Documents légaux

Généré le 4 novembre 2026

CGU — WakaStart v1.1

cgu · Version 1.1 · en vigueur depuis le 29 avril 2026

Applicables aux Clients et Utilisateurs accédant à la Solution SaaS développée et exploitée par JDS CONSEIL

Entrée en vigueur le 15 avril 2026\\

*

Identification du Prestataire

JDS CONSEIL — Société par Actions Simplifiée (SAS), opérant sous la marque commerciale WakaStellar pour l'ensemble de ses produits et modules de la gamme Waka (dont WakaStart, Waka HDS, WakaSign, WakaSeal, WakaInvoice).

- Capital social : 440 760 € (après réduction du 30/12/2024)
- Siège social : Parc d'Activité de Tournebride, 44118 LA CHEVROLIÈRE, France
- RCS : Nantes 529 773 368
- SIRET : 529 773 368 00012
- Code APE/NAF : 6420Z
- N° TVA intracommunautaire : FR45 529 773 368
- Présidente : Jannick SCHIRRA
- Directeur Général : Denis SCHIRRA
- Site web : www.wakastellar.com
- Contact contractuel : <contact@wakastellar.com>

Ci-après dénommée « JDS CONSEIL » ou le « Prestataire ». Le terme « WakaStellar » désigne la marque commerciale sous laquelle JDS CONSEIL opère ses produits ; il ne désigne aucune entité juridique distincte de JDS CONSEIL.

*

Article 1 – Préambule et Objet

1.1 Préambule

Les présentes Conditions Générales d'Utilisation (les « CGU ») définissent les règles d'accès et d'utilisation applicables à la Solution SaaS fournie par JDS CONSEIL au Client et aux Utilisateurs, dans le cadre du Contrat conclu entre les Parties.

Elles s'articulent avec les autres documents contractuels dans l'ordre de priorité suivant, conformément à l'Article 2 des CGV WakaStart :

- Les CGV WakaStart définissent le cadre contractuel général entre le Prestataire et le Client,
- Les présentes CGU précisent les conditions opérationnelles d'accès et d'utilisation de la Solution SaaS par les Utilisateurs,
- La Charte de Confidentialité encadre les traitements de données à caractère personnel réalisés par le Prestataire en qualité de Responsable de Traitement,
- Le DPA encadre les traitements de données à caractère personnel réalisés par le Prestataire en qualité de Sous-traitant pour le compte du Client.

1.2 Objet

Les présentes CGU :

- (i) font partie intégrante du Contrat au sens de l'Article 2 des CGV WakaStart et sont valables de façon permanente pendant toute sa durée,
- (ii) ont pour objet de définir les termes et conditions dans lesquels le Client et les Utilisateurs accèdent à la Solution SaaS et l'utilisent, dans l'objectif d'en garantir la conformité d'utilisation, la

sécurité et la disponibilité,

- (iii) s'appliquent de plein droit à tout accès et toute utilisation de la Solution SaaS par le Client ou par ses Utilisateurs, quel que soit le moyen technique d'accès (navigateur, application mobile, API, etc.).

1.3 Acceptation des CGU

Les présentes CGU sont acceptées :

- Par le Client : de façon irrévocable lors de la signature du Devis valant acceptation sans réserve des CGV et des documents annexes, conformément à l'Article 1 des CGV WakaStart.
- Par chaque Utilisateur : de façon individuelle, lors de sa première connexion à la Solution SaaS, par un mécanisme de validation explicite (case à cocher « J'accepte les CGU ») conditionnant l'accès effectif.

En cas de modification substantielle des présentes CGU, les Utilisateurs sont invités à accepter à nouveau la version mise à jour lors de leur connexion suivant l'entrée en vigueur de la nouvelle version, dans les conditions prévues à l'Article 11.

Les termes employés avec une majuscule initiale dans les présentes CGU ont la signification qui leur est donnée à l'Article 2 des CGV WakaStart, sauf définitions spécifiques introduites ci-après.

1.4 Définitions complémentaires

- « Compte Utilisateur » — Espace d'accès personnel et nominatif ouvert par le Client pour le compte d'un Utilisateur, permettant à ce dernier de se connecter à la Solution SaaS au moyen de ses Identifiants et d'accéder aux fonctionnalités selon les droits et privilèges qui lui sont attribués.
- « Contenu » — Ensemble des textes, images, vidéos, documents, paramétrages, messages et tout autre élément téléversé, saisi, créé ou diffusé par le Client ou les Utilisateurs dans la Solution SaaS. Le Contenu est compris dans les Données Client au sens de l'Article 2 des CGV.
- « Identifiants » — Moyens d'authentification personnels et confidentiels attribués à chaque Utilisateur (identifiant et mot de passe, jetons d'authentification, facteurs d'authentification multi-facteurs le cas échéant) permettant l'accès sécurisé à la Solution SaaS.
- « Manquement » — Tout non-respect par le Client ou un Utilisateur de l'une quelconque des obligations prévues aux présentes CGU ou dans les autres documents contractuels.
- « Tiers » — Toute personne physique ou morale autre que les Parties et les Utilisateurs dûment autorisés.

*

Article 2 – Finalité de la Solution SaaS

2.1 Nature de la Solution

La Solution SaaS consiste en une application logicielle développée par JDS CONSEIL pour le compte du Client, sur la base du Framework WakaStart, dont la nature fonctionnelle et le périmètre métier sont définis au Devis et formalisés dans les Spécifications validées au titre de l'Article 7.2 des CGV.

Compte tenu du caractère hautement variable des applications SaaS développées par le Prestataire, la Solution SaaS peut couvrir des usages métier très divers (outils de gestion, plateformes collaboratives, progiciels sectoriels, solutions de facturation, applications métier verticales, etc.), tels que précisés par les Spécifications propres à chaque Contrat.

2.2 Destinataires

La Solution SaaS s'adresse exclusivement à des Clients et Utilisateurs professionnels agissant dans le cadre de leur activité professionnelle ou de celle du Client.

Sauf information préalable du Prestataire et sous réserve de faisabilité technique validée lors de la Phase d'Audit & Cadrage, la Solution SaaS ne saurait tenir compte de contraintes ou spécificités

propres au Client et/ou aux Utilisateurs non prévues aux Spécifications.

2.3 Données sensibles — Interdiction par défaut

La configuration technique de la Solution SaaS est prévue pour les usages définis au Devis et aux Spécifications. En conséquence, et sauf activation expresse du périmètre HDS au sens de l'Article 3.2 des CGV, le Client et les Utilisateurs s'interdisent formellement de collecter, saisir, téléverser, traiter, stocker, sauvegarder et diffuser dans la Solution SaaS :

- Des Données de Santé au sens de l'article 4.15 du RGPD et de l'article L.1111-8 du Code de la Santé Publique,
- Des données biométriques aux fins d'identifier une personne physique de manière unique,
- Des données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale,
- Des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique,
- Des données génétiques.

En cas d'activation du périmètre HDS, les Données de Santé peuvent être traitées dans la Solution SaaS selon les modalités techniques et contractuelles spécifiques définies au Devis, à l'avenant HDS et au DPA HDS. Les autres catégories de données sensibles ci-dessus demeurent interdites, sauf adaptation contractuelle expresse.

