

## Annexe n° 3 – Hébergement de Données Personnelles de Santé (HDS)

### 1- DEFINITIONS

**Données personnelles de santé** : Désigne les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique qui révèlent les informations sur l'état de santé de cette personne, indépendamment de leur source.

**Hébergement** : Désigne la prestation de stockage au profit du Client de ses Ressources comprenant des Données personnelles de santé.

**Certification HDS** : Désigne la certification définie et encadrée par l'article L. 1111-8 du Code de la santé publique et ses textes d'application ; le Service d'Hébergement bénéficie d'une Certification HDS en tant que Service d'Hébergement de données de santé à caractère personnel.

**Personne Concernée** : Désigne une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, ou à un ou plusieurs éléments spécifiques propres à son identité et dont les données de santé à caractère personnel sont hébergées par Bouygues Telecom Business Solution

**Violation de données à caractère personnel** : Désigne 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 traitées d'une autre manière, ou l'accès non autorisé à de telles données.

**Données temporaires** : Désigne les données générées pendant l'exécution d'une tâche (exemples : fichier de rollback, fichier de mise à jour d'une base de données, etc.), inutiles une fois la tâche terminée.

**Ressources** : Applications de santé appartenant au Client qu'elles soient développées par ce dernier ou par un fournisseur tiers d'application de données de santé.

**Utilisateur final** : concerne toute personne (patient, établissement de santé, personnels de santé ou fournisseurs) dont les données de santé sont collectées et hébergées sur les infrastructures d'Bouygues Telecom Business Solution par le biais des Ressources du Client.

## Annexe n° 3 – Hébergement de Données Personnelles de Santé (HDS)

### **2- CERTIFICATION**

En application de l'article L. 1111-8 du Code de la Santé Publique, Bouygues Telecom Business Solution déclare bénéficiaire de la certification HDS n°39678-0 émise le 12 Février 2024 par LNE, sur le périmètre suivant : Hébergeur infogéreur.

La Certification est valable trois (3) ans, soit jusqu'au 11 Février 2027, renouvelable tous les trois (3) ans.

Elle concerne les activités suivantes, fournies par Bouygues Telecom Business Solution au titre du Contrat :

*2) Mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.*

*4) Mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information de santé*

*6) Sauvegardes externalisées des données de santé.*

La Certification est mise à disposition du Client à tout moment.

Sur demande du Client, Bouygues Telecom Business Solution mettra à disposition du Client les rapports d'audit de certification pour une consultation sur site chez Bouygues Telecom Business Solution uniquement.

### **3- CONTINUITÉ ET REPRISE D'ACTIVITÉ**

Afin d'assurer la disponibilité des Ressources et des Données personnelles de santé, conformément aux engagements définis dans le présent document, Bouygues Telecom Business Solution met en œuvre une démarche de continuité et de reprise d'activité telle que définie dans la PSI disponible sur demande du Client.

En cas de restauration des Données personnelles de santé, Bouygues Telecom Business Solution s'engage à restaurer l'ensemble desdites données et fichiers suivant la Politique de sauvegarde. Les données et fichiers seront restaurés en l'état de leur plus récente sauvegarde.

### **4- SERVICE LEGAL AGREEMENT (SLA)**

## Annexe n° 3 – Hébergement de Données Personnelles de Santé (HDS)

Bouygues Telecom Business Solution garanti un taux de disponibilité mensuelle de 99,95 % de la plateforme virtuelle. Le pourcentage de disponibilité est communiqué au Client par machines virtuelles.

Le Taux de disponibilité est calculé ainsi :

*Minutes mensuelles disponibles maximum – minutes mensuelles d'indisponibilité*

\_\_\_\_\_ X 100

*Minutes mensuelles disponibles maximum*

Le taux d'indisponibilité correspond au nombre total de minutes mensuelles où le service n'est plus disponible étant entendu qu'une minute est considérée comme indisponible si l'une des conditions ci-dessous est remplie :

- Perte de connectivité du cluster pendant 4 minutes consécutives
- Perte d'accès au stockage des VM du cluster pendant 4 minutes consécutives
- Perte du vCenter qui impacte le fonctionnement des services pendant 4 minutes consécutives
- Perte du NSX Manager qui impacte le fonctionnement des services pendant 4 minutes consécutives

Seront exclus du calcul du taux de disponibilité les interruptions résultant des causes ci-dessous :

- les interruptions de services en cas de maintenance réalisées par Bouygues Telecom Business Solution ;
- d'une modification de la Prestation demandée par le Client ;
- d'un cas de force majeure ;
- du fait d'un tiers ;
- du fait du Client et en particulier du non-respect des spécifications techniques fournies par Bouygues Telecom Business Solution pour la mise en œuvre du service ;
- d'un élément non installé et/ou exploité par Bouygues Telecom Business Solution ;
- les perturbations ou interruptions des moyens de télécommunication fournis par le ou les exploitants des réseaux auxquels sont raccordées les installations du Client,
- de modifications dues à des prescriptions de toutes autorités.

