

ACCORD DE SOUS-TRAITANCE DES DONNÉES À CARACTÈRE PERSONNEL (DPA)

Version 1.3 du 12.06.2026

Le présent Accord de sous-traitance des données à caractère personnel (ci-après le « DPA ») constitue une annexe au Contrat conclu entre Cloud Temple et le Client. Il définit les conditions dans lesquelles Cloud Temple, en qualité de sous-traitant, traite les Données à Caractère Personnel pour le compte du Client, responsable de traitement, conformément à l'article 28 du Règlement (UE) 2016/679 (« RGPD »).

ARTICLE 1 : DÉFINITIONS	2
ARTICLE 2 : OBJET	2
ARTICLE 3 : OBLIGATIONS DU RESPONSABLE DE TRAITEMENT	2
ARTICLE 4 : OBLIGATIONS DU SOUS-TRAITANT	3
ARTICLE 5 : DESCRIPTION DES TRAITEMENTS	3
ARTICLE 6 : DROITS DES PERSONNES CONCERNÉES	4
ARTICLE 7 : MESURES DE SÉCURITÉ ET DE CONFIDENTIALITÉ	4
ARTICLE 8 : NOTIFICATION DES VIOLATIONS DE DONNÉES	5
ARTICLE 9 : TRANSFERTS DE DONNÉES HORS DE L'UNION EUROPÉENNE	5
ARTICLE 10 : DURÉE ET FIN DU TRAITEMENT	6
ARTICLE 11 : DOCUMENTATION ET AUDITS	6
ARTICLE 12 : REGISTRES DES ACTIVITÉS DE TRAITEMENT	6
ARTICLE 13 : LES SOUS-TRAITANTS ULTÉRIEURS	7
ARTICLE 14 : RESPONSABILITÉ	8
ARTICLE 15 : MODIFICATIONS	8
ARTICLE 16 : LOI APPLICABLE ET JURIDICTION COMPÉTENTE	8

ARTICLE 1 : DÉFINITIONS

- Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée »), telle que définie par le Règlement Général sur la Protection des Données (RGPD).
- Responsable de traitement : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données à caractère personnel.
- Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du Responsable de traitement.
- Traitement : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel.
- Instruction documentée : toute instruction du Responsable de traitement encadrant le traitement des données à caractère personnel par le Sous-traitant, prenant l'une des deux formes suivantes :
- Instruction spécifique : instruction contenue dans le Contrat principal, ses annexes, ou toute demande écrite ultérieure du Responsable de traitement (courrier, courriel, ticket du portail de support, compte rendu de comité de suivi signé ou validé par les deux Parties) ;
- Instruction générique : instruction résultant de l'utilisation, par le Responsable de traitement, des Services tels que décrits dans le catalogue de services de Cloud Temple (accessible sur docs.cloud-temple.com et tenu à jour), notamment via la Console ou les interfaces de programmation (API) mises à disposition, dans les limites des paramètres et fonctionnalités proposés par ces Services.
- Si le Sous-traitant considère qu'une instruction constitue une violation du RGPD ou de toute autre disposition relative à la protection des données, il en informe immédiatement le Responsable de traitement, conformément à l'article 28.3.a du RGPD.
- Violation de données : une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou autrement traitées, ou l'accès non autorisé à de telles données.
- Transfert de données : tout transfert de données à caractère personnel en dehors de l'Espace Économique Européen (EEE), y compris vers un pays tiers ou une organisation internationale.
- Service Cloud : tout service de traitement, stockage ou gestion de données à caractère personnel fourni par le Sous-traitant via des infrastructures cloud.
- Accès nécessaire au service : tout accès aux données à caractère personnel strictement requis pour l'exécution des services contractuels définis, incluant la fourniture, la maintenance, le support technique, la supervision des systèmes et la résolution d'incidents, à l'exclusion de tout accès à des fins d'analyse commerciale, de profilage ou de marketing direct.
- HDS (Hébergeur de Données de Santé) : statut spécifique en France pour les hébergeurs de données de santé, nécessitant une certification délivrée par un organisme accrédité.