*

Article 3 – Accès à la Solution SaaS

3.1 URL d'accès

La Solution SaaS est accessible :

- Pour la plateforme WakaStart : à l'adresse sécurisée https://app.wakastart.app/,
- Pour les applications spécifiques développées pour le Client : à une URL dédiée propre au Client, définie au Devis ou communiquée au Client par le Prestataire à l'entrée en vigueur du Contrat (de type <client>.wakastart.app ou URL personnalisée sous nom de domaine du Client, selon le périmètre convenu).

L'accès est opéré en mode SaaS, via le réseau Internet, au moyen d'une connexion sécurisée TLS/SSL (protocole https), depuis un ordinateur, une tablette ou un smartphone via navigateur ou application mobile compatible.

3.2 Prérequis techniques

Préalablement à la conclusion du Contrat et de façon permanente pendant toute sa durée, le Client s'assure qu'il est en mesure de bénéficier de la Solution SaaS, notamment que :

- (i) la souscription du Contrat et son exécution sont conformes à toutes les règles internes en vigueur au sein de son organisation, notamment en matière informatique (charte informatique, politique de sécurité, etc.),
- (ii) les Utilisateurs disposent de façon permanente d'une connexion Internet suffisante et stable (haut débit type ADSL, fibre ou équivalent), des privilèges adéquats, ainsi que d'un environnement matériel sécurisé, fiable et à jour (systèmes d'exploitation supportés, navigateurs supportés, antivirus, mises à jour de sécurité appliquées).

Le Prestataire n'assume aucune responsabilité quant à l'inadéquation des moyens techniques mis en œuvre par le Client ou les Utilisateurs, conformément à l'Article 13.3 des CGV (Exclusions SLA).

3.3 Activation des Comptes Utilisateurs

À l'entrée en vigueur du Contrat, le Prestataire procède à la création et au paramétrage du Compte Utilisateur administrateur du Client, avec les droits et privilèges les plus élevés conformément aux Spécifications.

Par la suite, le Client procède lui-même et sous sa responsabilité exclusive à la création des autres Comptes Utilisateurs, en se conformant à la procédure associée fournie par le Prestataire et aux règles définies aux Spécifications.

Chaque Utilisateur se conforme à la procédure de création et de validation de son mot de passe personnel afin d'activer son accès individuel à la Solution SaaS.

3.4 Identification et authentification

L'accès à la Solution SaaS s'effectue de façon sécurisée à partir des Identifiants propres à chaque Utilisateur.

Les Identifiants sont strictement personnels, incessibles et confidentiels. Chaque Utilisateur est tenu de prendre toutes les mesures nécessaires afin d'en maintenir la confidentialité et de prévenir tout usage par un tiers non autorisé.

Toute action accomplie via les Identifiants d'un Utilisateur est réputée accomplie par cet Utilisateur, sauf preuve contraire fondée sur une compromission notifiée au Prestataire conformément à l'Article 5.3.

3.5 Inactivité des Comptes Utilisateurs

En cohérence avec les exigences de sécurité du SMSI ISO 27001 du Prestataire, les Comptes Utilisateurs n'ayant enregistré aucune connexion pendant une durée continue de douze (12) mois pourront faire l'objet d'une désactivation automatique par le Prestataire, sans préjudice des droits du Client à les réactiver selon les procédures prévues.

Le Client est informé de cette désactivation par notification à son administrateur principal, conformément à l'Article 18 des CGV, dans un délai raisonnable permettant la reprise éventuelle de l'accès.

*

Article 4 – Gestion des Comptes Utilisateurs et des Accès

4.1 Principe de responsabilité exclusive du Client

De façon permanente pendant toute la durée du Contrat, le Client procède, sous sa responsabilité exclusive, à la gestion des accès à la Solution SaaS par les Utilisateurs, en ce compris :

- (i) La création, désactivation et suppression des Comptes Utilisateurs au moyen des fonctionnalités mises à sa disposition dans la Solution SaaS,
- (ii) L'attribution et la révocation des rôles et niveaux de privilèges de chaque Utilisateur au moyen des fonctionnalités mises à sa disposition,
- (iii) La sensibilisation et la formation des Utilisateurs aux présentes CGU, aux réglementations applicables (notamment en matière de protection des données) et aux règles internes de sécurité de l'organisation du Client.

Le Client demeure seul garant de ses propres opérations de gestion des Identifiants et des accès vis-à-vis de son organisation, du Prestataire, des Utilisateurs et de tout Tiers.

4.2 Notification de changement d'administrateur principal

Le Client s'engage à notifier au Prestataire, dans les meilleurs délais et par les moyens prévus à l'Article 18 des CGV, tout changement d'administrateur principal ou d'interlocuteur opérationnel habilité à représenter le Client auprès du Prestataire, afin de garantir la continuité des échanges contractuels et opérationnels.

4.3 Principe du moindre privilège

Le Client est tenu d'appliquer, dans l'attribution des droits et privilèges aux Utilisateurs, le principe du moindre privilège recommandé par les bonnes pratiques de sécurité et par le référentiel ISO 27001 :

chaque Utilisateur ne dispose que des droits strictement nécessaires à l'exercice de ses fonctions.

*

Article 5 – Sécurité

5.1 Obligation générale de sécurité du Client

Le Client assure, sous sa responsabilité exclusive, la sécurité de l'accès à la Solution SaaS ainsi que des Données Client et du Contenu qui y sont téléversés, hébergés ou stockés par lui-même, par les Utilisateurs ou par le Prestataire pour son compte.

5.2 Prescriptions applicables au Client et aux Utilisateurs

Le Client garantit, sans réserve, se conformer, et faire en sorte que ses Utilisateurs se conforment, aux prescriptions suivantes :

- (i) Déployer toutes mises à jour ordonnées par le Prestataire, tant directement que par l'intermédiaire de la Solution SaaS,
- (ii) Respecter les termes du Contrat ainsi que toutes les instructions raisonnables du Prestataire,
- (iii) Maintenir la confidentialité de ses propres Identifiants ainsi que de ceux des Utilisateurs,
- (iv) Effectuer un usage assurant le bon fonctionnement de la Solution SaaS, sans tenter de contourner ou dévoyer les moyens de sécurité mis en place par le Prestataire,
- (v) Donner l'accès à la Solution SaaS uniquement aux personnes autorisées,
- (vi) Effectuer et conserver, par ses propres moyens et à ses propres frais, des copies ou extractions complémentaires à jour des Données Client et du Contenu selon ses besoins métier, étant rappelé que le Prestataire assure déjà des sauvegardes quotidiennes avec rétention de 30 jours glissants conformément à l'Article 13.4 des CGV,
- (vii) Utiliser la Solution SaaS et ses fonctionnalités conformément à leur finalité, de façon légitime et appropriée, sans en faire usage à des fins détournées,
- (viii) Respecter les moyens techniques de sécurité et de surveillance mis à sa disposition, sans tenter de les détourner.