Aucun engagement de disponibilité n'est consenti par Bouygues Telecom Business Solution en cas de dysfonctionnement des Ressources, notamment des Ressources propriétés du Client, ou de toutes applications tierces c'est-à-dire dont Bouygues Telecom Business Solution n'est pas l'éditeur. Dans le cas où une application tierce est incluse dans le périmètre d'intervention d'Bouygues Telecom Business Solution tel que délimité à la documentation Bouygues Telecom Business Solution du Service, l'intervention de Bouygues Telecom Business Solution se limite à l'application de patchs correctifs mis à disposition du Client par

## Annexe n° 3 –

### Hébergement de Données Personnelles de Santé (HDS)

l'éditeur et que Bouygues Telecom Business Solution mettrait en œuvre pour le compte du Client. De convention expresse, Bouygues Telecom Business Solution n'est pas tenue d'intervenir d'une autre manière en cas d'incident affectant toutes Ressources et les pénalités prévues aux présentes en cas d'Interruptions ou d'indisponibilités causées par les applications tierces ne sont pas applicables.

En cas de manquement à ses engagements, le Client pourra prétendre à une indemnité libératoire définie dans l'Annexe n° 2 -Engagements de niveau de Services.

#### **5- LOCALISATION DES DONNEES PERSONNELLES DE SANTE**

Les Données personnelles de santé sont stockées en France sur les sites listés ci-dessous :

- PA 3 / 114 rue Ambroise Croizat, Saint-Denis, France, 93200
- PA 4 / 110 Bis avenue du Général Leclerc, Pantin, France, 93500

#### **6- OBLIGATION DE BOUYGUES TELECOM BUSINESS SOLUTION**

##### **6.1- Sécurité**

Bouygues Telecom Business Solution assure la sécurité nécessaire à la réalisation des Services selon la PSI adressée au Client sur première demande.

Bouygues Telecom Business Solution mettra en œuvre, maintiendra, et fera en sorte que chacun de ses Sous-traitants impliqués dans les Services mette en œuvre et maintienne, des politiques et procédures de gestion des incidents de sécurité et de continuité des activités conformes à la PSI et, en tout état de cause, aux standards élevés de l'industrie.

Bouygues Telecom Business Solution met en place les mesures de sécurité techniques et opérationnelles nécessaires à la protection des données personnelles de santé. Ces dernières sont définies dans le Plan d'Assurance Sécurité (PAS) qui sera communiqué au Client sur demande. Bouygues Telecom Business Solution s'engage à le maintenir régulièrement à jour.

##### **6.2- Gestion des traces**

Les traces des administrateurs Bouygues Telecom Business Solution sont fournies sur demandes via une requête par e-mail à l'adresse [support@oncloud.fr](mailto:support@oncloud.fr) en précisant les services concernés et la période de temps, dans la limite d'un an.

Le Client doit s'assurer que ses Ressources permettent de mettre à disposition de la personne concernée par les Données personnelles de santé : l'historique des accès, l'historique des consultations / modifications, le contenu des informations accédées et la nature des

C o n f i d e n t i e l

Annexe 3 – Hébergement de Données Personnelles de Santé

V1.1 20250721

## Annexe n° 3 –

### Hébergement de Données Personnelles de Santé (HDS)

Traitements éventuellement opérés (lecture, écriture, modification et/ou suppression). Le Client reconnaît et accepte que cette traçabilité applicative des actions relève de sa seule responsabilité.

#### **6.3 - Surveillance et gestion des incidents**

Bouygues Telecom Business Solution assure une surveillance constante pour relever tout incident et/ou défaillance et, en cas de survenance, s'engage à mettre en œuvre les moyens nécessaires pour y remédier dans les meilleurs délais.

En l'occurrence, Bouygues Telecom Business Solution notifiera au Client toute attaque et/ou intrusion qu'elle constaterait, fera ses meilleurs efforts afin de les faire cesser ou d'en réduire l'impact sur la disponibilité du service d'hébergement et la confidentialité des données, et transmettra au Client l'ensemble des éléments de preuve collectés permettant d'identifier son auteur. Bouygues Telecom Business Solution apportera au Client toute l'aide nécessaire pour réprimer l'attaque et/ou l'intrusion.

De manière générale, Bouygues Telecom Business Solution notifiera par ailleurs au Client tout incident, quelle qu'en soit la nature (divulgaration, altération, suppression de ses fichiers et/ou données, incident d'exploitation impactant la disponibilité) et déclenchera les mesures appropriées telles que figurant dans la PSI.

Le Client informera sans délai Bouygues Telecom Business Solution de tout incident et/ou défaillance constaté dans le cadre de la réalisation de la prestation en adressant un mail au support à l'adresse [support@oncloud.fr](mailto:support@oncloud.fr).

Le Client décrira de manière précise les détails de l'incident et/ou défaillance qu'il aura constaté et notamment, communiquera à Bouygues Telecom Business Solution tous les éléments de nature à identifier précisément l'incident et/ou la défaillance.

Bouygues Telecom Business Solution informera le Client des moyens mis en œuvre pour régulariser l'incident et/ou la défaillance.

