

Direction des Systèmes d'Information (DSN)

## **CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)**

### Objet du marché

Prestation d'hébergement physique sécurisé des équipements informatiques du Centre Hospitalier Universitaire de Toulouse dans un datacenter externalisé, incluant la mise à disposition de l'infrastructure, et les services associés.

## Sommaire

|                                                                                                          |           |
|----------------------------------------------------------------------------------------------------------|-----------|
| <b>1. Objet du marché .....</b>                                                                          | <b>3</b>  |
| <b>2. Présentation du CHU de Toulouse.....</b>                                                           | <b>3</b>  |
| <b>3. Objectif du CCTP.....</b>                                                                          | <b>4</b>  |
| <b>4. Description générale du besoin.....</b>                                                            | <b>4</b>  |
| <b>5. Exigences techniques générales .....</b>                                                           | <b>4</b>  |
| 5.1. Prérequis obligatoire et localisation du datacenter et raccordement à la boucle optique du CHU..... | 4         |
| <b>5.1.1. Localisation de la boucle optique du CHU de Toulouse .....</b>                                 | <b>4</b>  |
| <b>5.1.2. Prérequis et obligations.....</b>                                                              | <b>5</b>  |
| 5.2. Spécificités générales .....                                                                        | 5         |
| 5.3. Gestion des accès.....                                                                              | 6         |
| 5.4. Prérequis électriques .....                                                                         | 6         |
| 5.5. Refroidissement .....                                                                               | 7         |
| 5.6. Détection incendie .....                                                                            | 7         |
| 5.7. Accès opérateurs.....                                                                               | 7         |
| <b>5.7.1. Pénétrations et Cheminements.....</b>                                                          | <b>7</b>  |
| <b>5.7.2. Exigences attendues des Salles Opérateurs.....</b>                                             | <b>8</b>  |
| 5.8. Assistance au déploiement .....                                                                     | 8         |
| <b>6. Exigences RGPD.....</b>                                                                            | <b>8</b>  |
| <b>7. Exigences de reporting .....</b>                                                                   | <b>9</b>  |
| <b>8. Services de proximité .....</b>                                                                    | <b>9</b>  |
| <b>9. Exigences RSE.....</b>                                                                             | <b>9</b>  |
| 9.1. Performance énergétique & sobriété numérique .....                                                  | 9         |
| 9.2. Exigences techniques RSE spécifiques à un datacenter.....                                           | 10        |
| <b>10. Réversibilité.....</b>                                                                            | <b>10</b> |
| 10.1. Objet de la réversibilité .....                                                                    | 10        |
| 10.2. Principe général.....                                                                              | 10        |
| 10.3. Maintien des conditions d'hébergement pendant la phase de réversibilité .....                      | 10        |
| 10.4. Accès et opérations de retrait des équipements .....                                               | 11        |
| 10.5. Assistance à la réversibilité .....                                                                | 11        |
| 10.6. Sécurité et confidentialité.....                                                                   | 11        |
| 10.7. Fin de réversibilité .....                                                                         | 11        |
| 10.8. Auditabilité .....                                                                                 | 12        |
| <b>11. Planning attendu.....</b>                                                                         | <b>12</b> |

## 1. Objet du marché

Le présent CCTP a pour objet la prestation d'hébergement physique sécurisé des équipements informatiques du Centre Hospitalier Universitaire de Toulouse dans un datacenter externalisé, incluant la mise à disposition de l'infrastructure, et les services associés.

Le Centre Hospitalier Universitaire de Toulouse (ci-après « le CHU » ) souhaite une mise à disposition de solutions d'hébergement sécurisées, performantes et évolutives pour ses équipements informatiques, en appui direct du fonctionnement de son système d'information et de la continuité de ses missions de service public hospitalier.