5.3 Notification d'incident de sécurité

En cas de faille de sécurité constatée ou suspectée (compromission d'Identifiants, intrusion, perte ou divulgation non autorisée de Données Client, etc.), le Client s'engage à :

- (i) Prendre sans délai toutes mesures conservatoires afin d'en limiter les conséquences, notamment, s'il s'agit d'Identifiants, procéder ou faire procéder au changement immédiat de ceux qui sont concernés,
- (ii) Informer sans délai le Prestataire par les moyens prévus à l'Article 18 des CGV, pour lui permettre de prendre immédiatement toute mesure adaptée (investigation, confinement, remédiation, notification réglementaire le cas échéant),
- (iii) Mettre en place un plan d'action pour prévenir tout nouvel incident et coopérer de bonne foi avec le Prestataire pour sa mise en œuvre.

Cette obligation s'entend sans préjudice des obligations respectives des Parties au titre du DPA et du RGPD en matière de notification des violations de données.

5.4 Usage équitable des ressources (Fair Use)

Le Client et les Utilisateurs s'engagent à faire un usage raisonnable et équitable des ressources techniques mises à disposition dans la Solution SaaS, dans le respect du dimensionnement convenu au Devis (volumétrie, nombre d'Utilisateurs, stockage, appels API, etc.).

Sont notamment prohibés, sauf autorisation expresse et écrite préalable du Prestataire :

- Les tests de charge ou tests de performance non autorisés,
- Les opérations d'aspiration massive de données (_scraping_) non conformes aux Spécifications,

- L'utilisation de la Solution SaaS aux fins de bombardement d'emails, de SMS ou de notifications,
- Toute utilisation de nature à dégrader significativement la qualité de service pour les autres Clients hébergés sur l'infrastructure mutualisée.

En cas de dépassement significatif du dimensionnement convenu, le Prestataire se réserve le droit d'émettre un avenant tarifaire ou, à défaut d'accord, de limiter techniquement l'usage dans des conditions raisonnables.

*

Article 6 – Données Client et Contenu

6.1 Principe de gestion exclusive par le Client

Le Client opère seul, sous sa responsabilité exclusive, la gestion des Données Client et du Contenu hébergés dans la Solution SaaS. Le terme « gestion » s'entend, sans limitation, des opérations suivantes effectuées par le Client ou sous sa responsabilité par les Utilisateurs :

- Sélection, vérification de l'authenticité et de la fiabilité,
- Sécurisation applicative et organisationnelle,
- Collecte, saisie (y compris dans les champs de texte libre ou de commentaire), téléversement,
- Stockage, sauvegarde complémentaire, diffusion,
- Suppression et effacement.

Le Client en demeure seul garant vis-à-vis de son organisation, du Prestataire, des Utilisateurs et de tout Tiers. Il fait son affaire personnelle, sous sa responsabilité et à ses frais exclusifs, d'obtenir et de maintenir l'ensemble des droits nécessaires à la gestion des Données Client et du Contenu de façon régulière, licite et légale.

6.2 Contenus et données interdits

Est strictement interdite la saisie, le téléversement, le stockage, le traitement ou la diffusion, dans la Solution SaaS, de Données Client ou de Contenu qui :

- (i) Relèvent des données sensibles interdites au titre de l'Article 2.3 des présentes, hors activation du périmètre HDS pour les Données de Santé,
- (ii) Sont manifestement offensants, discriminatoires, illicites, illégaux ou confidentiels par leur nature et qui ne devraient pas être traités dans la Solution SaaS,
- (iii) Constituent une atteinte, ou sont susceptibles de porter atteinte, aux droits de Tiers et/ou une violation de la loi ou de la réglementation applicable (propriété intellectuelle, droit à l'image, vie privée, secret des affaires, etc.),
- (iv) Constituent une menace pour l'intégrité ou la sécurité de la Solution SaaS (codes malveillants, virus, scripts d'attaque, etc.),
- (v) Portent atteinte, ou sont susceptibles de porter atteinte, à l'image du Prestataire,
- (vi) D'une manière générale, ne sont pas conformes à la finalité de la Solution SaaS définie à l'Article 2 et à l'objet du Contrat.

6.3 Garanties du Client sur le Contenu

Le Client garantit au Prestataire :

- (i) Être titulaire de tous les droits et autorisations nécessaires lui permettant d'opérer la gestion du Contenu de façon licite et légale,
- (ii) Être à jour du règlement de tous droits ou redevances éventuels y afférents (droits d'auteur, droits voisins, redevances SACEM, etc.),
- (iii) Que les Données Client sont authentiques, exactes, complètes et à jour.

6.4 Droits conférés au Prestataire

Dans le cadre du Contrat et sous réserve de son exécution conforme, le Client concède au

Prestataire, à titre non exclusif et pour la seule durée nécessaire à l'exécution du Contrat, le droit d'héberger, de stocker, de copier, de sauvegarder, de transférer et d'afficher les Données Client et le Contenu, dans la stricte mesure nécessaire à la fourniture des prestations.

En outre, le Client autorise expressément le Prestataire à accéder et à supprimer toute Donnée Client ou Contenu non conforme aux dispositions de l'Article 6.2, ou plus largement susceptible de menacer l'intégrité ou la sécurité de la Solution SaaS, à condition d'en informer le Client dans les meilleurs délais.

6.5 Articulation avec la protection des données personnelles

Le traitement des Données à Caractère Personnel contenues dans les Données Client est régi par le DPA mentionné à l'Article 8.4 des CGV, qui prévaut sur les présentes CGU pour toute question relative à la protection des données personnelles.

*

Article 7 – Cookies et Traceurs

La Solution SaaS utilise exclusivement des cookies techniques nécessaires à son fonctionnement (gestion de session, authentification, préférences d'interface), exemptés de consentement au sens de la délibération de la CNIL en vigueur.

Aucun cookie tiers à finalité publicitaire, de profilage comportemental ou de traçage croisé n'est déposé par la Solution SaaS elle-même.

L'utilisation éventuelle de cookies analytiques non exemptés, le cas échéant et selon le paramétrage fonctionnel du Client, est soumise au recueil préalable du consentement explicite des Utilisateurs, dans les conditions de la Charte de Confidentialité.

*

Article 8 – Disponibilité de la Solution SaaS

Le Prestataire s'engage, dans le cadre d'une obligation de moyens, à assurer la disponibilité de la Solution SaaS conformément aux engagements de niveau de service définis à l'Article 13 des CGV WakaStart (taux de disponibilité mensuel de 99 %, fenêtres de maintenance planifiées avec préavis, sauvegardes quotidiennes avec rétention de 30 jours glissants).

Les exclusions, modalités de calcul, sauvegardes et conditions complémentaires applicables sont décrites à l'Article 13 des CGV, auquel les présentes CGU renvoient expressément.

*

Article 9 – Propriété Intellectuelle et Interdictions

9.1 Propriété exclusive du Prestataire

La Solution SaaS, y compris son interface utilisateur, sa charte graphique, ses composants techniques, son Framework WakaStart et l'ensemble de ses éléments constitutifs, sont la propriété exclusive du Prestataire en tant que concepteur, éditeur et développeur, conformément à l'Article 6 des CGV.

Les présentes CGU ne confèrent au Client et aux Utilisateurs qu'un droit d'utilisation limité à la durée du Contrat et conforme à sa finalité, sans aucun transfert de droits de propriété intellectuelle.