En tout état de cause, Bouygues Telecom Business Solution interviendra selon les modalités et dans les délais tels que figurant dans les Conditions Générales de Vente.

Le contact professionnel de santé du Client sera associé à l'ensemble du processus de gestion des incidents et ce, en sa qualité de garant de la confidentialité des Données personnelles de santé.

#### **6.4 -Audits**

- Sur les Infrastructures mutualisées.

## Annexe n° 3 –

### Hébergement de Données Personnelles de Santé (HDS)

Bouygues Telecom Business Solution commanditera régulièrement un audit indépendant pour évaluer et documenter la pertinence des mesures techniques et organisationnelles mise en œuvre dans le cadre du Service d'Hébergement, et partagera un récapitulatif des résultats de cet audit et/ou d'autres informations connexes que le Client peut raisonnablement exiger. Le Client adressera alors, une demande écrite auprès de Bouygues Telecom Business Solution pour obtenir les résultats. Il pourra aussi venir les consulter sur site moyennant un préavis de trente jours calendaires. Ces informations sont des informations confidentielles de Bouygues Telecom Business Solution.

Si Bouygues Telecom Business Solution ne commande pas de tels audits ou n'en partage pas les résultats, le Client est autorisé à vérifier la pertinence des mesures techniques et organisationnelles de Bouygues Telecom Business Solution par lui-même ou par l'intermédiaire d'un représentant autorisé du Client. Si le Client décide d'auditer Bouygues Telecom Business Solution, le Client doit fournir à Bouygues Telecom Business Solution un plan d'audit écrit (comprenant des détails techniques complets qui pourraient avoir un impact sur l'hébergement des données) pour approbation par Bouygues Telecom Business Solution, avec un préavis de trois (3) mois. Tout aspect de cet audit est une information confidentielle de Bouygues Telecom Business Solution.

Bouygues Telecom Business Solution pourra également répondre à toute question d'audit écrite qui lui sera soumise par le Client. Les réponses de Bouygues Telecom Business Solution sont des informations confidentielles de Bouygues Telecom Business Solution.

Si pour les besoins d'un audit, le Client devait désigner un prestataire, le Client devrait en aviser Bouygues Telecom Business Solution suivant les mêmes modalités que le plan d'audit, Bouygues Telecom Business Solution se réservant la faculté de refuser le prestataire désigné par le Client en cas de risque de conflit d'intérêts ou de concurrence.

– Sur les infrastructures dédiées.

A l'issue des douze (12) premiers mois suivants la date de prise d'effet du Contrat, le Client pourra réaliser ou faire réaliser, sur les infrastructures dédiées uniquement, à ses frais, dans la limite d'une fois par an, un audit afin de vérifier la conformité des prestations objet du Contrat, sous réserve du respect des conditions suivantes :

(i) Le Client devra avertir Bouygues Telecom Business Solution de son intention de réaliser un audit, par courrier recommandé avec accusé de réception, moyennant le respect d'un préavis de trente (30) jours calendaires. Le courrier adressé à Bouygues Telecom Business Solution devra indiquer l'objet, le périmètre souhaité de l'audit, et l'identité de l'auditeur qui serait retenu. Bouygues Telecom Business Solution se réserve la faculté de s'opposer au choix de l'auditeur retenu par le Client. Bouygues Telecom Business Solution adressera alors un courrier ou un mail au Client pour l'informer du refus en indiquant et justifiant les raisons de ce refus dans un délai de dix (10) jours suivant la réception de la demande d'audit.

(ii) Un protocole d'audit détaillant les conditions de réalisation de l'audit sera convenu entre les Parties avant le démarrage de l'audit ;

## Annexe n° 3 – Hébergement de Données Personnelles de Santé (HDS)

(iii) La durée de l'audit ne pourra excéder deux (2) jours ouvrés, travail préparatoire des équipes de Bouygues Telecom Business Solution inclus. Au-delà, la mobilisation des équipes de Bouygues Telecom Business Solution concernées pendant la durée de l'audit sera facturée au Client sur la base d'un devis préalablement remis par Bouygues Telecom Business Solution au Client ;

(iv) L'audit devra être réalisé pendant les jours et heures d'ouverture de Bouygues Telecom Business Solution et ne pas perturber le déroulement de son activité. Bouygues Telecom Business Solution ne pourra pas s'opposer à l'audit (sauf contraintes légales ou réglementaires spécifiques s'imposant à Bouygues Telecom Business Solution) mais pourra demander à ce qu'il soit repoussé ;

(v) L'audit sera soumis aux politiques de protection et de sécurité en vigueur au sein de Bouygues Telecom Business Solution ainsi qu'à toute autre mesure nécessaire pour assurer la confidentialité des données de Bouygues Telecom Business Solution et/ou de ses clients ;

(vi) Lorsque l'auditeur est un tiers extérieur, le Client se porte fort de la signature d'un accord de confidentialité par l'auditeur. De plus, le Client s'engage également à ce que les personnes désignées se conforment aux politiques et mesures de sécurité applicables chez Bouygues Telecom Business Solution ;

(vii) Le rapport d'audit ne pourra pas être communiqué à des tiers sans l'accord préalable de Bouygues Telecom Business Solution ;

Bouygues Telecom Business Solution s'engage à collaborer de bonne foi avec l'auditeur, et à lui prêter assistance. Il facilitera l'accès de l'auditeur à tout document ou information lui permettant de vérifier la conformité des prestations de Bouygues Telecom Business Solution et répondra à toute question portant sur le périmètre de l'audit. L'auditeur ne pourra toutefois pas avoir accès aux informations pouvant porter atteinte au savoir-faire ou au secret des affaires de Bouygues Telecom Business Solution, à celles relatives aux autres clients de Bouygues Telecom Business Solution, aux droits des tiers et de façon générale aux informations soumises à une obligation de confidentialité.