ARTICLE 2 : OBJET

Le présent DPA a pour objet de définir les conditions et modalités de traitement des données à caractère personnel dans le cadre du Contrat principal, incluant l'utilisation de services cloud. Il vise à garantir la conformité des Parties aux obligations découlant du RGPD et des lois françaises relatives à la protection des données personnelles, dans le cas où le Sous-traitant est certifié HDS, ainsi qu'aux exigences du code de conduite CISPE.

ARTICLE 3 : OBLIGATIONS DU RESPONSABLE DE TRAITEMENT

- Licéité du traitement : le Responsable de traitement s'engage à traiter les données à caractère personnel de manière licite, loyale et transparente, conformément aux articles 5 et 6 du RGPD.
- Finalités déterminées : les données à caractère personnel ne doivent être collectées que pour des finalités déterminées, explicites et légitimes, et ne doivent pas être traitées ultérieurement de manière incompatible avec ces finalités.
- Minimisation des données : le Responsable de traitement doit veiller à ce que les données collectées soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

- ☐ Exactitude des données : il incombe au Responsable de traitement de s'assurer que les données à caractère personnel sont exactes et, si nécessaire, tenues à jour.
- ☐ Sécurité des données : le Responsable de traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD, ce qui inclut l'évaluation régulière des mesures de sécurité des services cloud utilisés.

ARTICLE 4 : OBLIGATIONS DU SOUS-TRAITANT

4.1 Traitement conforme aux instructions et limitation des accès

Le Sous-traitant s'engage à :

- ☐ ne traiter les données à caractère personnel que sur instruction documentée du Responsable de traitement, telle que définie à l'Article 1, y compris en ce qui concerne les transferts vers un pays tiers ou une organisation internationale, sauf obligation légale contraire ;
- ☐ limiter strictement ses accès aux seuls accès nécessaires au service tels que définis à l'Article 1 ;
- ☐ s'interdire formellement tout traitement à des fins d'exploration de données (data mining) ;
- ☐ s'interdire le profilage des utilisateurs finaux ou l'analyse comportementale ;
- ☐ s'interdire le marketing direct ou la publicité ciblée ;
- ☐ s'interdire toute utilisation commerciale non liée à l'exécution des services contractuels.

4.2 Politique de gestion des accès

Le Sous-traitant maintient une politique détaillée de gestion des accès aux données clients qui inclut :

- ☐ les procédures d'autorisation et de révocation des accès ;
- ☐ l'identification des personnes habilitées et leurs niveaux d'accès ;
- ☐ les contrôles d'accès physiques et techniques aux infrastructures ;
- ☐ la journalisation complète des accès avec conservation sur 24 mois minimum ;
- ☐ les procédures de gestion des accès d'urgence et de supervision.

4.3 Obligations générales

- ☐ Confidentialité : le Sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.
- ☐ Certification HDS : le Sous-traitant déclare être certifié Hébergeur de Données de Santé et maintiendra cette certification pendant toute la durée du Contrat.
- ☐ Sécurité des traitements : le Sous-traitant met en œuvre les mesures techniques et organisationnelles appropriées pour garantir la sécurité des données à caractère personnel qu'il traite, y compris via des services cloud, conformément à l'article 32 du RGPD.
- ☐ Sous-traitance ultérieure : le Sous-traitant ne recourt à un autre sous-traitant que dans les conditions prévues à l'Article 13. En cas de sous-traitance ultérieure autorisée, il s'assure que le sous-traitant ultérieur respecte les mêmes obligations de protection des données.
- ☐ Assistance au Responsable de traitement : le Sous-traitant assiste le Responsable de traitement, dans la mesure du possible, pour s'acquitter de ses obligations en matière de sécurité des données, de notification des violations, de réalisation d'analyses d'impact (AIPD) et de consultations préalables auprès des autorités de contrôle.
- ☐ Localisation des données : le Sous-traitant fournit des informations claires sur les lieux de stockage et de traitement des données dans les infrastructures cloud, et s'assure que ces lieux respectent les réglementations applicables.

