, traçabilité des événements et protection des données. Le traitement d'un incident avéré relève de l'axe 2 du SLA (cf. 2.3.1) et de la gestion des incidents (cf. 2.4.1).

Gestion des correctifs et veille des vulnérabilités

Le prestataire assure une veille continue des vulnérabilités (CVE, bulletins de l'ANSSI et du CERT-FR, avis des éditeurs) sur l'ensemble des composants du catalogue (cf. 4.1). Il tient à jour un inventaire des versions en service. Une attention particulière est portée aux composants installés depuis les sources (SATOSA, SwitchWAYF), dont les mises à jour ne sont pas automatiques.

Chaque vulnérabilité applicable est évaluée selon sa gravité (score CVSS), son exploitabilité et l'exposition du composant, puis corrigée dans les délais suivants, qui complètent le SLA :

- vulnérabilité critique, ou activement exploitée : sous 72 heures .
- vulnérabilité élevée : sous 7 jours .
- vulnérabilité moyenne : sous 30 jours .
- vulnérabilité faible : à la prochaine maintenance planifiée.

Lorsqu'un correctif n'est pas disponible ou présente un risque de régression, le prestataire met en place une mesure de contournement et en informe Progédo. Tout correctif est d'abord validé en préproduction, sauf urgence justifiée.

Gestion des identités et des accès

Les accès sont nominatifs et attribués selon le principe du moindre privilège, pour le prestataire comme pour les utilisateurs de Progédo. Tout accès d'administration passe par une authentification multi-facteurs (MFA). Les comptes partagés sont proscrits, sauf compte de service documenté.

Les secrets (mots de passe, clés, jetons) sont stockés dans un coffre dédié et jamais dans le code ni dans les dépôts. Ils sont renouvelés selon une périodicité définie avec Progédo, et immédiatement en cas de départ d'un intervenant ou de suspicion de compromission.

Une revue des droits est présentée en COSEC deux fois par an. Elle recense les comptes, les privilèges et les accès du prestataire, et donne lieu à la suppression des droits devenus inutiles.

Journalisation et détection

Les journaux centralisés (cf. 2.4.1) sont exploités à des fins de sécurité : ils couvrent au minimum les authentifications, les actions d'administration, les accès aux données et les événements système. Ils sont protégés contre toute modification et conservés pendant une durée définie avec Progédo, dans le respect du RGPD. Le prestataire définit et fait évoluer des règles de détection des comportements anormaux (tentatives d'accès répétées, connexions inhabituelles, volumes de téléchargement atypiques, modifications de configuration non prévues). Toute alerte confirmée déclenche la procédure d'escalade et de confinement de l'axe 2 (cf. 2.3.1).

Protection des données

Au titre du RGPD et des recommandations de l'ANSSI (cf. 2.3.1), le prestataire n'accède aux données que dans la mesure nécessaire à sa mission. Les données sont chiffrées en transit et, lorsque c'est pertinent, au repos. Le prestataire signale à Progédo tout traitement de données personnelles qu'il identifie, l'assiste dans la tenue du registre des traitements et lui fournit les éléments nécessaires à une éventuelle analyse d'impact.

Le respect de ces exigences est contrôlable dans le cadre du droit d'audit (cf. 2.3.4), et les indicateurs associés (délais de correction, revue des droits) sont publiés dans le tableau de bord de suivi (cf. 2.4.4).

2.4.3 Volet technique

Le volet technique décrit les pratiques d'ingénierie vers lesquelles tend Progédo : automatisation, reproductibilité, sécurité par conception. Le système actuel est constitué de serveurs dédiés installés et configurés pour l'essentiel de manière manuelle ou semi-manuelle (cf. 4.1), et n'y répond pas encore pleinement. Le prestataire est donc tenu de contribuer à cette trajectoire de façon progressive et priorisée, sans que le MCO en soit fragilisée ni le SLA remis en cause (cf. 2.3.1).