L'auditeur ne pourra transmettre au Client que les informations nécessaires à ce dernier pour juger du respect par Bouygues Telecom Business Solution des dispositions spécifiques du Contrat qui auront fait l'objet de l'audit.

A l'issue de l'audit, un exemplaire du rapport d'audit sera remis à Bouygues Telecom Business Solution gratuitement afin qu'il puisse formuler ses observations. Ce rapport pourra ensuite être examiné conjointement par les Parties dans le cadre d'un comité ad hoc.

Dans le cas où le rapport d'audit ferait apparaître un manquement non contesté par Bouygues Telecom Business Solution à ses obligations contractuelles, Bouygues Telecom Business Solution prendra les mesures correctives nécessaires dans le délai raisonnable convenu entre les Parties, dans le comité susvisé.

## Annexe n° 3 –

### Hébergement de Données Personnelles de Santé (HDS)

#### **6.5- Mise à disposition du personnel compétent pour réaliser la prestation d'hébergement**

Bouygues Telecom Business Solution confirme disposer d'un personnel composé de professionnels qualifiés pour assurer la prestation d'hébergement, lesquels sont notamment astreints au secret professionnel.

#### **6.6- Limitations**

Dans le cadre exclusif du Service d'Hébergement fourni par Bouygues Telecom Business Solution, Bouygues Telecom Business Solution s'engage à n'utiliser les Données du Client que dans la limite de l'exécution du Service d'Hébergement et conformément aux instructions du Client.

Dans le cadre exclusif du Service d'Hébergement, Bouygues Telecom Business Solution s'engage et garantit que les Données du Client ne seront pas utilisées à d'autres fins que celles spécifiées par le Client, et notamment à des fins marketing, publicitaires, commerciales ou statistiques. Dans le cas où cela s'avérerait nécessaire, par exemple dans le cadre du support, Bouygues Telecom Business Solution contactera l'interlocuteur professionnel de santé désigné par le Client, afin qu'il accède seul aux Données Personnelles de Santé concernées.

En tout état de cause, il est rappelé au Client qu'il lui appartient de veiller à ce que les Utilisateurs de la Plateforme ne fassent apparaître aucune Donnée Personnelle et, en particulier, Donnée personnelle de santé, lorsqu'ils sollicitent l'intervention du support de Bouygues Telecom Business Solution.

#### **6.7- Sous-traitance**

Les Données Personnelles de Santé sont hébergées auprès du prestataire d'hébergement EQUINIX. EQUINIX dispose de la certification HDS n°FR072821 délivrée par BUREAU VERITAS le 08 mars 2023, et couvrant le périmètre « hébergeur d'infrastructure physique » suivant :

- 1. La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé.*
- 2. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.*

Bouygues Telecom Business Solution s'assure en tout temps du maintien de la certification de la société EQUINIX et des mesures de sécurité suffisantes conformes à la certification et à la réglementation applicable. L'ensemble des obligations prises par Bouygues Telecom Business Solution au titre du Contrat sont reportées dans les conditions contractuelles conclues avec

## Annexe n° 3 –

### Hébergement de Données Personnelles de Santé (HDS)

cet hébergeur. En tout état de cause, Bouygues Telecom Business Solution demeure responsable envers le Client de ce sous-traitant ultérieur.

Le Client autorise Bouygues Telecom Business Solution à faire appel à des sous-traitants, sous sa pleine et entière responsabilité, sous réserve d'en notifier préalablement le Client et de conclure un accord écrit avec les sous-traitants dont les garanties ne pourront être en deçà de celles conclues avec le Client. Bouygues Telecom Business Solution dispose d'une liste des sous-traitants pouvant être communiquée aux clients suite à leur demande.

#### **7- OBLIGATIONS DU CLIENT**

##### ***7.1- Respect de la législation concernant les Données Personnelles de Santé hébergées***

Le Client garantit la légalité du traitement des Données Personnelles de Santé objets de l'hébergement. En particulier, le Client garantit Bouygues Telecom Business Solution qu'il a informé les personnes concernées de ce que leurs Données Personnelles de Santé seront stockées sur les serveurs de la société EQUINIX et, le cas échéant, a recueilli leur consentement à cet effet. Le Client garantit qu'il respecte en tout temps les droits des personnes concernées sur leurs Données Personnelles de Santé et, plus généralement, la réglementation applicable en cette matière.