ARTICLE 5 : DESCRIPTION DES TRAITEMENTS

Le Sous-traitant est autorisé à traiter, pour le compte du Responsable de traitement, les données à caractère personnel nécessaires à la fourniture des Services. La nature et la catégorie des opérations réalisées sur les données sont définies par le Responsable de traitement selon les besoins spécifiques de chaque Service. Les

finalités du traitement sont déterminées par le Responsable de traitement et communiquées au Sous-traitant. La nature et la catégorie des données traitées, ainsi que les catégories de personnes concernées, sont spécifiées par le Responsable de traitement. Pour l'exécution des Services, le Responsable de traitement met à la disposition du Sous-traitant les informations nécessaires. La durée du traitement est fixée par le Responsable de traitement en fonction des exigences des Services fournis.

ARTICLE 6 : DROITS DES PERSONNES CONCERNÉES

- ☐ Accès et rectification : les Parties permettent aux personnes concernées d'exercer leurs droits d'accès et de rectification, conformément aux articles 15 et 16 du RGPD.
- ☐ Effacement et limitation du traitement : les personnes concernées peuvent exercer leurs droits à l'effacement (droit à l'oubli) ou à la limitation du traitement, conformément aux articles 17 et 18 du RGPD.
- ☐ Portabilité des données : le Responsable de traitement assure, lorsque cela est applicable, la portabilité des données, conformément à l'article 20 du RGPD.
- ☐ Opposition : les personnes concernées peuvent exercer leur droit d'opposition, conformément à l'article 21 du RGPD.

6.1 Modalités d'exercice des droits

En tant que Sous-traitant, Cloud Temple assiste le Responsable de traitement dans l'exercice des droits des personnes concernées selon les modalités suivantes.

Processus standard : les demandes sont généralement adressées par le Responsable de traitement via les canaux habituels (Account Manager et Service Delivery Manager) ; le Sous-traitant fournit son assistance technique dans les limites de son rôle et des capacités de ses services.

Contact direct : pour les cas exceptionnels, le Délégué à la Protection des Données de Cloud Temple peut être contacté directement (DPD@cloud-temple.com). Un circuit de validation par le DPO de Cloud Temple est maintenu pour assurer la cohérence des réponses, et une traçabilité des demandes et actions est assurée.

Réception des demandes : dans l'éventualité où une personne concernée adresserait directement une demande d'exercice de ses droits au Sous-traitant, ce dernier s'engage à la transmettre au Client par écrit, via le portail de support ou l'adresse DPD@cloud-temple.com, dans un délai maximum de 72 heures. Le Sous-traitant ne répond pas directement à la personne concernée sans instruction écrite préalable du Responsable de traitement.

Assistance technique et exécution : le Sous-traitant assiste le Client dans les conditions suivantes :

- ☐ Accès et portabilité : mise à disposition des outils ou procédures permettant l'extraction des données dans un format structuré et couramment utilisé.
- ☐ Consultation des traces : l'Hébergeur permet au Client de consulter les traces d'accès aux Données de Santé à Caractère Personnel (DSCP).
- ☐ Rectification et effacement : exécution, sur demande motivée du Client, des opérations techniques de modification ou de suppression définitive dans les environnements de production et de sauvegarde, avec confirmation écrite.
- ☐ Limitation : mise en œuvre, en collaboration avec le Client, des mesures techniques d'isolation ou de verrouillage des données concernées.
- ☐ Documentation : mise à disposition des informations nécessaires pour démontrer le respect effectif des droits des personnes.