9.2 Interdictions expresses

Le Client s'interdit, tant directement que par l'intermédiaire d'un Utilisateur ou d'un Tiers, de :

- (i) Reproduire, copier ou modifier tout ou partie de la Solution SaaS,
- (ii) Accéder et/ou utiliser tout ou partie de la Solution SaaS de manière différente et/ou à toute autre fin que celles expressément prévues au Contrat,

- (iii) Représenter le Prestataire auprès des Tiers,
- (iv) Désassembler, décompiler, effectuer l'ingénierie inverse de tout ou partie de la Solution SaaS, ou tenter d'en découvrir de quelque manière que ce soit le code source ou tout autre secret de conception ou de fabrication, sous réserve des dispositions impératives de l'article L.122-6-1 du Code de la Propriété Intellectuelle relatives à l'interopérabilité,
- (v) Modifier, adapter, traduire et/ou créer des produits, services ou œuvres dérivés de tout ou partie de la Solution SaaS,
- (vi) Diffuser, représenter, publier, republier ou distribuer tout ou partie de la Solution SaaS,
- (vii) Accéder ou utiliser tout ou partie de la Solution SaaS en vue de développer ou de maintenir — ou d'aider un Tiers à développer ou maintenir — des produits ou services concurrents de ceux du Prestataire,
- (viii) Commercialiser, distribuer, vendre, concéder en licence, donner à bail, transférer, céder, héberger, externaliser, promouvoir ou exploiter commercialement de toute autre manière, ou mettre à disposition de quelque manière que ce soit, tout ou partie de la Solution SaaS,
- (ix) Permettre l'accès par un Tiers autre que les Utilisateurs autorisés à tout ou partie de la Solution SaaS, par quelque moyen que ce soit,
- (x) Supprimer ou modifier la marque, le logo ou tout autre signe distinctif du Prestataire contenus dans la Solution SaaS, étant rappelé que les Marques Waka demeurent la propriété exclusive de JDS CONSEIL conformément à l'Article 6.6 des CGV,
- (xi) Effectuer tout acte ou agissement non expressément autorisé par le Contrat ou susceptible de porter atteinte aux droits de propriété intellectuelle du Prestataire,
- (xii) Plus généralement, utiliser la Solution SaaS à des fins illicites ou contraires à l'ordre public, aux lois et/ou réglementations en vigueur.

9.3 Développements Spécifiques — Renvoi

Les dispositions relatives à la cession conditionnelle des droits sur les Développements Spécifiques réalisés par JDS CONSEIL pour le compte du Client figurent à l'Article 6.3 des CGV WakaStart, qui prévaut sur les présentes CGU pour cette question.

*

Article 10 – Suspension et Résiliation

10.1 Suspension par le Prestataire

Le Prestataire se réserve le droit de suspendre l'accès à la Solution SaaS, en tout ou partie, de façon temporaire et sans préavis, dans les cas suivants :

- (i) En cas de risque avéré pour l'intégrité, la sécurité ou la disponibilité de la Solution SaaS (tentative d'intrusion, Manquement grave aux obligations de sécurité de l'Article 5, comportement d'un Utilisateur compromettant la plateforme),
- (ii) En cas de Contenu manifestement illicite ou prohibé au titre de l'Article 6.2, jusqu'à remédiation par le Client,
- (iii) En cas de défaut de paiement du Client dans les conditions prévues à l'Article 5 des CGV,
- (iv) Sur demande d'une autorité publique ou judiciaire compétente,
- (v) En cas de Cas de Force Majeure dans les conditions prévues à l'Article 20 des CGV.

La suspension fait l'objet d'une notification au Client dans les meilleurs délais, conformément à l'Article 18 des CGV, avec l'indication des motifs et, lorsque cela est possible, des mesures de remédiation attendues.

La levée de la suspension intervient dès que la cause ayant motivé la suspension a disparu et que les éventuelles mesures correctives ont été mises en œuvre.

10.2 Résiliation

Les conditions de résiliation anticipée du Contrat sont régies par l'Article 10 des CGV WakaStart. Tout

Manquement grave aux présentes CGU peut constituer un motif légitime de résiliation à ses torts exclusifs, sans préjudice des autres moyens conférés au Prestataire par le Contrat et le droit.

*

Article 11 – Responsabilités

11.1 Obligation essentielle du Client

Le strict respect des présentes CGU par le Client et par les Utilisateurs constitue l'une des obligations essentielles du Client aux termes du Contrat. À ce titre, le Client fait son affaire exclusive, sous son entière responsabilité et, le cas échéant, à ses frais, de les faire respecter et de les rendre opposables aux Utilisateurs.

11.2 Effets d'un Manquement du Client

Tout Manquement du Client ou d'un Utilisateur aux présentes CGU a pour effet de plein droit :

- (i) De dégager la responsabilité du Prestataire tant vis-à-vis du Client que des Tiers pour les conséquences dommageables directement ou indirectement liées au Manquement,
- (ii) D'engager la responsabilité exclusive du Client tant vis-à-vis du Prestataire que des Utilisateurs et des Tiers,
- (iii) De l'exposer à l'entière réparation des dommages causés et à assumer toute sanction financière qui pourrait en résulter,
- (iv) De constituer un motif légitime de résiliation du Contrat à ses torts exclusifs, conformément à l'Article 10 des CGV, sans préjudice des autres moyens conférés au Prestataire par le Contrat et le droit.

11.3 Causes d'exonération du Prestataire

Le Prestataire décline toute responsabilité en cas de difficulté d'exécution du Contrat ayant une cause extérieure à lui, notamment inhérente directement ou indirectement :

- (i) À la création des Comptes Utilisateurs, à l'activation de l'accès à la Solution SaaS par les Utilisateurs et/ou aux droits attribués par le Client à ses Utilisateurs, ainsi qu'à leur gestion,
- (ii) Aux règles internes du Client ou de Tiers en matière informatique,
- (iii) Au réseau Internet, à la connexion Internet et/ou à l'environnement matériel du Client,
- (iv) À la gestion des Données Client et du Contenu par le Client ou les Utilisateurs,
- (v) À l'absence de copies ou sauvegardes complémentaires effectuées par le Client, étant rappelé que le Prestataire assure les sauvegardes standard prévues à l'Article 13.4 des CGV,
- (vi) Plus largement, à tout Manquement constitutif d'un usage inapproprié, illégitime, illicite ou illégal, d'une divulgation d'Identifiants ou d'accès non autorisés.

11.4 Plafond de responsabilité

Le régime de responsabilité du Prestataire, y compris les plafonds applicables et les exclusions légales, est celui défini à l'Article 9 des CGV WakaStart, auquel les présentes CGU renvoient expressément.

Toute sanction prononcée en raison d'un Manquement du Client aux présentes CGU et tous les préjudices subis par le Prestataire ou par des Tiers et résultant directement ou indirectement de ce Manquement restent à la charge exclusive et entière du Client et devront être intégralement réparés par lui.

*

Article 12 – Modification des CGU

Le Prestataire se réserve le droit de modifier les présentes CGU à tout moment, notamment pour tenir compte de l'évolution de la réglementation applicable, de la Solution SaaS, des retours d'expérience

opérationnels ou des bonnes pratiques de sécurité.

Toute modification substantielle fait l'objet d'une notification au Client, conformément à l'Article 18 des CGV WakaStart, avec un préavis raisonnable permettant au Client et aux Utilisateurs d'en prendre connaissance, sans qu'il soit nécessaire de procéder par voie d'Avenant au Contrat.