Le Client garantit Bouygues Telecom Business Solution contre toute réclamation qui pourrait être engagée par une personne concernée par le stockage de ses Données Personnelles de Santé, ainsi que par tout tiers ou toute autorité compétente, à l'encontre de Bouygues Telecom Business Solution et qui résulterait, directement ou non, du non-respect par le Client, salariés et/ou sous-traitants des obligations légales et réglementaires relatives à l'activité du Client et aux traitements de Données Personnelles de Santé opérés dans ce cadre.

Le Client demeure responsable du signalement aux Autorités et Utilisateurs finaux de tout incidents de sécurité impactant les Ressources du Client ayant entraîné l'altération, la destruction ou la divulgation non autorisée de données de santé

##### ***7.2 - Contact Client***

Le Client s'engage à désigner dès la signature du Contrat un interlocuteur unique disposant des compétences nécessaires et dûment habilité à agir au nom du Client pour toute décision relative aux Données Personnelles de Santé, objet du Contrat (accès aux données, gestion des incidents, etc.).

Il est de la seule responsabilité du Client de s'assurer que le contact qu'il a désigné dispose des qualités et habilitations nécessaires et à jour pour accéder aux Données Personnelles de Santé. Le Client s'engage à informer immédiatement Bouygues Telecom Business Solution en cas de changement d'interlocuteur. En aucun cas la responsabilité de Bouygues Telecom

## Annexe n° 3 – Hébergement de Données Personnelles de Santé (HDS)

Business Solution ne pourra être engagée du fait d'un manquement du Client à cette obligation essentielle du Contrat, Bouygues Telecom Business Solution n'opérant aucune vérification des habilitations et qualité du contact client.

Le point de contact du Client référencé aux fins d'exécution du Contrat doit être renseigné au moment de la souscription au Contrat et maintenu à jour par le Client.

### ***7.3- Obligations en matière d'accès aux Données Personnelles de Santé***

Tout accès aux Données Personnelles de Santé nécessaire pour répondre à une requête d'une personne concernée ou de tout tiers autorisé, devra se faire par l'intermédiaire du contact Client professionnel de santé, étant entendu que le Client, Responsable de traitement, demeure en tout état de cause, responsable de l'exercice des droits des personnes sur les Données Personnelles de Santé les concernant.

Plus généralement, le Client prendra soin de conserver les informations qui lui seront le cas échéant communiquées par Bouygues Telecom Business Solution concernant ses modalités d'authentification et de contrôle d'accès à la Plateforme, à l'aide de moyens sécurisés conformes à la PGSSI-S.

Le Client informera Bouygues Telecom Business Solution dans les meilleurs délais en cas de perte ou de vol des éléments d'authentification et plus généralement, en cas de dysfonctionnement constaté concernant l'accès aux Données Personnelles de Santé.

La mise à disposition des Données Personnelles de Santé se faisant par le biais des Ressources du Client, il incombe au Client de mettre en œuvre les moyens de traçabilité d'accès aux données de santé, de sauvegardes des traces ainsi que des accès aux traces d'accès pour les Utilisateurs Finaux aux données de santé hébergées.

De même, le Client est informé que pour les Ressources permettant un accès aux Utilisateurs finaux aux Données Personnelles de Santé hébergées, il lui incombe de mettre en place une procédure d'authentification forte qui ne peut se limiter à une authentification de type « identifiant + mot de passe ».

### ***7.4- Confidentialité des Données Personnelles de Santé.***

Outre l'obligation de confidentialité à laquelle il s'astreint, le Client s'engage à faire respecter par ses salariés, préposés, sous-traitants, et plus généralement toute personne assurant une mission liée à la présente prestation d'hébergement, la confidentialité des Données Personnelles de Santé dès lors que l'accès aux dites données repose sur un fondement juridique valide.

Le Client garantit Bouygues Telecom Business Solution contre toute réclamation qui pourrait être engagée par la personne concernée par des Données hébergées, ainsi que par tout tiers ou toute Autorité compétente, à l'encontre de Bouygues Telecom Business Solution et qui

## Annexe n° 3 – Hébergement de Données Personnelles de Santé (HDS)

résulterait, directement ou non, du non-respect par le Client, ses préposés, salariés et/ou sous-traitants des obligations relatives à la confidentialité des Données Personnelles de Santé.

### **7.5- Archivage des Données Personnelles de Santé**

Le Client garantit que les Ressources permettent de sauvegarder et archiver les Données Personnelles de Santé de manière à garantir leur conservation dans le temps, leur intégrité et leur confidentialité, pendant les délais légaux applicables.

### **7.6- Adhésion et Respect de la PGSSI -S**

Conformément aux exigences du référentiel Hébergement de Données de Santé, le Client s'engage à respecter l'ensemble des règles édictées par la norme PGSSI-S, dans sa version la plus à jour, dès lorsqu'il traite des Données Personnelles de Santé au travers des Ressources hébergées sur la Plateforme. A ce titre, le Client s'engage à maintenir un niveau de sécurité des Ressources et, plus généralement, de son système d'information, au moins aussi strictes que celles édictées par la norme précitée.