## 2. Présentation du CHU de Toulouse

Établissement public de santé de référence, le CHU de Toulouse occupe une place majeure dans l'organisation sanitaire régionale et nationale. Premier hôpital public au palmarès 2024 et 2025 du magazine Le Point, il se distingue par l'excellence de ses pratiques médicales, la diversité de son offre de soins et la forte mobilisation de ses équipes. Le CHU regroupe plus de 16 900 professionnels, dispose d'un capacitaire d'environ 3 000 lits et places, et assure chaque année des volumes d'activité considérables, dépassant un million de consultations externes, plus de 300 000 séjours et environ 230 000 passages aux urgences. Ces missions sont rendues possibles grâce à un système d'information stratégique, dont la disponibilité et la sécurité conditionnent la qualité et la continuité du service rendu aux patients.

L'établissement est structuré autour de multiples sites hospitaliers – notamment Purpan, Rangueil–Larrey, Hôpital des Enfants, Hôtel-Dieu Saint-Jacques, Paule-de-Viguer, La Grave, ainsi que l'Institut Universitaire du Cancer Toulouse – Oncopole – couvrant l'ensemble des disciplines médicales et médico-techniques. Ce maillage territorial lui permet de remplir pleinement ses missions de soins, d'enseignement, de recherche et d'innovation, en lien étroit avec l'Université de Toulouse.

Le CHU met en œuvre un projet d'établissement 2023-2028 visant à renforcer son excellence médicale, moderniser ses infrastructures, améliorer la prise en charge des patients et soutenir ses équipes. Ce projet s'accompagne d'un plan d'investissement majeur de 550 millions d'euros destiné notamment à moderniser l'Hôpital des Enfants et à renforcer les capacités de l'Oncopole. Dans ce contexte d'évolution et de transformation à grande échelle, la sécurisation, la performance et la résilience du système d'information constituent des enjeux prioritaires.

Le recours au présent CCTP répond ainsi à la nécessité pour le CHU de disposer d'un environnement d'hébergement hautement fiable, sécurisé, scalable, et conforme aux exigences applicables aux établissements de santé. L'objectif est de garantir la continuité des services numériques critiques, de renforcer la protection du patrimoine informationnel, et d'accompagner la montée en charge des projets numériques actuels et futurs.

Le titulaire devra, à ce titre, proposer une solution d'hébergement répondant aux standards les plus exigeants en matière de disponibilité, de cybersécurité, de performance, de pilotage opérationnel et d'interopérabilité, afin de soutenir durablement le fonctionnement du système d'information du CHU.

### 3. Objectif du CCTP

Le présent Cahier des Clauses Techniques Particulières (CCTP) a pour objectif de définir les exigences liées à la prestation d'hébergement physique des équipements informatiques du Centre Hospitalier Universitaire (CHU) de Toulouse dans un datacenter externalisé.

La prestation inclut la mise à disposition d'espaces, d'équipements, de services et de garanties permettant d'assurer un hébergement sécurisé, conforme et opérationnel.

### 4. Description générale du besoin

Le CHU de Toulouse souhaite externaliser une partie de son infrastructure informatique au sein d'un datacenter certifié Hébergeur de Données de Santé (HDS), pour l'activité 1 conformément au Référentiel Hébergeur de Données de Santé<sup>1</sup> et de l'article R.1111.9 du Code de la santé publique. La volumétrie cible actuelle est de 13 baies 42U complètes, destinées à recevoir des équipements réseau (3 baies), des serveurs et unités de stockage (10 baies) du CHU.

Les exigences incluent également une haute disponibilité, la cybersécurité, la continuité d'activité et le respect des normes en vigueur.

### 5. Exigences techniques générales

#### 5.1. Prérequis obligatoire et localisation du datacenter et raccordement à la boucle optique du CHU

##### 5.1.1. Localisation de la boucle optique du CHU de Toulouse

Le CHU de Toulouse dispose d'une infrastructure réseau interconnectant ses différents sites via une boucle optique Zefil, maintenue auprès de l'opérateur SPL RIN. Les sites actuellement desservis par cette boucle sont les suivants:

- Numih France (Basso Cambo),
- LogiPharma (Cugnaux),
- Le Chapitre (zone Thibaud),
- IUCT-Oncopole,
- Rangueil,
- L'Hôtel-Dieu,
- Purpan.