Pratiques visées :

- Infrastructure as Code. L'objectif est que la configuration des serveurs, des services et des règles de pare-feu soit décrite dans des dépôts versionnés, relue et déployée de façon automatisée, plutôt que modifiée directement sur les machines. Le prestataire commence par les composants les plus sensibles ou les plus fréquemment modifiés (authentification, pare-feu, supervision), et traite toute nouvelle installation selon ce principe. Le prestataire pourra recommander des solutions alternatives à l'hébergement actuel pour réaliser cet objectif.
- Immutabilité et reproductibilité des environnements. L'objectif est de pouvoir reconstruire un service à l'identique, à partir du dépôt, en préproduction comme en production, et de remplacer un composant plutôt que de le modifier en place. Cette pratique soutient directement le plan de reprise (cf. 2.4.1) et la réversibilité (cf. 2.3.3). À court terme, le prestataire documente les écarts de configuration entre environnements et les réduit progressivement.
- Approche Zero Trust. L'objectif est qu'aucun flux, aucun utilisateur ni aucun composant ne soit considéré comme fiable par défaut : chaque accès est authentifié, autorisé au plus juste et journalisé, y compris entre services internes. Cette approche est complémentaire et ne se substitue pas aux défenses périmétriques actuellement mises en œuvre.
- Pipeline CI/CD avec scans de sécurité automatisés. L'objectif est que toute modification, de code comme d'infrastructure, passe par un pipeline qui exécute des tests et des scans automatisés (dépendances, analyse statique, secrets, images) avant déploiement, et bloque les livraisons présentant une vulnérabilité critique. Les exigences détaillées de la chaîne de livraison applicative figurent en 3.3.

2.4.4 Gouvernance

La gouvernance désigne les instances, les documents et les outils par lesquels Progédo pilote le marché, contrôle le respect des engagements du prestataire et arbitre les décisions. Elle s'appuie sur trois éléments : deux comités (COPIL et COSEC), et un tableau de bord partagé.

Instances

Le comité de pilotage (COPIL) se réunit chaque trimestre. Il donne à Progédo une vision d'ensemble du MCO, de la TMA et des projets en cours (cf. 3.2). Il examine les indicateurs du tableau de bord, les incidents et post-mortems, la consommation des bons de commande, l'avancement de la feuille de route technique (cf. 2.4.3) et les évolutions du périmètre. Progedo, en consultation avec le prestataire, arbitre les priorités et valide les plans d'action correctifs en cas de non-respect du SLA (cf. 2.3.1).

Le comité de suivi sécurité (COSEC) se réunit deux fois par an, et de façon exceptionnelle après un incident de sécurité majeur ou un audit (cf. 2.3.4). Il est consacré aux sujets de sécurité : revue des droits d'accès, état des vulnérabilités et des correctifs, incidents de sécurité, suites des audits et conformité à la PSSI-CNRS. Le RSSI du CNRS y est associé.

Le comité opérationnel de la TMA (cf. 3.2) reste distinct de ces deux instances. Il traite le backlog, tandis que le COPIL et le COSEC traitent le pilotage et la sécurité.

Pour chaque comité, le prestataire transmet un support et les indicateurs associés cinq jours ouvrés avant la séance, puis un compte rendu comportant le relevé des décisions et des actions, avec leur responsable et leur échéance, dans les cinq jours ouvrés suivant la séance. Les rôles de chaque partie sont ceux de la matrice RACI (cf. 2.3.2).

Documentation vivante

Le prestataire constitue et maintient la documentation du système : architecture, inventaire des composants et des versions, procédures d'exploitation, plan de reprise (cf. 2.4.1), matrice RACI, feuille de route et décisions structurantes. Cette documentation est dite vivante, car elle évolue avec le système au lieu d'être produite en fin de mission. Toute modification du système (déploiement, changement de configuration, intégration d'un nouveau service) entraîne sa mise à jour, qui fait partie de la définition de « terminé » du changement.

Elle est stockée dans des dépôts versionnés, dans des formats ouverts et structurés, et accessible à Progédo en permanence, conformément au principe de documentation as code (cf. 3.3).