Les Utilisateurs sont invités à accepter la nouvelle version lors de leur connexion suivant l'entrée en vigueur, dans les conditions de l'Article 1.3 des présentes. À défaut d'acceptation, l'accès à la Solution SaaS pourra être restreint aux fonctionnalités compatibles avec la version antérieure ou suspendu, selon les cas.

Les modifications mineures ou rédactionnelles n'affectant pas les droits substantiels des Parties peuvent être publiées directement, sans préavis, avec mise à jour de la date d'entrée en vigueur portée en tête des présentes.

*

Article 13 – Dispositions survivant à la fin du Contrat

Les obligations du Client et des Utilisateurs au titre des présentes CGU, et notamment celles relatives à la propriété intellectuelle (Article 9), à la confidentialité des Identifiants, à la responsabilité pour Manquement (Article 11) et aux effets d'un usage non conforme, survivent à la fin du Contrat pour toute la durée pendant laquelle elles demeurent utiles à la protection des droits du Prestataire et des Tiers, conformément aux dispositions des CGV et du droit applicable.

*

Article 14 – Langue, Loi applicable et Juridiction

La langue originale et faisant foi des présentes CGU est la langue française.

Les présentes CGU sont régies par le droit français. En cas de litige, les dispositions de l'Article 12 des CGV WakaStart relatives à la loi applicable et à la juridiction compétente s'appliquent.

*

Document contractuel - _JDS CONSEIL_

CGV — WakaStart v1.6

cgv · Version 1.6 · en vigueur depuis le 3 novembre 2026

Charte RGPD — WakaStart v1.0

rgpd · Version 1.0 · en vigueur depuis le 28 avril 2026

Applicables aux Clients et Utilisateurs accédant à la Solution SaaS développée et exploitée par JDS CONSEIL

Entrée en vigueur le 15 avril 2026

Identification du Prestataire

JDS CONSEIL — Société par Actions Simplifiée (SAS), opérant sous la marque commerciale WakaStellar pour l'ensemble de ses produits et modules de la gamme Waka (dont WakaStart, Waka HDS, WakaSign, WakaSeal, WakaInvoice).

- Capital social : 440 760 € (après réduction du 30/12/2024)
- Siège social : Parc d'Activité de Tournebride, 44118 LA CHEVROLIÈRE, France
- RCS : Nantes 529 773 368
- SIRET : 529 773 368 00012
- Code APE/NAF : 6420Z
- N° TVA intracommunautaire : FR45 529 773 368
- Présidente : Jannick SCHIRRA
- Directeur Général : Denis SCHIRRA
- Site web : www.wakastellar.com
- Contact contractuel : contact@wakastellar.com

Ci-après dénommée « JDS CONSEIL » ou le « Prestataire ». Le terme « WakaStellar » désigne la marque commerciale sous laquelle JDS CONSEIL opère ses produits ; il ne désigne aucune entité juridique distincte de JDS CONSEIL.

Article 1 – Préambule et Objet

1.1 Préambule

Les présentes Conditions Générales d'Utilisation (les « CGU ») définissent les règles d'accès et d'utilisation applicables à la Solution SaaS fournie par JDS CONSEIL au Client et aux Utilisateurs, dans le cadre du Contrat conclu entre les Parties.

Elles s'articulent avec les autres documents contractuels dans l'ordre de priorité suivant, conformément à l'Article 2 des CGV WakaStart :

- Les CGV WakaStart définissent le cadre contractuel général entre le Prestataire et le Client,
- Les présentes CGU précisent les conditions opérationnelles d'accès et d'utilisation de la Solution SaaS par les Utilisateurs,
- La Charte de Confidentialité encadre les traitements de données à caractère personnel réalisés par le Prestataire en qualité de Responsable de Traitement,
- Le DPA encadre les traitements de données à caractère personnel réalisés par le Prestataire en qualité de Sous-traitant pour le compte du Client.

1.2 Objet

Les présentes CGU :

- (i) font partie intégrante du Contrat au sens de l'Article 2 des CGV WakaStart et sont valables de façon permanente pendant toute sa durée,
- (ii) ont pour objet de définir les termes et conditions dans lesquels le Client et les Utilisateurs

accèdent à la Solution SaaS et l'utilisent, dans l'objectif d'en garantir la conformité d'utilisation, la sécurité et la disponibilité,

- (iii) s'appliquent de plein droit à tout accès et toute utilisation de la Solution SaaS par le Client ou par ses Utilisateurs, quel que soit le moyen technique d'accès (navigateur, application mobile, API, etc.).

1.3 Acceptation des CGU

Les présentes CGU sont acceptées :

- Par le Client : de façon irrévocable lors de la signature du Devis valant acceptation sans réserve des CGV et des documents annexes, conformément à l'Article 1 des CGV WakaStart.
- Par chaque Utilisateur : de façon individuelle, lors de sa première connexion à la Solution SaaS, par un mécanisme de validation explicite (case à cocher « J'accepte les CGU ») conditionnant l'accès effectif.

En cas de modification substantielle des présentes CGU, les Utilisateurs sont invités à accepter à nouveau la version mise à jour lors de leur connexion suivant l'entrée en vigueur de la nouvelle version, dans les conditions prévues à l'Article 11\.

Les termes employés avec une majuscule initiale dans les présentes CGU ont la signification qui leur est donnée à l'Article 2 des CGV WakaStart, sauf définitions spécifiques introduites ci-après.

1.4 Définitions complémentaires

- « Compte Utilisateur » — Espace d'accès personnel et nominatif ouvert par le Client pour le compte d'un Utilisateur, permettant à ce dernier de se connecter à la Solution SaaS au moyen de ses Identifiants et d'accéder aux fonctionnalités selon les droits et privilèges qui lui sont attribués.
- « Contenu » — Ensemble des textes, images, vidéos, documents, paramétrages, messages et tout autre élément téléversé, saisi, créé ou diffusé par le Client ou les Utilisateurs dans la Solution SaaS. Le Contenu est compris dans les Données Client au sens de l'Article 2 des CGV.
- « Identifiants » — Moyens d'authentification personnels et confidentiels attribués à chaque Utilisateur (identifiant et mot de passe, jetons d'authentification, facteurs d'authentification multi-facteurs le cas échéant) permettant l'accès sécurisé à la Solution SaaS.
- « Manquement » — Tout non-respect par le Client ou un Utilisateur de l'une quelconque des obligations prévues aux présentes CGU ou dans les autres documents contractuels.
- « Tiers » — Toute personne physique ou morale autre que les Parties et les Utilisateurs dûment autorisés.

Article 2 – Finalité de la Solution SaaS

2.1 Nature de la Solution

La Solution SaaS consiste en une application logicielle développée par JDS CONSEIL pour le compte du Client, sur la base du Framework WakaStart, dont la nature fonctionnelle et le périmètre métier sont définis au Devis et formalisés dans les Spécifications validées au titre de l'Article 7.2 des CGV.

Compte tenu du caractère hautement variable des applications SaaS développées par le Prestataire, la Solution SaaS peut couvrir des usages métier très divers (outils de gestion, plateformes collaboratives, progiciels sectoriels, solutions de facturation, applications métier verticales, etc.), tels que précisés par les Spécifications propres à chaque Contrat.