ARTICLE 7 : MESURES DE SÉCURITÉ ET DE CONFIDENTIALITÉ

Le Sous-traitant s'engage à mettre en place les mesures suffisantes pour assurer la sécurité et la confidentialité des Données Personnelles, notamment de santé, confiées et traitées dans le cadre des Services, à savoir notamment :

- ☐ mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte, l'altération, l'utilisation détournée, la diffusion ou l'accès non autorisés, ainsi que contre toute autre forme de traitement illicite ;

- ☐ ne pas utiliser les données pour son propre compte ou pour le compte de tiers, et ne pas les transférer sans l'autorisation écrite et préalable du Responsable de traitement ou du client final ;
- ☐ veiller à ce que les personnes autorisées à traiter les données soient soumises à des obligations appropriées de confidentialité ;
- ☐ ne pas réaliser de copies ou duplications des données sans l'autorisation écrite préalable du Responsable de traitement, sauf nécessité d'exécution des Services ;
- ☐ informer le Responsable de traitement de tout accès accidentel ou non autorisé, de tout manquement ou suspicion de manquement à la réglementation, dans les meilleurs délais et, si possible, 48 heures au plus tard après en avoir pris connaissance ;
- ☐ selon le choix du Responsable de traitement, supprimer ou restituer les données au terme du Contrat et détruire les copies existantes, sauf obligation légale de conservation ;
- ☐ mettre en œuvre une politique de sécurité des systèmes d'information et de gestion des autorisations d'accès logique et physique, maintenue et mise à jour pendant toute la durée du Contrat ;
- ☐ chiffrer les données stockées.

Le Sous-traitant met en œuvre un système de contrôle d'accès aux données clients comprenant :

- ☐ un système d'authentification forte et de gestion des identités ;
- ☐ une politique de moindre privilège avec révision périodique des autorisations ;
- ☐ une séparation des environnements clients et une isolation des données ;
- ☐ un système de journalisation complet avec alertes automatiques ;
- ☐ des audits périodiques des accès et des contrôles de sécurité.

ARTICLE 8 : NOTIFICATION DES VIOLATIONS DE DONNÉES

En cas de violation de données à caractère personnel ou de Données de Santé à Caractère Personnel, le Sous-traitant notifie cette violation au Responsable de traitement sans délai indu après en avoir pris connaissance. Cette notification inclut :

- ☐ la nature de la violation ;
- ☐ les catégories et le nombre approximatif de personnes concernées ;
- ☐ les catégories et le nombre approximatif d'enregistrements de données concernés ;
- ☐ le nom et les coordonnées du point de contact où des informations supplémentaires peuvent être obtenues ;
- ☐ les conséquences probables de la violation ;
- ☐ les mesures prises ou envisagées pour remédier à la violation et atténuer ses effets négatifs.

La notification précise l'impact potentiel sur les données hébergées dans le cloud et les mesures prises pour y remédier, permettant au Responsable de traitement de notifier cette violation à l'autorité de contrôle compétente et, le cas échéant, aux personnes concernées, conformément à l'article 33 du RGPD.

ARTICLE 9 : TRANSFERTS DE DONNÉES HORS DE L'UNION EUROPÉENNE

9.1 Localisation des données selon les services

Services Cloud :

- ☐ toutes les données à caractère personnel sont exclusivement traitées et stockées au sein de l'Union européenne ;
- ☐ l'ensemble des infrastructures et datacenters sont situés dans l'Union européenne ;
- ☐ le Client peut sélectionner les zones géographiques de traitement parmi les localisations européennes disponibles ; aucun traitement ou stockage n'a lieu en dehors de l'Union européenne.

Services Managés (Infogérance) :

- ☐ les données à caractère personnel sont par défaut traitées et stockées au sein de l'Union européenne ;

- ☐ des équipes de support technique situées hors de l'Union européenne peuvent être amenées à accéder aux données dans le cadre de la prestation, uniquement avec l'accord préalable et écrit du Responsable de traitement ;
- ☐ ces accès sont strictement limités aux besoins opérationnels et encadrés par les garanties appropriées du RGPD.