Tableau de bord de suivi

Le prestataire alimente le tableau de bord partagé de Progédo ou tout outil équivalent proposé par le prestataire et validé par Progédo. Il est accessible à Progédo en lecture, à tout moment, et ses données sont exportables dans un format ouvert. Il agrège, à partir des outils de supervision et de ticketing (cf. 2.4.1) :

- les indicateurs du SLA, pour la disponibilité comme pour la sécurité (cf. 2.3.1) .
- les délais de correction des vulnérabilités et la revue des droits (cf. 2.4.2) .
- le suivi des incidents, des problèmes et des post-mortems .
- l'avancement de la trajectoire technique (cf. 2.4.3) et de la TMA .
- la consommation des bons de commande en cours (cf. 2.2).

Les indicateurs sont mis à jour au moins une fois par mois. Les écarts par rapport aux seuils contractuels y sont signalés et présentés au COPIL.

3. La Tierce Maintenance Applicative (TMA)

La TMA doit intégrer la maintenance corrective (bug ou anomalie), la maintenance évolutive (ajout de fonctionnalité), la maintenance adaptative et la maintenance préventive (diminution de la dette technique). Elle se distingue du MCO (cf. 2), qui maintient les services en état de fonctionnement : un incident de production est traité au titre du MCO, et la correction durable du code qui en est la cause relève de la TMA. La TMA fonctionne selon deux modes, adaptés à la taille et à la complexité des travaux.

3.1 Modes de fonctionnement

Mode au fil de l'eau

Le mode au fil de l'eau s'applique aux travaux de faible ampleur : anomalies, évolutions bien circonscrites, adaptations mineures, actions de réduction de la dette technique. Chaque demande est enregistrée sous forme de ticket, décrite, chiffrée par le prestataire, puis priorisée par Progédo dans un backlog partagé (cf. 3.2). Le prestataire traite les tickets dans l'ordre de priorité fixé, sans engagement de résultat global au-delà de la conformité de chaque ticket à sa description.

Les travaux sont imputés sur les bons de commande glissants du marché (cf. 2.2) selon le temps passé, dans la limite de l'estimation validée par Progédo. Tout dépassement prévisible est signalé avant d'être engagé.

Mode projet

Lorsque la complexité d'une demande le justifie, elle passe en mode projet. Le prestataire constitue alors une équipe dédiée, dont la composition est validée par Progédo et qui s'engage sur sa disponibilité pendant la durée du projet. Le prestataire remet une proposition qui précise le périmètre, les lots, les livrables, les jalons, les critères de recette, le calendrier et un prix forfaitaire. Elle est validée par Progédo et fait l'objet d'un bon de commande dédié.

Le prestataire s'engage sur le résultat : les livrables sont conformes à la description validée et livrés aux dates convenues. Toute évolution du périmètre en cours de projet fait l'objet d'un avenant au bon de commande. Un comité de projet assure le suivi (cf. 3.2). Les grands chantiers envisagés pour 2027 (cf. 4.2), tels que le formulaire de dépôt, la consolidation du pipeline et la mise en production du TRE, sont susceptibles de relever de ce mode.

Le passage du mode 1 au mode 2 est proposé par le prestataire ou par Progédo, et décidé par Progédo. Une demande relève du mode 2 dès lors qu'elle remplit l'un des critères suivants :

- une charge estimée supérieure à 10 jours-homme .
- une incidence sur plusieurs composants du catalogue (cf. 4.1) ou une phase de conception ou d'architecture préalable .
- la nécessité de jalons, de livraisons intermédiaires ou d'une recette formalisée .

3.2 Gouvernance de la TMA

La gouvernance de la TMA désigne les instances par lesquelles Progédo priorise les travaux confiés au prestataire, suit leur avancement et valide leurs livrables. Elle est adaptée à chaque mode de fonctionnement (cf. 3.1) : un comité opérationnel pour les petits tickets, un comité dédié à chaque projet, le tout intégré au COPIL (cf. 2.4.4).

Comité opérationnel (mode 1)

Le comité opérationnel gère le flux des petits tickets. Il réunit un référent technique de Progédo, qui arbitre, et le responsable de la TMA côté prestataire. Il se tient une fois toutes les deux semaines. Les séances sont courtes et centrées sur le backlog.