Le Client garantit avoir pris connaissance et respecter les dispositions du corpus documentaire constituant la PGSSI-S disponible sur le site de L'Agence du Numérique en Santé ([esante.gouv.fr](http://esante.gouv.fr)).

## **8- DROITS DES PERSONNES CONCERNEES**

### **8.1- Exercice des droits des Personnes Concernées**

Le Client s'engage à garantir le respect des droits des Personnes Concernées par les données hébergées, et notamment à :

- Les informer du recours à un hébergeur de données de santé certifié ;
- Les informer qu'elles disposent à cet effet d'un droit d'opposition à cet hébergement, sous réserve d'invoquer un motif légitime, conformément aux dispositions de l'article L. 1111-8 du Code de la santé publique ;
- Les informer qu'elles disposent :
  - D'un droit d'accès ;
  - D'un droit d'opposition ;
  - D'un droit de rectification ;
  - D'un droit de limitation du traitement ;
  - D'un droit à l'effacement ;
  - D'un droit à la portabilité ;
  - D'un droit d'introduire une réclamation auprès de la CNIL ;
  - D'un droit de communiquer ses directives concernant le sort de ses données à caractère personnel après sa mort.

Bouygues Telecom Business Solution s'engage, dans toute la mesure du possible, à aider le Client dans la gestion d'une demande d'exercice de droits d'une Personne Concernée.

C o n f i d e n t i e l

Annexe 3 – Hébergement de Données Personnelles de Santé

V1.1 20250721

## Annexe n° 3 –

### Hébergement de Données Personnelles de Santé (HDS)

Lorsqu'une Personne Concernée exerce ses droits directement auprès de Bouygues Telecom Business Solution à l'adresse suivante : [dpo@bouyguetelecom-solution.fr](mailto:dpo@bouyguetelecom-solution.fr) - Bouygues Telecom Business Solution - 1 le Parvis de la Défense – Paroi Nord de la Grande Arche - 92800 PUTEAUX, Bouygues Telecom Business Solution s'engage, dès réception de cette demande, à l'adresser au Client par e-mail (à l'exclusion de toute communication de Données de Santé à Caractère Personnel). Bouygues Telecom Business Solution ne répondra pas directement à une demande d'exercice de droit en lien avec le Service d'Hébergement de Données de Santé à Caractère Personnel.

#### **8.2- Information des Personnes Concernées**

Le Client s'engage, en tant que responsable de traitement au sens de la Réglementation, à mettre en œuvre un dispositif écrit d'information et de recueil du consentement adapté et conforme à la Réglementation en vue de garantir l'information complète des Personnes Concernées. Le Client s'engage à ce que ce dispositif d'information décrive de manière intelligible et adaptée le Service d'Hébergement des Données de Santé à Caractère Personnel des Personnes Concernées, ainsi que les modalités d'accès et de transmission de ces dernières. Le Client s'engage en outre à informer les Personnes Concernées de l'ensemble des évolutions susceptibles d'intervenir sur le Service d'Hébergement chaque fois que Bouygues Telecom Business Solution l'en informe.

#### **9- VIOLATION DES DONNEES A CARACTERE PERSONNEL DE SANTE**

Bouygues Telecom Business Solution s'engage à informer le Client dans les meilleurs délais dès qu'il aura connaissance d'une Violation de Données à Caractère Personnel affectant les Données Personnelles de Santé des clients par Bouygues Telecom Business Solution dans le cadre du Service d'Hébergement.

Bouygues Telecom Business Solution s'engage à fournir au Client les informations suffisantes lui permettant de répondre à toute obligation de signalement ou d'information des Personnes Concernées.

Bouygues Telecom Business Solution s'engage à coopérer avec le Client et à prendre toutes les mesures commerciales raisonnables qui lui seront demandées par le Client pour l'aider à enquêter, atténuer et remédier à chacune des Violations de Données à Caractère Personnel portant sur les données de santé hébergées.

#### **10- EVOLUTION DU SERVICE D'HEBERGEMENT DE DONNEES**

Bouygues Telecom Business Solution a la possibilité de modifier le Service d'Hébergement, ses outils ou les infrastructures nécessaires à la réalisation du Service d'Hébergement, à condition de garantir une qualité de Service d'Hébergement et un Niveau de Service au moins équivalents. En tout état de cause, les éventuelles modifications opérées par Bouygues Telecom Business Solution au Service d'Hébergement fourni, en termes de techniques,

## Annexe n° 3 –

### Hébergement de Données Personnelles de Santé (HDS)

méthodes de travail, outils, savoir-faire et/ou procédés de mise en œuvre ne devront pas être de nature à compromettre la bonne et complète exécution du Service d'Hébergement, ni le niveau de sécurité convenu. Dans tous les cas, Bouygues Telecom Business Solution s'engage à informer le Client dans les meilleurs délais de toute modification impactant le Service d'Hébergement, qu'il s'agisse de modifications techniques, de méthodes de travail, d'outils, de savoir-faire et/ou de procédés de mise en œuvre.