9.2 Conditions des transferts hors UE

Tout accès ou transfert de données vers des pays tiers ne peut être effectué qu'avec :

- ☐ l'autorisation préalable et écrite du Responsable de traitement pour le service concerné ;
- ☐ le respect des conditions prévues par le RGPD, notamment ses articles 44 à 50 ;
- ☐ la mise en place de garanties appropriées (clauses contractuelles types approuvées par la Commission européenne ou décision d'adéquation) ;
- ☐ la limitation des accès aux seuls besoins opérationnels.

ARTICLE 10 : DURÉE ET FIN DU TRAITEMENT

10.1 Fin de contrat

À l'issue du Contrat principal, le Sous-traitant s'engage, selon les instructions du Responsable de traitement, à supprimer toutes les données à caractère personnel ou à les restituer, et à détruire les copies existantes, sauf obligation légale contraire.

10.2 Processus de récupération

Le Sous-traitant fournit un guide détaillé permettant au Responsable de traitement de récupérer ses données dans un format standard et exploitable, incluant les formats d'export disponibles, les procédures de récupération, les délais de mise à disposition et l'assistance technique disponible.

10.3 Délais de suppression des données

Le Sous-traitant s'engage sur les délais suivants :

- ☐ suppression logique : dans les 48 heures suivant la demande ;
- ☐ suppression physique définitive : dans les 30 jours calendaires suivant la suppression logique ;
- ☐ confirmation de suppression : certificat de destruction fourni dans les 5 jours ouvrés suivant la suppression physique.

Cette obligation inclut les données stockées sur des supports de sauvegarde, sauf obligation légale de conservation ; dans ce cas, le Sous-traitant en informe le Responsable de traitement avec justification légale et délai de conservation.

ARTICLE 11 : DOCUMENTATION ET AUDITS

Le Sous-traitant met à la disposition du Responsable de traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues par le présent DPA et autorise les audits, y compris les inspections, par le Responsable de traitement ou un auditeur mandaté, afin de vérifier la conformité avec le présent DPA et le RGPD.

Le Sous-traitant met à disposition :

- ☐ une page dédiée listant l'ensemble des démarches de conformité, tenue à jour à l'adresse cloud-temple.com/demarches-conformite ;
- ☐ les attestations de conformité disponibles (ISO 27001, SecNumCloud, HDS, ISAE 3402, etc.) ;
- ☐ des recommandations pour l'utilisation sécurisée des services Cloud Temple, incluant les bonnes pratiques de protection de l'accès à la Console, la gestion maîtrisée des accès et permissions, et la sécurisation des ressources déployées.

ARTICLE 12 : REGISTRES DES ACTIVITÉS DE TRAITEMENT

12.1 Contenu des registres

Cloud Temple agit (i) en qualité de Sous-traitant pour les données à caractère personnel traitées pour le compte du Client dans le cadre des Services (« Données Client »), et (ii) en qualité de Responsable de traitement pour les données traitées pour ses propres finalités (« Données de Service »), notamment la gestion de la relation client, la gestion des accès techniques et la journalisation, ainsi que la conformité et la sécurité.

Ainsi, Cloud Temple collecte des données et maintient deux registres électroniques des activités de traitement selon les cas suivants :

Données Client :

- ☐ les coordonnées de la société cliente et du délégué à la protection des données (nom, prénom, téléphone, mail) ;
- ☐ les catégories de traitement effectuées pour le compte de ce client ;
- ☐ les transferts hors Union européenne, le cas échéant ;
- ☐ les mesures techniques et organisationnelles de sécurité mises en œuvre.