2.2 Destinataires

La Solution SaaS s'adresse exclusivement à des Clients et Utilisateurs professionnels agissant dans le cadre de leur activité professionnelle ou de celle du Client.

Sauf information préalable du Prestataire et sous réserve de faisabilité technique validée lors de la Phase d'Audit & Cadrage, la Solution SaaS ne saurait tenir compte de contraintes ou spécificités propres au Client et/ou aux Utilisateurs non prévues aux Spécifications.

2.3 Données sensibles — Interdiction par défaut

La configuration technique de la Solution SaaS est prévue pour les usages définis au Devis et aux Spécifications. En conséquence, et sauf activation expresse du périmètre HDS au sens de l'Article 3.2 des CGV, le Client et les Utilisateurs s'interdisent formellement de collecter, saisir, téléverser, traiter, stocker, sauvegarder et diffuser dans la Solution SaaS :

- Des Données de Santé au sens de l'article 4.15 du RGPD et de l'article L.1111-8 du Code de la Santé Publique,
- Des données biométriques aux fins d'identifier une personne physique de manière unique,
- Des données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale,
- Des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique,
- Des données génétiques.

En cas d'activation du périmètre HDS, les Données de Santé peuvent être traitées dans la Solution SaaS selon les modalités techniques et contractuelles spécifiques définies au Devis, à l'avenant HDS et au DPA HDS. Les autres catégories de données sensibles ci-dessus demeurent interdites, sauf adaptation contractuelle expresse.

Article 3 – Accès à la Solution SaaS

3.1 URL d'accès

La Solution SaaS est accessible :

- Pour la plateforme WakaStart : à l'adresse sécurisée https://app.wakastart.app/,
- Pour les applications spécifiques développées pour le Client : à une URL dédiée propre au Client, définie au Devis ou communiquée au Client par le Prestataire à l'entrée en vigueur du Contrat (de type <client>.wakastart.app ou URL personnalisée sous nom de domaine du Client, selon le périmètre convenu).

L'accès est opéré en mode SaaS, via le réseau Internet, au moyen d'une connexion sécurisée TLS/SSL (protocole https), depuis un ordinateur, une tablette ou un smartphone via navigateur ou application mobile compatible.

3.2 Prérequis techniques

Préalablement à la conclusion du Contrat et de façon permanente pendant toute sa durée, le Client s'assure qu'il est en mesure de bénéficier de la Solution SaaS, notamment que :

- (i) la souscription du Contrat et son exécution sont conformes à toutes les règles internes en vigueur au sein de son organisation, notamment en matière informatique (charte informatique, politique de sécurité, etc.),
- (ii) les Utilisateurs disposent de façon permanente d'une connexion Internet suffisante et stable (haut débit type ADSL, fibre ou équivalent), des privilèges adéquats, ainsi que d'un environnement matériel sécurisé, fiable et à jour (systèmes d'exploitation supportés, navigateurs supportés, antivirus, mises à jour de sécurité appliquées).

Le Prestataire n'assume aucune responsabilité quant à l'inadéquation des moyens techniques mis en œuvre par le Client ou les Utilisateurs, conformément à l'Article 13.3 des CGV (Exclusions SLA).

3.3 Activation des Comptes Utilisateurs

À l'entrée en vigueur du Contrat, le Prestataire procède à la création et au paramétrage du Compte Utilisateur administrateur du Client, avec les droits et privilèges les plus élevés conformément aux Spécifications.

Par la suite, le Client procède lui-même et sous sa responsabilité exclusive à la création des autres Comptes Utilisateurs, en se conformant à la procédure associée fournie par le Prestataire et aux règles définies aux Spécifications.

Chaque Utilisateur se conforme à la procédure de création et de validation de son mot de passe personnel afin d'activer son accès individuel à la Solution SaaS.

3.4 Identification et authentification

L'accès à la Solution SaaS s'effectue de façon sécurisée à partir des Identifiants propres à chaque Utilisateur.

Les Identifiants sont strictement personnels, incessibles et confidentiels. Chaque Utilisateur est tenu de prendre toutes les mesures nécessaires afin d'en maintenir la confidentialité et de prévenir tout usage par un tiers non autorisé.

Toute action accomplie via les Identifiants d'un Utilisateur est réputée accomplie par cet Utilisateur, sauf preuve contraire fondée sur une compromission notifiée au Prestataire conformément à l'Article 5.3.

3.5 Inactivité des Comptes Utilisateurs

En cohérence avec les exigences de sécurité du SMSI ISO 27001 du Prestataire, les Comptes Utilisateurs n'ayant enregistré aucune connexion pendant une durée continue de douze (12) mois pourront faire l'objet d'une désactivation automatique par le Prestataire, sans préjudice des droits du Client à les réactiver selon les procédures prévues.

Le Client est informé de cette désactivation par notification à son administrateur principal, conformément à l'Article 18 des CGV, dans un délai raisonnable permettant la reprise éventuelle de l'accès.

Article 4 – Gestion des Comptes Utilisateurs et des Accès

4.1 Principe de responsabilité exclusive du Client

De façon permanente pendant toute la durée du Contrat, le Client procède, sous sa responsabilité exclusive, à la gestion des accès à la Solution SaaS par les Utilisateurs, en ce compris :

- (i) La création, désactivation et suppression des Comptes Utilisateurs au moyen des fonctionnalités mises à sa disposition dans la Solution SaaS,
- (ii) L'attribution et la révocation des rôles et niveaux de privilèges de chaque Utilisateur au moyen des fonctionnalités mises à sa disposition,
- (iii) La sensibilisation et la formation des Utilisateurs aux présentes CGU, aux réglementations applicables (notamment en matière de protection des données) et aux règles internes de sécurité de l'organisation du Client.

Le Client demeure seul garant de ses propres opérations de gestion des Identifiants et des accès vis-à-vis de son organisation, du Prestataire, des Utilisateurs et de tout Tiers.

4.2 Notification de changement d'administrateur principal

Le Client s'engage à notifier au Prestataire, dans les meilleurs délais et par les moyens prévus à l'Article 18 des CGV, tout changement d'administrateur principal ou d'interlocuteur opérationnel habilité à représenter le Client auprès du Prestataire, afin de garantir la continuité des échanges contractuels et opérationnels.

4.3 Principe du moindre privilège

Le Client est tenu d'appliquer, dans l'attribution des droits et privilèges aux Utilisateurs, le principe du moindre privilège recommandé par les bonnes pratiques de sécurité et par le référentiel ISO 27001 : chaque Utilisateur ne dispose que des droits strictement nécessaires à l'exercice de ses fonctions.

Article 5 – Sécurité

5.1 Obligation générale de sécurité du Client

Le Client assure, sous sa responsabilité exclusive, la sécurité de l'accès à la Solution SaaS ainsi que des Données Client et du Contenu qui y sont téléversés, hébergés ou stockés par lui-même, par les Utilisateurs ou par le Prestataire pour son compte.