#### **11- COMMUNICATION DES DONNEES**

##### **11.1- Saisie des données**

En cas de saisies judiciaires portant sur des Données de Santé à Caractère Personnel, Bouygues Telecom Business Solution s'engage à respecter la procédure de saisies des données de Bouygues Telecom Business Solution (cf. BTEO - Procédure de Transmission Violation des données de santé -v0.1 -20230425). Bouygues Telecom Business Solution s'engage à répondre aux questions de son Client à propos de la procédure des saisies judiciaires de Bouygues Telecom Business Solution. Le Client est invité à transmettre ces questions à l'adresse suivante : [dpo@bouyguetelecom-solution.fr](mailto:dpo@bouyguetelecom-solution.fr) - Bouygues Telecom Business Solution – Paroi Nord de la Grande Arche -1 Parvis de la Défense \_92044 Paris La Défense Cedex. Le Client reconnaît avoir pris connaissance de la politique de saisie des données et déclare l'accepter sans réserve. La politique prévoit notamment les modalités de notification d'une telle saisie au Client, à moins que cette notification soit interdite par le droit applicable.

##### **11.2- Communications aux autorités compétentes.**

En cas de demandes émanant des autorités compétentes, Bouygues Telecom Business Solution devra communiquer les éléments souhaités sans pouvoir voier sa responsabilité engagée.

Dans cette hypothèse, Bouygues Telecom Business Solution informera le Client de cette exigence légale dans la limite de ce qui est permis par les lois en vigueur, avant de répondre à la demande d'exercice de droit.

##### **11.3- Données temporaires**

Bouygues Telecom Business Solution définira en concertation avec le Client une période de rétention des Données temporaires et respectera ce délai. Bouygues Telecom Business Solution s'engage à documenter et mettre en place les moyens permettant de s'assurer que les données temporaires sont effacées à expiration de ce délai.

## Annexe n° 3 –

### Hébergement de Données Personnelles de Santé (HDS)

#### 12- REGIONALISATION

Bouygues Telecom Business Solution assurera au Client des interfaces et un support de premier niveau en langue française.

#### 13- REVERSIBILITE

##### **13.1- Réversibilité suite à la résiliation par un des Parties ou échéance du Contrat.**

Au terme du présent Contrat, quelle qu'en soit la cause, Bouygues Telecom Business Solution assurera une réversibilité des Services et restituera la totalité des Données Personnelles de Santé du Client conformément au présent article.

La réversibilité consiste à permettre au Client de récupérer toutes les Données hébergées sur la Plateforme. Pour ce faire, Bouygues Telecom Business Solution met à la disposition du Client ou des tiers compétents désignés par lui des API ouvertes, ainsi que la documentation associée, qui lui permettent d'assurer la récupération et le transfert de ses Données.

En cas de résiliation du Contrat, pour quelque raison que ce soit, y compris à la l'initiative de Bouygues Telecom Business Solution, Bouygues Telecom Business Solution garantira l'accès aux sauvegardes des Données pendant quinze (15) jours à compter de la date de fin du Contrat, permettant au Client de récupérer l'ensemble de ses Données.

À l'issue de ce délai, le Client transmettra à Bouygues Telecom Business Solution un procès-verbal signé de « Récupération des Données terminée ». À compter de la réception de ce dernier, Bouygues Telecom Business Solution mettra fin à l'accès nécessaire à la récupération des Données, effacera toutes les Données du Client et n'en conservera aucune trace. Toutes les Données du Client sont effacées définitivement au plus tard quinze (15) jours après la fin du Contrat. Il s'agit du délai de conservation de la sauvegarde.

Si à l'issue de ce délai, le Client n'a pas adressé de procès-verbal signé de « Récupération des Données terminée » ou de demande de suppression du Compte auprès du support de Bouygues Telecom Business Solution, et après mise en demeure par lettre recommandée avec avis de réception au Client, d'émettre le procès-verbal signé de « Récupération des données terminée», restée infructueuse pendant les quinze (15) jours ouvrés suivant sa réception, Bouygues Telecom Business Solution pourra facturer l'immobilisation des espaces de stockage sur lesquels les Données sont encore présentes pendant 11 (onze) mois maximum. Au-delà de ce délai, Bouygues Telecom Business Solution se réserve le droit de supprimer les Données dont il est question, ce que le Client reconnaît et accepte.

##### **13-2 Réversibilité suite à la perte de la certification par Bouygues Telecom Business Solution.**

Bouygues Telecom Business Solution informera immédiatement le Client en cas de perte de la Certification, entraînant la résiliation automatique du Contrat. Conformément à la

### Annexe n° 3 – Hébergement de Données Personnelles de Santé (HDS)

réglementation applicable, Bouygues Telecom Business Solution supprimera les Données Personnelles de Santé, et détruira toutes copies et sauvegardes qu'elle pourrait avoir sur ses serveurs, sur autorisation expresse du Client. Bouygues Telecom Business Solution délivrera une attestation de destructions des Données Personnelles de Santé à la demande du Client.