Il assure :

- la priorisation du backlog, dont l'ordre est arrêté par Progédo .
- la validation des estimations de charge proposées par le prestataire .
- le suivi des tickets en cours, des blocages et des tickets livrés en attente de recette .
- l'identification des demandes qui doivent basculer en mode projet (cf. 3.1).

Les décisions sont consignées directement dans les tickets, sans compte rendu formel.

Comité de projet (mode 2)

Chaque projet en mode 2 dispose de son propre comité, créé au lancement et dissous à la clôture de la recette finale. Il réunit le chef de projet du prestataire, un référent de Progédo, responsable de la recette, et selon les sujets, un intervenant extérieur. Il se réunit à chaque jalon, selon un calendrier fixé dans la proposition du projet.

Il porte sur :

- l'avancement par rapport aux lots et au calendrier .
- la validation des jalons et des livrables intermédiaires .
- la recette, prononcée par Progédo : acceptée, acceptée avec réserves ou refusée. Dans ces deux derniers cas, le prestataire corrige dans un délai convenu avant une nouvelle recette .
- le suivi des risques, des dépendances externes et des demandes de changement de périmètre, qui donnent lieu à un avenant (cf. 3.1).

Le prestataire remet un compte rendu comportant les décisions, les actions, leur responsable et leur échéance, dans les cinq jours ouvrés suivant chaque séance.

Intégration au COPIL

Le COPIL trimestriel (cf. 2.4.4) donne à Progédo une vision globale de l'ensemble de la TMA. Le prestataire lui présente pour la TMA :

- l'état du backlog et les délais moyens de traitement des tickets .
- la consommation des bons de commande du mode 1 .
- l'avancement, les risques et les écarts de chaque projet en cours .
- les projets à venir et les demandes de bascule en mode projet.

Le COPIL arbitre les priorités entre le flux de tickets et les projets, ainsi qu'entre projets concurrents, et tranche les points d'escalade remontés par les comités. Un blocage qui ne peut être levé en comité opérationnel ou en comité de projet est porté au COPIL, qui peut se réunir de façon exceptionnelle si le calendrier l'exige.

3.3 Exigences techniques et qualité

Les exigences de cette section fixent les pratiques d'ingénierie que le prestataire applique à toute modification du code dans le cadre de la TMA, pour que le code livré soit fiable, maintenable, sécurisé et transférable. Elles détaillent, côté applicatif, la trajectoire décrite en 2.4.3. Elles sont obligatoires pour les nouveaux développements et appliquées de façon progressive et priorisée à l'existant, selon la feuille de route validée en COPIL. Leur mise en place ne doit pas retarder le traitement des tickets ni des projets en cours (cf. 3.1).

Exigences techniques

- CI/CD. Toute modification passe par un dépôt versionné et par un pipeline d'intégration et de livraison continues, qui compile le code, exécute les tests, puis déploie en préproduction et en production. Les déploiements sont automatisés, traçables et réversibles. La branche principale est protégée : aucune modification n'y est poussée directement, elle n'y entre que par fusion après validation du pipeline et revue (cf. 4.2.2).
- Feature flags. Le prestataire dissocie le déploiement d'une fonctionnalité de son activation, en la livrant désactivée derrière un drapeau. Celle-ci peut alors être ouverte progressivement (à quelques utilisateurs, puis à tous) et désactivée sans redéploiement en cas de problème. Les drapeaux devenus inutiles sont retirés une fois la fonctionnalité stabilisée. La solution de gestion des feature flags est à mettre en place.
- Infrastructure as Code. Tout nouveau composant applicatif est livré avec sa définition de déploiement (configuration, conteneurs, variables d'environnement) dans le dépôt, sans étape manuelle non documentée. Pour l'existant, la convergence suit la feuille de route de 2.4.3.
- Analyse de la dette technique. Le prestataire établit un état des lieux initial de la dette technique du code (dépendances obsolètes, complexité, absence de tests, documentation manquante), le tient à jour et le présente en COPIL. Les actions de réduction sont proposées sous forme de tickets priorisés par Progédo (cf. 3.1), afin que la maintenance préventive fasse l'objet d'un volume de travail identifié et non de simples bonnes intentions.
- Tests automatisés. Tout nouveau développement est livré avec ses tests (unitaires et d'intégration), et toute anomalie corrigée avec un test de non-régression. Le pipeline bloque la livraison en cas d'échec. Les seuils de couverture sont définis avec Progédo composant par composant et relevés progressivement. Ces tests n'exonèrent pas de la recette par Progédo.
- Documentation as Code. La documentation technique (architecture, API, procédures de déploiement, décisions structurantes) est rédigée dans un format ouvert, stockée dans le dépôt avec le