Données de Service :

- ☐ gestion de la relation client (CRM, contrats, annuaire, demandes d'achat, communication) ;
- ☐ gestion des accès techniques (comptes utilisateurs, accès console, journalisation des logs) ;
- ☐ gestion opérationnelle (incidents, alertes, notifications, reporting) ;
- ☐ gestion de la conformité et de la sécurité (registre RGPD, audits).

12.2 Gestion automatisée

Les registres sont automatiquement mis à jour lors de l'établissement de nouveaux contrats clients, des modifications de services existants et des évolutions des mesures de sécurité.

12.3 Accès aux registres

Sur demande écrite, le Responsable de traitement ou le Client peut accéder uniquement aux informations le concernant dans les registres de traitement ; les autorités compétentes (CNIL, ANSSI, etc.) peuvent accéder aux registres complets dans le cadre de leurs missions de contrôle. Le Sous-traitant et/ou Cloud Temple dispose d'un délai de 15 jours ouvrés pour communiquer les informations demandées à compter de la réception de la demande. Un processus de validation des demandes légitimes est mis en place pour assurer la confidentialité des informations sensibles.

ARTICLE 13 : LES SOUS-TRAITANTS ULTÉRIEURS

Le Sous-traitant peut recourir à un ou plusieurs prestataires externes pour la prise en charge de prestations spécifiques relevant du Contrat, sous sa responsabilité, aux seules fins de fournir une partie des prestations nécessaires.

Le Sous-traitant s'engage à conclure un acte juridique contraignant avec tout sous-traitant ultérieur, afin de lui imposer le respect des exigences du RGPD et les mêmes obligations que celles prévues par le présent DPA, notamment à l'Article 4 (Obligations du Sous-traitant). Il s'assure que le sous-traitant ultérieur présente des garanties suffisantes, notamment dans le cadre des données de santé.

En cas de défaillance du sous-traitant ultérieur, le Sous-traitant demeure pleinement responsable à l'égard du Responsable de traitement, sans préjudice des droits des personnes concernées prévus aux articles 79 et 82 du RGPD.

La liste des sous-traitants ultérieurs autorisés est la suivante :

Sous-traitant	Activité	Localisation	Date d'autorisation
Digital Realty	Hébergement datacenter	France/UE	15/01/2025
Data4	Hébergement datacenter	France/UE	15/01/2025
Telehouse	Hébergement datacenter	France/UE	15/01/2025
Iron Mountain	Externalisation sur bande	France/UE	15/01/2025

À ces sous-traitants s'ajoutent ceux du Contrat. Il est précisé qu'Iron Mountain n'est pas certifié HDS.

En cours d'exécution du Contrat, le Responsable de traitement peut accéder à tout moment à l'actualisation de cette liste. Le Sous-traitant notifie par écrit toute modification de sous-traitant ultérieur au minimum 30 jours calendaires avant sa mise en œuvre. Pour tout nouveau sous-traitant critique, une autorisation préalable spécifique du Responsable de traitement est requise.

ARTICLE 14 : RESPONSABILITÉ

Le Responsable de traitement et le Sous-traitant reconnaissent qu'ils peuvent être tenus responsables des dommages causés par un traitement non conforme au RGPD et aux lois françaises applicables. Le Sous-traitant est responsable des dommages causés par le traitement s'il n'a pas respecté les obligations du RGPD spécifiquement applicables aux sous-traitants, ou s'il a agi en dehors des instructions légales du Responsable de traitement ou contrairement à celles-ci.

ARTICLE 15 : MODIFICATIONS

Toute modification du présent DPA doit faire l'objet d'un avenant écrit signé par les deux Parties. Les modifications doivent être conformes aux exigences du RGPD et des lois françaises relatives à la protection des données personnelles.

ARTICLE 16 : LOI APPLICABLE ET JURIDICTION COMPÉTENTE

Le présent DPA est régi par le droit français. Tout litige relatif à son interprétation ou à son exécution relève de la compétence exclusive des tribunaux français. En cas de divergence entre les versions linguistiques, la version française prévaut.