---

1. Arrêté du 26 avril 2024 modifiant l'arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel

### 5.1.2. Prérequis et obligations

Le datacenter objet du présent marché devra être obligatoirement raccordé à la boucle optique du CHU de Toulouse en tant que nouveau site de celui-ci.

Dans ce cadre, le titulaire devra :

1. **Vérifier la faisabilité technique auprès de SPL RIN** et s'assurer que son datacenter :
  - Est accessible par deux chemins distincts de fibre optique
  - Fournir un schéma détaillé du cheminement physique de ces deux liaisons, incluant les points de raccordement et les éventuels nœuds intermédiaires.
2. **Réaliser une étude de faisabilité** incluant :
  - L'évaluation des longueurs des tronçons supplémentaires de fibre optique entre le datacenter proposé et les sites les plus proches de la boucle optique existante du CHU de Toulouse.
  - L'estimation du coût mensuel de location pour chacun des deux tronçons.
  - Le calcul de l'atténuation maximale estimée (en dB) pour chaque tronçon, en précisant les hypothèses de calcul (type de fibre, longueurs d'onde utilisées, etc.).

➤ **Contacts pour l'étude de faisabilité :**

Les deux interlocuteurs à contacter pour mener cette étude sont :

| Noms            | Fonctions                                                                    | Courriel                 |
|-----------------|------------------------------------------------------------------------------|--------------------------|
| Philippe Mlakar | Directeur Général<br>Réseaux d'Infrastructures<br>Numériques                 | philippe.mlakar@zefil.fr |
| Yannick Marsal  | Responsable Travaux et Prévention<br>Réseaux d'Infrastructures<br>Numériques | yannick.marsal@zefil.fr  |

L'offre du titulaire inclura la liste des risques environnementaux associés à la localisation du datacenter.

Le titulaire devra être impérativement éligible au raccordement à la boucle.

## 5.2. Spécificités générales

Le datacenter devra obligatoirement répondre à des exigences Tiers III minimum en termes de continuité de service et assurer une disponibilité minimale de 99,95% (SLA).

L'hébergeur devra obligatoirement disposer de certifications ISO27001 et HDS en cours de validité, couvrant a minima les périmètres : hébergement physique, hébergement d'infrastructure, exploitation et administration. Le titulaire devra amener la preuve de ces certifications et fournir annuellement la mise à jour de ses certificats en y ajoutant la déclaration d'applicabilité associée.

L'hébergeur devra mettre à disposition de 13 baies 42U verrouillables. Ces baies devront être localisées dans des cages mutualisées uniquement pour le CHU de Toulouse.

Des cages privatives pourront être demandées en cours de marché selon la survenance des besoins.

Les racks mis à disposition devront être modulable afin d'accueillir les équipements d'une profondeur utile supérieure à 1000mm .

La capacité de charge de ces racks devra être conforme aux équipements lourds, minimum 1000kg par baies.

L'hébergeur devra être en capacité de mettre à disposition des intervenants externes un espace de travail distinct du datacenter pour des opérations ponctuelles.

### 5.3. Gestion des accès

Le datacenter devra être accessible 24h/24, 7j/7 pour les agents autorisés par le CHU de manière permanente. L'accès ponctuel au datacenter demandé pour un intervenant devra se faire avec l'accompagnement permanent d'un agent DSN habilité ou personnel de l'hébergeur avec autorisation écrite préalable d'un agent DSN habilité.

Un contact humain devra être possible 24h/24, 7j/7 et une procédure d'escalade managériale de l'hébergeur devra être communiquée au CHU.

L'hébergeur devra mettre à disposition du CHU un quai de livraison compatible avec un acheminement d'équipements par un semi-remorque ainsi qu'une zone de stockage temporaire pour le matériel livré. Il devra également mettre à disposition une zone de stationnement pour les intervenants du datacenter. L'hébergeur devra fournir dans son mémoire technique, le détail du cheminement d'un matériel depuis la zone de décharge jusqu'aux baies d'hébergement.