code et relue avec lui. Sa mise à jour fait partie de la définition de « terminé » de chaque ticket ou lot (cf. 2.4.4).

Exigences de sécurité

- Scans dans la CI. Le pipeline exécute automatiquement, à chaque modification, la recherche de dépendances vulnérables, de secrets exposés dans le code et, le cas échéant, l'analyse des images de conteneurs et des définitions d'infrastructure. Une vulnérabilité critique bloque la livraison. Les délais de correction sont ceux de 2.4.2.
- Analyse statique du code. Le code est soumis à une analyse statique à chaque modification. Le prestataire trie les résultats, corrige les alertes pertinentes et justifie par écrit les faux positifs ou les risques acceptés.
- Mise à jour des dépendances. Le prestataire met en place Renovate, ou une solution équivalente validée par Progédo, qui détecte les nouvelles versions et propose automatiquement les mises à jour. Celles-ci sont validées par le pipeline puis intégrées selon leur criticité, dans les délais de 2.4.2. Les mises à jour de faible enjeu peuvent être regroupées pour limiter la charge de relecture.
- Revue de code. Toute modification est relue par une personne autre que son auteur avant fusion. Cette revue est réalisée par le prestataire ou par l'équipe interne, selon ce qui est convenu au lancement. Les modifications touchant à l'authentification, aux droits d'accès, à l'accès aux données ou au TRE (cf. 4.2.4) font l'objet d'une seconde revue, par Progédo ou par un relecteur qu'il désigne. Les revues sont tracées dans les demandes de fusion.

3.4 Transfert de connaissances

Le transfert de connaissances désigne l'ensemble des actions par lesquelles le prestataire partage avec les équipes de Progédo la compréhension du système, du code et des choix techniques, de sorte que Progédo ne dépende pas d'une seule équipe pour le faire évoluer et l'exploiter. Il est continu, mené tout au long du marché, et se distingue de la réversibilité (cf. 2.3.3), qui organise la sortie du marché.

Le prestataire s'engage à transférer ses compétences et ses connaissances à Progédo, par les moyens suivants :

- le pairing : sur les sujets qui le justifient, les équipes internes de Progédo et celles du prestataire travaillent ensemble (programmation en binôme, revues de code partagées, interventions conjointes sur le MCO/TMA). Il est proposé par le prestataire ou demandé par Progédo, et planifié au comité opérationnel (cf. 3.2) .
- la documentation vivante (cf. 2.4.4), qui constitue le socle du transfert : décisions structurantes, procédures d'exploitation et documentation as code (cf. 3.3) .
- des sessions de présentation des livrables majeurs à la fin de chaque projet en mode 2 (architecture, choix techniques, exploitation, limites connues), et, à la demande de Progédo, des sessions thématiques sur les composants du catalogue (cf. 4.1) .
- l'accueil de nouveaux intervenants : le prestataire accompagne l'intégration de tout nouveau membre de l'équipe interne de Progédo.

Le prestataire veille également à la continuité de ses propres équipes. Tout changement d'intervenant est notifié à Progédo et accompagné d'une période de recouvrement suffisante pour que les connaissances ne soient pas perdues.

Le temps consacré au transfert est valorisé au même titre que les autres prestations : il est prévu dans les estimations des tickets et des projets, et non facturé à part.