5.2 Prescriptions applicables au Client et aux Utilisateurs

Le Client garantit, sans réserve, se conformer, et faire en sorte que ses Utilisateurs se conforment, aux prescriptions suivantes :

- (i) Déployer toutes mises à jour ordonnées par le Prestataire, tant directement que par l'intermédiaire de la Solution SaaS,
- (ii) Respecter les termes du Contrat ainsi que toutes les instructions raisonnables du Prestataire,
- (iii) Maintenir la confidentialité de ses propres Identifiants ainsi que de ceux des Utilisateurs,
- (iv) Effectuer un usage assurant le bon fonctionnement de la Solution SaaS, sans tenter de contourner ou dévoyer les moyens de sécurité mis en place par le Prestataire,
- (v) Donner l'accès à la Solution SaaS uniquement aux personnes autorisées,
- (vi) Effectuer et conserver, par ses propres moyens et à ses propres frais, des copies ou extractions complémentaires à jour des Données Client et du Contenu selon ses besoins métier, étant rappelé que le Prestataire assure déjà des sauvegardes quotidiennes avec rétention de 30 jours glissants conformément à l'Article 13.4 des CGV,
- (vii) Utiliser la Solution SaaS et ses fonctionnalités conformément à leur finalité, de façon légitime et appropriée, sans en faire usage à des fins détournées,
- (viii) Respecter les moyens techniques de sécurité et de surveillance mis à sa disposition, sans tenter de les détourner.

5.3 Notification d'incident de sécurité

En cas de faille de sécurité constatée ou suspectée (compromission d'Identifiants, intrusion, perte ou divulgation non autorisée de Données Client, etc.), le Client s'engage à :

- (i) Prendre sans délai toutes mesures conservatoires afin d'en limiter les conséquences, notamment, s'il s'agit d'Identifiants, procéder ou faire procéder au changement immédiat de ceux qui sont concernés,
- (ii) Informer sans délai le Prestataire par les moyens prévus à l'Article 18 des CGV, pour lui permettre de prendre immédiatement toute mesure adaptée (investigation, confinement, remédiation, notification réglementaire le cas échéant),
- (iii) Mettre en place un plan d'action pour prévenir tout nouvel incident et coopérer de bonne foi avec le Prestataire pour sa mise en œuvre.

Cette obligation s'entend sans préjudice des obligations respectives des Parties au titre du DPA et du RGPD en matière de notification des violations de données.

5.4 Usage équitable des ressources (Fair Use)

Le Client et les Utilisateurs s'engagent à faire un usage raisonnable et équitable des ressources

techniques mises à disposition dans la Solution SaaS, dans le respect du dimensionnement convenu au Devis (volumétrie, nombre d'Utilisateurs, stockage, appels API, etc.).

Sont notamment prohibés, sauf autorisation expresse et écrite préalable du Prestataire :

- Les tests de charge ou tests de performance non autorisés,
- Les opérations d'aspiration massive de données (scraping) non conformes aux Spécifications,
- L'utilisation de la Solution SaaS aux fins de bombardement d'emails, de SMS ou de notifications,
- Toute utilisation de nature à dégrader significativement la qualité de service pour les autres Clients hébergés sur l'infrastructure mutualisée.

En cas de dépassement significatif du dimensionnement convenu, le Prestataire se réserve le droit d'émettre un avenant tarifaire ou, à défaut d'accord, de limiter techniquement l'usage dans des conditions raisonnables.

Article 6 – Données Client et Contenu

6.1 Principe de gestion exclusive par le Client

Le Client opère seul, sous sa responsabilité exclusive, la gestion des Données Client et du Contenu hébergés dans la Solution SaaS. Le terme « gestion » s'entend, sans limitation, des opérations suivantes effectuées par le Client ou sous sa responsabilité par les Utilisateurs :

- Sélection, vérification de l'authenticité et de la fiabilité,
- Sécurisation applicative et organisationnelle,
- Collecte, saisie (y compris dans les champs de texte libre ou de commentaire), téléversement,
- Stockage, sauvegarde complémentaire, diffusion,
- Suppression et effacement.

Le Client en demeure seul garant vis-à-vis de son organisation, du Prestataire, des Utilisateurs et de tout Tiers. Il fait son affaire personnelle, sous sa responsabilité et à ses frais exclusifs, d'obtenir et de maintenir l'ensemble des droits nécessaires à la gestion des Données Client et du Contenu de façon régulière, licite et légale.

6.2 Contenus et données interdits

Est strictement interdite la saisie, le téléversement, le stockage, le traitement ou la diffusion, dans la Solution SaaS, de Données Client ou de Contenu qui :

- (i) Relèvent des données sensibles interdites au titre de l'Article 2.3 des présentes, hors activation du périmètre HDS pour les Données de Santé,
- (ii) Sont manifestement offensants, discriminatoires, illicites, illégaux ou confidentiels par leur nature et qui ne devraient pas être traités dans la Solution SaaS,
- (iii) Constituent une atteinte, ou sont susceptibles de porter atteinte, aux droits de Tiers et/ou une violation de la loi ou de la réglementation applicable (propriété intellectuelle, droit à l'image, vie privée, secret des affaires, etc.),
- (iv) Constituent une menace pour l'intégrité ou la sécurité de la Solution SaaS (codes malveillants, virus, scripts d'attaque, etc.),
- (v) Portent atteinte, ou sont susceptibles de porter atteinte, à l'image du Prestataire,
- (vi) D'une manière générale, ne sont pas conformes à la finalité de la Solution SaaS définie à l'Article 2 et à l'objet du Contrat.

6.3 Garanties du Client sur le Contenu

Le Client garantit au Prestataire :

- (i) Être titulaire de tous les droits et autorisations nécessaires lui permettant d'opérer la gestion du Contenu de façon licite et légale,
- (ii) Être à jour du règlement de tous droits ou redevances éventuels y afférents (droits d'auteur, droits voisins, redevances SACEM, etc.),
- (iii) Que les Données Client sont authentiques, exactes, complètes et à jour.

6.4 Droits conférés au Prestataire

Dans le cadre du Contrat et sous réserve de son exécution conforme, le Client concède au Prestataire, à titre non exclusif et pour la seule durée nécessaire à l'exécution du Contrat, le droit d'héberger, de stocker, de copier, de sauvegarder, de transférer et d'afficher les Données Client et le Contenu, dans la stricte mesure nécessaire à la fourniture des prestations.

En outre, le Client autorise expressément le Prestataire à accéder et à supprimer toute Donnée Client ou Contenu non conforme aux dispositions de l'Article 6.2, ou plus largement susceptible de menacer l'intégrité ou la sécurité de la Solution SaaS, à condition d'en informer le Client dans les meilleurs délais.

6.5 Articulation avec la protection des données personnelles

Le traitement des Données à Caractère Personnel contenues dans les Données Client est régi par le DPA mentionné à l'Article 8.4 des CGV, qui prévaut sur les présentes CGU pour toute question relative à la protection des données personnelles.

Article 7 – Cookies et Traceurs

La Solution SaaS utilise exclusivement des cookies techniques nécessaires à son fonctionnement (gestion de session, authentification, préférences d'interface), exemptés de consentement au sens de la délibération de la CNIL en vigueur.

Aucun cookie tiers à finalité publicitaire, de profilage comportemental ou de traçage croisé n'est déposé par la Solution SaaS elle-même.

L'utilisation éventuelle de cookies analytiques non exemptés, le cas échéant et selon le paramétrage fonctionnel du Client, est soumise au recueil préalable du consentement explicite des Utilisateurs, dans les conditions de la Charte de Confidentialité.