L'hébergeur devra garantir une autonomie de travail (installation et intervention) aux personnels du CHU et de maintenances identifiés, dans le strict respect des bonnes pratiques imposées par l'hébergeur.

Les accès aux baies devront être gérés par des systèmes de contrôle d'accès physiques (clés, badges, biométrie, ...), tracés (6 mois minimum de rétention, idéalement 1 an) et devront faire l'objet d'une vidéosurveillance continue avec une rétention des enregistrements à expliciter, idéalement entre 15 jours à 1 mois. Le CHU, dans le cadre de sa propre certification, pourra se réserver le droit de demander des extractions ponctuelles des journaux d'accès voire des vidéos de surveillance si un acte malveillant est suspecté.

L'hébergeur devra garantir une sécurité périmétrique renforcée du datacenter via des alarmes ou de la surveillance humaine 24/7.

### 5.4. Prérequis électriques

La redondance électrique du datacenter doit être N+1 ou supérieure. Les équipements nécessaires à la fourniture d'électricité au datacenter doivent être supervisés et faire l'objet d'alarmes dédiées et de procédures de remédiation associées.

Les groupes électrogènes doivent être régulièrement testés et des comptes-rendus de ces tests doivent être communiqués au CHU.

Chaque rack mis à disposition du CHU doit être équipé :

- D'une double alimentation électrique A+B
- D'une capacité minimale de 3 à 8kVA
- De connecteurs de type C13 et C19 pour une trentaine de points de connexion
- D'un système de mesure de la consommation électrique

Les relevés de consommation seront transmis régulièrement au travers des comités de pilotage.

### 5.5. Refroidissement

La capacité de refroidissement du datacenter doit être redondée N+1 minimum. Les équipements nécessaires au refroidissement du datacenter doivent être supervisés et faire l'objet d'alarmes dédiées et de procédures de remédiation associées.

La bascule des éléments de refroidissement doit être régulièrement testée et des comptes-rendus de ces tests doivent être communiqués au CHU.

Le datacenter doit être équipé d'appareil de mesure de la température et de l'hygrométrie. Les plages cibles acceptables sont celles d'un datacenter classique à savoir :

- Température : 20-28°C
- Hygrométrie : 40-60%

### 5.6. Détection incendie

Le datacenter doit être équipé d'une détection incendie (type VESDA) et d'une extinction automatique sans résidu (gaz inerte).

### 5.7. Accès opérateurs

Le site d'hébergement doit obligatoirement disposer d'une double pénétration (est/ouest ou nord/sud), ainsi que de salles d'arrivée dédiées pour accueillir les équipements des opérateurs télécom (RAD, routeurs, commutateurs, etc.).

#### 5.7.1. Pénétrations et Cheminements

- Les deux pénétrations opérateurs doivent être physiquement distinctes et disposer de cheminements séparés jusqu'au domaine public, afin d'éliminer tout Single Point of Failure (SPOF).
- La distance minimale entre les deux trajets physiques doit être de 20 mètres, pour éviter qu'un incident localisé n'impacte simultanément les deux cheminements.
- Les cheminements sont composés de fourreaux rigides et étanches, dont le taux d'occupation doit permettre le déploiement et l'évolution des opérateurs nécessaires à l'hébergement du système d'information des Hôpitaux de Toulouse.

### 5.7.2. Exigences attendues des Salles Opérateurs

Les salles opérateurs doivent répondre aux mêmes critères techniques décrits dans les *Chapitres précédents*, plus ceux ci-dessous :

- **Sécurité physique**
  - Sas d'entrée sécurisés avec détection d'intrusion.
  - Accès strictement contrôlé et réservé aux techniciens agréés.
- **Infrastructure réseau**
  - Rocades cuivre (catégorie 6) et fibres optiques (monomode et/ou multimode) en nombre suffisant.
  - Minimum de 12 fibres optiques et 12 câbles RJ45 disponibles entre les deux salles d'arrivées opérateurs, ainsi qu'entre chacune d'elles et les baies télécom mises à disposition dans le cadre du marché.
- **Cheminements dédiés**
  - Les rocade cuivre et optique entre les baies télécom du CHU de Toulouse et les deux salles d'arrivées opérateurs doivent disposer de cheminements propres et indépendants.