3.5 Utilisation de l’intelligence artificielle générative

Progédo n'encourage ni ne décourage l'usage d'outils d'intelligence artificielle (assistants de code, modèles de langues, outils de génération de documentation, de tests ou d'analyse) dans l'exécution du marché. Il exige en revanche que cet usage soit *transparent*.

Obligation de signalement

Le prestataire signale systématiquement les usages d'IA qu'il fait ou envisage de faire, à deux moments :

- dans sa réponse à la consultation : il décrit les outils, les usages prévus et les mesures prises pour protéger les données de Progédo.
- au cours du marché : il informe Progédo de tout nouvel usage, ou de tout changement significatif d'outil, avant sa mise en œuvre. Le suivi est assuré par un registre des usages tenu par le prestataire, présenté en COPIL (cf. 2.4.4).

Ce signalement est informatif : il vise la transparence, non la restriction. Progédo peut toutefois s'opposer à un usage incompatible avec les exigences de sécurité, de confidentialité ou de propriété intellectuelle du marché.

Responsabilité

L'usage de l'IA ne modifie pas les obligations du prestataire. Il reste entièrement responsable de la qualité, de la sécurité et de la conformité de ses livrables, comme s'ils avaient été produits sans IA, et ils sont soumis aux mêmes revues, tests et scans (cf. 3.3). Il veille à ce que ses usages respectent la PSSI-CNRS, le RGPD et les droits de propriété intellectuelle (cf. 2.3.1). Aucune donnée non publique ou personnelle de Progédo n'est transmise à un service d'IA externe sans son accord préalable.

4. Annexes

4.1 Catalogue des services existants

Le tableau suivant liste les composants actuellement en service dans l'infrastructure Progédo.

Composant	Description
nginx-auth	—
nginx-catalog	—
Nodejs	—
Keycloak	—
ElasticSearch	—
SATOSA	L'application SATOSA, en Python, est installée depuis les sources via Git sur le serveur progedo-auth : https://github.com/IdentityPython/SATOSA
nextcloud	—
WAYF	L'application SwitchWAYF, en PHP, est installée depuis les sources via Git sur le serveur progedo-file (https://gitlab.switch.ch/aai/SWITCHwayf). Elle est installée sur le même serveur que Nextcloud afin de bénéficier de l'environnement PHP déjà en place et d'éviter l'ajout de paquets supplémentaires sur le serveur progedo-auth.
backend	—
NAS	Les serveurs progedo-file (Nextcloud) et progedo-support (Zammad) disposent d'une partition de données fournie par un NAS externe (montage NFS) . les données de Nextcloud et Zammad ne sont donc pas directement hébergées par les serveurs respectifs.
Relai mail	Tous les mails sortants depuis les serveurs de la plateforme transitent par un relais mail externe (relay.huma-num.fr).
Zimbra	Fournit un service IMAP utilisé par progedo-support (Zammad), permettant au logiciel de ticketing de récupérer les mails envoyés par les demandeurs.
Sauvegardes TSM	Les configurations locales des serveurs peuvent être expor-

	tées via le logiciel TSM vers un serveur de sauvegarde chez Huma-Num. À ce jour, ces sauvegardes ne sont pas activées, mais les flux réseau nécessaires sont paramétrés.
Serveur NTP	L'horloge de tous les serveurs de la plateforme est synchronisée via ntpsec sur un serveur NTP de Huma-Num.
BackupPC	—
Icinga2	—
nftables (auth / file / catalog / backend / support)	Règles de pare-feu appliquées sur chacun des serveurs correspondants.
Zammad	—
Zammad DB	—
Data Catalogue DB	Base PostgreSQL du catalogue.
Telegraf	Collecte, sur chaque machine, des métriques systèmes et applicatifs, transmises à une base de données InfluxDB hébergée chez Easter-Eggs et publiées via le frontend Grafana.
Apache server	—
Postfix	—
NTPsec	Implémentation sécurisée et durcie du protocole NTP (Network Time Protocol), dérivée de NTP Classic.
Loki	Puits de logs recevant les journaux collectés par l'agent Alloy.
Alloy	Agent de collecte des logs, pour envoi à Loki sur progedo-adm.