Cette autorisation devra être donnée dans les vingt-quatre (24) heures suivant la notification de la perte de la Certification. Au-delà, la responsabilité de Bouygues Telecom Business Solution ne pourra plus être engagée du fait du non-respect, par le Client, de ses obligations légales au titre de l'hébergement des Données Personnelles de Santé.

#### **13-3 Demande spécifique de rétention des Données Personnelles de Santé.**

Hors le cas d'une résiliation du Contrat pour perte de la Certification, il est entendu entre les Parties que toute demande de rétention des Données Personnelles de Santé au-delà du terme du présent Contrat, devra être communiquée à Bouygues Telecom Business Solution au moment de la souscription du Contrat et fera l'objet d'un devis spécifique.

**DATE :**

**SOCIETE :**

**Nom :**

**Cachet et signature \***

\* Faire précéder la signature de la mention « lu et approuvé »

Merci de parapher chacune des pages précédentes de ce document

### Annexe n° 3 –

## Hébergement de Données Personnelles de Santé (HDS)

### Appendice I- Listes des acteurs intervenants dans le cadre de l'hébergement de données personnelles de santé.

Raison sociale de l'acteur	Rôle dans le cadre de la prestation d'hébergement (Hébergeur/sous-traitant de l'Hébergeur)	Certifié HDS (oui/non/exempté)	Qualifié SecNu mCloud 3.2	Activités d'hébergement sur laquelle l'acteur intervient	Accès aux données de santé à caractère personnel depuis des pays tiers à l'Espace Economique Européen, par l'Hébergeur ou l'un de ses sous-traitants (exigence n° 29 du référentiel HDS)	Hébergeur ou sous-traitant soumis à un risque d'accès aux données de santé à caractère personnel depuis des pays tiers à l'Espace Economique Européen, imposé par la législation d'un pays tiers en violation du droit de l'Union (exigence n° 30 du référentiel HDS)
BOYGUES TELECOM BUSINESS SOLUTION  Paroi Nord de la Grande Arche 1 Parvis de la Défense	<input checked="" type="checkbox"/> Hébergeur  <input type="checkbox"/> Sous traitant	<input checked="" type="checkbox"/> Oui <input type="checkbox"/> Non <input type="checkbox"/> Exempté	<input type="checkbox"/> Oui, aucun risque d'accès non autorisé aux données visé par l'exigence n°30 du	2) Mise à disposition et maintien en condition opérationnelle de l'infrastructure	<input type="checkbox"/> Oui  <input checked="" type="checkbox"/> Non, aucun accès aux données depuis un pays tiers à l'Espace Economique Européen	<input type="checkbox"/> Oui  <input checked="" type="checkbox"/> Non :

### Annexe n° 3 – Hébergement de Données Personnelles de Santé (HDS)

<p>92044 PARIS LA DEFENSE CEDEX</p>			<p>référentiel HDS</p> <p><input checked="" type="checkbox"/> Non</p>	<p><i>matérielle du système d'information utilisé pour le traitement de données de santé.</i></p> <p><i>4) Mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information de santé</i></p> <p><i>6) Sauvegardes externalisées des données de santé.</i></p>		
<p>EQUINIX France SAS</p> <p>35 Rue de la Fédération 75015 PARIS</p> <p>Datacenter :</p> <p>PA3 114 rue Ambroise Croizat 93200 SAINT DENIS, France</p> <p>Datacenter :</p>	<p><input type="checkbox"/> Hébergeur</p> <p><input checked="" type="checkbox"/> Sous traitant</p>	<p><input checked="" type="checkbox"/> Oui</p> <p><input type="checkbox"/> Non</p> <p><input type="checkbox"/> Exempté</p>	<p><input type="checkbox"/> Oui, aucun risque d'accès non autorisé aux données visé par l'exigence n°30 du référentiel HDS</p> <p><input checked="" type="checkbox"/> Non</p>	<p><i>1. La mise à disposition et le maintien en condition opérationnel le des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé.</i></p> <p><i>2. La mise à disposition et le</i></p>	<p><input type="checkbox"/> Oui</p> <p><input checked="" type="checkbox"/> Non, aucun accès aux données depuis un pays tiers à l'Espace Economique Européen</p>	<p><input type="checkbox"/> Oui</p> <p><input checked="" type="checkbox"/> Non :</p>

**Annexe n° 3 –  
Hébergement de Données Personnelles de Santé (HDS)**

PA4 110 bis avenue Général Leclerc 93500 PANTIN France				<i>maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé.</i>		
Xpertcall  18 rue de l'artisanat - ZI Charguia 2/ 2035 TUNIS CARTHAGE - Tunisie	<input type="checkbox"/> Hébergeur  <input checked="" type="checkbox"/> Sous traitant	<input type="checkbox"/> Oui  <input checked="" type="checkbox"/> Non  <input type="checkbox"/> Exempté	<input type="checkbox"/> Oui, aucun risque d'accès non autorisé aux données visé par l'exigence n°30 du référentiel HDS  <input checked="" type="checkbox"/> Non	Gestion du support service client	<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non, aucun accès aux données depuis un pays tiers à l'Espace Economique Européen	<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non