### 5.8. Assistance au déploiement

Le titulaire s'engage à assister le CHU le jour des déménagements en assurant une présence physique le jour J et détaillera le plan d'assistance au déménagement qu'il propose.

## 6. Exigences RGPD

L'offre du titulaire inclura le clausier SSI/RGPD en annexe complété.

Plus particulièrement, le titulaire s'engage à garantir le stockage, la conservation et la protection des données hébergées du CHU de Toulouse présentes sur au sein du datacenter et à assurer par tout moyen approprié la confidentialité, l'intégrité et la sécurité des données hébergées contre les risques de perte d'altération ou d'accès non autorisé.

À ce titre, le titulaire s'engage à communiquer et à mettre en œuvre les mesures de sécurité techniques et organisationnelles adaptées au niveau de risque inhérent auquel sont exposés lesdites données, et de maintenir celles-ci à l'état de l'art technique en vigueur.

De plus, le titulaire, au travers de la complétion du Clausier devra garantir que son personnel est soumis au secret professionnel et s'engage à une obligation de confidentialité de toutes les données et informations dont il aurait connaissance du fait de l'exécution du service et s'engage également à une discrétion absolue sur le service et sur l'activité du CHU de Toulouse. En tout état de cause, le personnel du titulaire s'engage par ailleurs à ne pas utiliser les données, documents et informations traitées à des fins autres que celles spécifiées pour les besoins du Marché.

Le titulaire veillera à la sensibilisation de son personnel mais également de celui de ses éventuels Sous-traitants à la protection données du CHU de Toulouse en termes de disponibilité, confidentialité et intégrité des Données.

Enfin, le titulaire s'engage à lister ses sous-traitants et garantit que ces derniers ont les mêmes obligations en la matière encadrée contractuellement.

## 7. Exigences de reporting

Le titulaire s'engage à animer un comité de pilotage trimestriel dans lequel seront fournis les rapports suivants :

- Rapports des incidents déclarés dans la période :
  - Incidents d'infrastructure
  - Incidents sur les accès physiques
- Rapport de respect des délais de traitement des incidents/demandes
- Rapport d'avancement des maintenances annuelles prévues au datacenter par l'hébergeur
- Rapports de capacité par rack :
  - Utilisation de la capacité électrique
  - Utilisations de l'espace disponible (nombre de U)
- Rapport des activités de proximité
- Rapport des accès CHU au datacenter
- Faits marquants période passée et à venir

Le titulaire devra mettre en place une main courante numérique et en donner l'accès au CHU.

Le titulaire devra enfin s'engager à fournir les rapports d'audits de sécurité sur les services mutualisés à la demande du CHU tel que cela est demandé par la norme HDS annuellement à date anniversaire du marché. A ce titre il devra fournir son planning prévisionnel desdits audits.

## 8. Services de proximité

Le titulaire devra être en capacité de fournir les services de proximité suivants :

- Assurer l'accueil des fournisseurs du CHU
- Assurer des interventions sur les équipements CHU, pilotées à distance par un technicien du CHU, sous 4h ou immédiatement en urgence.
- Assurer des prestations de câblages (RJ45 et FC) dans un délai d'une semaine.

L'offre du titulaire inclura ses engagements de traitement des demandes du CHU pour chacune des tâches listées.

L'offre du titulaire explicitera la méthode de sollicitation :

- Mode d'urgence
- Mode standard

## 9. Exigences RSE

### 9.1. Performance énergétique & sobriété numérique

L'hébergement doit intégrer des critères permettant de réduire la consommation d'énergie, conformément aux pratiques RSE du secteur informatique, qui incluent :

- Optimisation énergétique des infrastructures IT et salles serveurs (conception, refroidissement, renouvellement efficace des équipements, monitoring énergétique).
- Mise en œuvre d'une informatique durable (Green IT) : audit des serveurs, infrastructures, logiciels pour réduire leur consommation.