4.2 Évolutions du système d'information envisagées pour 2027

Cette section donne des exemples des différents projets envisagés pour l'année 2027.

4.2.1 Backoffice — formulaire de dépôt vers un stockage S3

Les données sont actuellement transmises via France Transfert ou des services similaires. Le lien est transmis par email aux administrateurs, en charge d'ajouter la nouvelle entrée au catalogue. Cette étape implique un travail manuel qui n'est pas nécessaire, ainsi qu'une dépendance à un service tiers.

L'objectif de ce chantier est d'ajouter un formulaire de dépôt au catalogue, qui permettra de constituer automatiquement une première partie des métadonnées (l'essentiel de docDscr dans le standard DDI, une partie de stdyDscr avec le lien vers les fichiers de données, et une première partie de dataDscr avec les statistiques descriptives associées à chaque variable). Le formulaire disposera de deux vues : une vue utilisateur et une vue administrateur, cette dernière disposant de davantage de champs.

4.2.2 Consolidation du pipeline autour d'un flux de travail orienté Git

Le flux de travail permettant d'ajouter une entrée au catalogue est aujourd'hui largement manuel et laissé à la discrétion des administrateurs. Une brique logicielle, surnommée la « moulinette », est chargée de normaliser ces entrées afin qu'elles soient lisibles par le catalogue et moissonnables.

La consolidation du pipeline, avec pour point d'entrée le formulaire mentionné en 4.2.1, permettra de supprimer cette moulinette, d'intégrer un système de versionnement des métadonnées et des DOI, d'éviter les déplacements et copies de fichiers de données, et d'améliorer la sécurité et l'efficacité du système.

Cette consolidation passe notamment par la mise en place d'une intégration continue (CI) qui :

- réagira à un évènement de fusion d'une branche dans la branche principale, en effectuant une vérification des standards de qualité à l'aide d'un validateur XML et d'un validateur Schematron pour les règles métier propres à Progédo, puis générera un nouveau DOI via DataCite (référençant l'ancien DOI en cas de nouvelle version plutôt que de nouvelle entrée) .

- réagira également aux commits sur les branches préfixées staging-*, en relançant le calcul des statistiques descriptives pour les variables lorsque l'URI des fileDscr change .
- produira, lors de la fusion d'une branche staging-* dans main, un artefact distribué aux utilisateurs du catalogue (par téléchargement direct ou via le TRE), conforme à la convention https://opendataformat.github.io/.

4.2.3 Catalogue

- système de recherche .
- référencement (SEO) et moissonnage par d'autres entrepôts .
- lien de téléchargement direct via S3, lorsque autorisé .
- suppression du recours à Nextcloud .
- suppression de la « moulinette » .
- normalisation de la documentation.

4.2.4 TRE (Trusted Research Environment)

La mise en place d'un TRE (environnement de recherche sécurisé) est actuellement explorée pour devenir la principale façon d'accéder aux données, et se destine à remplacer les téléchargements directs.

La version actuelle du TRE repose sur un environnement Coder (https://coder.com) intégré à l'environnement de préproduction, chargé de provisionner des espaces de travail (RStudio / JupyterLab) pour les chercheurs qui en font la demande. Le code produit par les chercheurs est versionné et accessible via une instance Forgejo. Les fichiers de données ne quittent pas l'environnement . la sortie des analyses se fait sur demande directe du chercheur, après vérification automatique et humaine.

L'objectif de ce chantier est la mise en production de ce système, pouvant supporter environ 30 utilisateurs simultanés. L'infrastructure devra être élastique (les ressources ne sont mobilisées qu'en fonction du besoin réel).

La sécurité du système a été placée au cœur des développements . un des axes de travail restants est la mise en place de tests de résistance et d'intrusion pour éprouver le système, ainsi que son intégration aux outils de monitoring et d'alerting existants.

4.2.5 Site web progedo.fr

Refonte envisagée du site statique, avec un CMS basé sur Git.