L'offre du titulaire peut inclure à ce titre :

- Des indicateurs de performance énergétique (PUE, DCIE).
- Inventaire et plan de réduction des consommations électriques.
- Une justification de la politique énergétique du fournisseur (ISO 50001 ou équivalent).

## 9.2. Exigences techniques RSE spécifiques à un datacenter

D'après les bonnes pratiques du secteur :

- Contrôle continu du refroidissement, limitation des fuites énergétiques.
- Optimisation de la répartition de charge (virtualisation, mutualisation).
- Gestion responsable des infrastructures critiques (onduleurs, groupes électrogènes, batteries).

# 10. Réversibilité

## 10.1. Objet de la réversibilité

La présente clause a pour objet de définir les conditions dans lesquelles le CHU peut, à l'échéance du présent marché ou en cas de résiliation anticipée, cesser l'hébergement de ses équipements au sein des sites physiques du titulaire, dans le respect des exigences applicables à l'hébergement de données de santé à caractère personnel.

Le délai de réversibilité sera de 3 mois, en cas de dénonciation du marché.

Dans le cadre du renouvellement du marché impliquant un changement de titulaire, le délai de réversibilité sera d'un an.

## 10.2. Principe général

Le titulaire s'engage à permettre au CHU de reprendre l'entière maîtrise de ses équipements hébergés, ou de les transférer vers un autre site de son choix, sans interruption injustifiée des conditions d'hébergement, et dans des conditions garantissant la sécurité, l'intégrité et la confidentialité des données de santé concernées.

## 10.3. Maintien des conditions d'hébergement pendant la phase de réversibilité

Jusqu'à la date effective de sortie des équipements :

- Le titulaire maintiendra les conditions d'hébergement physique prévues au contrat, notamment en matière :
  - d'alimentation électrique,

- de climatisation,
  - de sécurité physique,
  - de détection et protection incendie ;
- aucune modification des conditions techniques ou organisationnelles ne peut être apportée sans information préalable du CHU, sauf impératif de sécurité.

#### **10.4. Accès et opérations de retrait des équipements**

Le titulaire s'engage à :

- autoriser l'accès du CHU ou de tout prestataire dûment mandaté par celui-ci aux sites concernés, dans le respect des règles de sécurité en vigueur ;
- définir des modalités d'accès compatibles avec les contraintes de sécurité du site, incluant la traçabilité des interventions ;
- permettre les opérations de désinstallation, déconnexion et retrait des équipements, dans des délais raisonnables et coordonnés.

#### **10.5. Assistance à la réversibilité**

Dans le cadre de la réversibilité, le titulaire s'engage à fournir au Client :

- les informations nécessaires relatives aux contraintes physiques et techniques du site (baies, alimentation, refroidissement, accès) ;
- une coopération raisonnable à la coordination des opérations, sans obligation de prestation d'ingénierie ou de migration.

Toute assistance complémentaire pourra faire l'objet d'une facturation spécifique selon les conditions prévues au contrat.

#### **10.6. Sécurité et confidentialité**

Pendant toute la durée de la réversibilité :

- les règles de contrôle d'accès physique et de confidentialité applicables à l'hébergement de données de santé sont maintenues ;
- le titulaire veillera à ce qu'aucune information relative aux données du CHU ne soit conservée ou exploitée au-delà de la sortie effective des équipements.

#### **10.7. Fin de réversibilité**

La réversibilité sera réputée achevée à la date à laquelle :

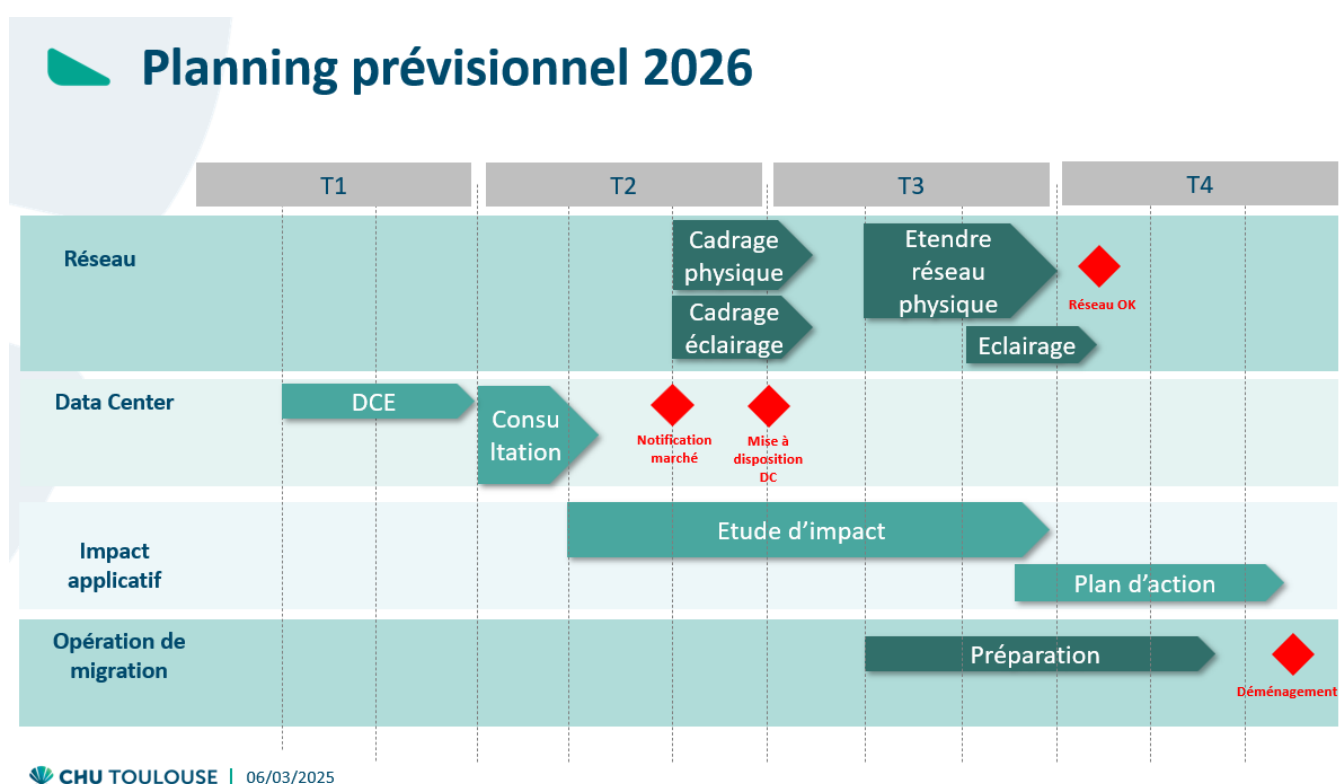
- l'ensemble des équipements du CHU a quitté les sites de l'Hébergeur, ou
- les emplacements concernés ont été libérés et restitués conformément aux stipulations contractuelles.

À compter de cette date, le titulaire n'assume plus aucune obligation au titre de l'hébergement des équipements du CHU.

### 10.8. Auditabilité

La présente clause et les procédures associées seront documentées et tenues à disposition en cas de contrôle ou d'audit relatif à la certification Hébergeur de Données de Santé.

## 11. Planning attendu



Les dates indiquées dans le schéma ci-dessus (T1-T2-T3-T4) sont prévisionnelles et pourront glisser en fonction du calendrier réel. Il en est de même des délais propres à chaque tâche ou entre plusieurs tâches, à l'exception du délai entre la notification du marché et la mise à disposition du datacenter, qui sera impérativement d'un mois maximum.