Article 8 – Disponibilité de la Solution SaaS

Le Prestataire s'engage, dans le cadre d'une obligation de moyens, à assurer la disponibilité de la Solution SaaS conformément aux engagements de niveau de service définis à l'Article 13 des CGV WakaStart (taux de disponibilité mensuel de 99 %, fenêtres de maintenance planifiées avec préavis, sauvegardes quotidiennes avec rétention de 30 jours glissants).

Les exclusions, modalités de calcul, sauvegardes et conditions complémentaires applicables sont décrites à l'Article 13 des CGV, auquel les présentes CGU renvoient expressément.

Article 9 – Propriété Intellectuelle et Interdictions

9.1 Propriété exclusive du Prestataire

La Solution SaaS, y compris son interface utilisateur, sa charte graphique, ses composants techniques, son Framework WakaStart et l'ensemble de ses éléments constitutifs, sont la propriété exclusive du Prestataire en tant que concepteur, éditeur et développeur, conformément à l'Article 6 des CGV.

Les présentes CGU ne confèrent au Client et aux Utilisateurs qu'un droit d'utilisation limité à la durée du Contrat et conforme à sa finalité, sans aucun transfert de droits de propriété intellectuelle.

9.2 Interdictions expresses

Le Client s'interdit, tant directement que par l'intermédiaire d'un Utilisateur ou d'un Tiers, de :

- (i) Reproduire, copier ou modifier tout ou partie de la Solution SaaS,
- (ii) Accéder et/ou utiliser tout ou partie de la Solution SaaS de manière différente et/ou à toute autre fin que celles expressément prévues au Contrat,
- (iii) Représenter le Prestataire auprès des Tiers,
- (iv) Désassembler, décompiler, effectuer l'ingénierie inverse de tout ou partie de la Solution SaaS, ou tenter d'en découvrir de quelque manière que ce soit le code source ou tout autre secret de conception ou de fabrication, sous réserve des dispositions impératives de l'article L.122-6-1 du Code de la Propriété Intellectuelle relatives à l'interopérabilité,
- (v) Modifier, adapter, traduire et/ou créer des produits, services ou œuvres dérivés de tout ou partie de la Solution SaaS,
- (vi) Diffuser, représenter, publier, republier ou distribuer tout ou partie de la Solution SaaS,
- (vii) Accéder ou utiliser tout ou partie de la Solution SaaS en vue de développer ou de maintenir — ou d'aider un Tiers à développer ou maintenir — des produits ou services concurrents de ceux du Prestataire,
- (viii) Commercialiser, distribuer, vendre, concéder en licence, donner à bail, transférer, céder, héberger, externaliser, promouvoir ou exploiter commercialement de toute autre manière, ou mettre à disposition de quelque manière que ce soit, tout ou partie de la Solution SaaS,
- (ix) Permettre l'accès par un Tiers autre que les Utilisateurs autorisés à tout ou partie de la Solution SaaS, par quelque moyen que ce soit,
- (x) Supprimer ou modifier la marque, le logo ou tout autre signe distinctif du Prestataire contenus dans la Solution SaaS, étant rappelé que les Marques Waka demeurent la propriété exclusive de JDS CONSEIL conformément à l'Article 6.6 des CGV,
- (xi) Effectuer tout acte ou agissement non expressément autorisé par le Contrat ou susceptible de porter atteinte aux droits de propriété intellectuelle du Prestataire,
- (xii) Plus généralement, utiliser la Solution SaaS à des fins illicites ou contraires à l'ordre public, aux lois et/ou réglementations en vigueur.

9.3 Développements Spécifiques — Renvoi

Les dispositions relatives à la cession conditionnelle des droits sur les Développements Spécifiques réalisés par JDS CONSEIL pour le compte du Client figurent à l'Article 6.3 des CGV WakaStart, qui prévaut sur les présentes CGU pour cette question.

Article 10 – Suspension et Résiliation

10.1 Suspension par le Prestataire

Le Prestataire se réserve le droit de suspendre l'accès à la Solution SaaS, en tout ou partie, de façon temporaire et sans préavis, dans les cas suivants :

- (i) En cas de risque avéré pour l'intégrité, la sécurité ou la disponibilité de la Solution SaaS (tentative d'intrusion, Manquement grave aux obligations de sécurité de l'Article 5, comportement d'un Utilisateur compromettant la plateforme),
- (ii) En cas de Contenu manifestement illicite ou prohibé au titre de l'Article 6.2, jusqu'à remédiation par le Client,

- (iii) En cas de défaut de paiement du Client dans les conditions prévues à l'Article 5 des CGV,
- (iv) Sur demande d'une autorité publique ou judiciaire compétente,
- (v) En cas de Cas de Force Majeure dans les conditions prévues à l'Article 20 des CGV.

La suspension fait l'objet d'une notification au Client dans les meilleurs délais, conformément à l'Article 18 des CGV, avec l'indication des motifs et, lorsque cela est possible, des mesures de remédiation attendues.

La levée de la suspension intervient dès que la cause ayant motivé la suspension a disparu et que les éventuelles mesures correctives ont été mises en œuvre.

10.2 Résiliation

Les conditions de résiliation anticipée du Contrat sont régies par l'Article 10 des CGV WakaStart. Tout Manquement grave aux présentes CGU peut constituer un motif légitime de résiliation à ses torts exclusifs, sans préjudice des autres moyens conférés au Prestataire par le Contrat et le droit.

Article 11 – Responsabilités

11.1 Obligation essentielle du Client

Le strict respect des présentes CGU par le Client et par les Utilisateurs constitue l'une des obligations essentielles du Client aux termes du Contrat. À ce titre, le Client fait son affaire exclusive, sous son entière responsabilité et, le cas échéant, à ses frais, de les faire respecter et de les rendre opposables aux Utilisateurs.

11.2 Effets d'un Manquement du Client

Tout Manquement du Client ou d'un Utilisateur aux présentes CGU a pour effet de plein droit :

- (i) De dégager la responsabilité du Prestataire tant vis-à-vis du Client que des Tiers pour les conséquences dommageables directement ou indirectement liées au Manquement,
- (ii) D'engager la responsabilité exclusive du Client tant vis-à-vis du Prestataire que des Utilisateurs et des Tiers,
- (iii) De l'exposer à l'entière réparation des dommages causés et à assumer toute sanction financière qui pourrait en résulter,
- (iv) De constituer un motif légitime de résiliation du Contrat à ses torts exclusifs, conformément à l'Article 10 des CGV, sans préjudice des autres moyens conférés au Prestataire par le Contrat et le droit.

11.3 Causes d'exonération du Prestataire

Le Prestataire décline toute responsabilité en cas de difficulté d'exécution du Contrat ayant une cause extérieure à lui, notamment inhérente directement ou indirectement :

- (i) À la création des Comptes Utilisateurs, à l'activation de l'accès à la Solution SaaS par les Utilisateurs et/ou aux droits attribués par le Client à ses Utilisateurs, ainsi qu'à leur gestion,
- (ii) Aux règles internes du Client ou de Tiers en matière informatique,
- (iii) Au réseau Internet, à la connexion Internet et/ou à l'environnement matériel du Client,
- (iv) À la gestion des Données Client et du Contenu par le Client ou les Utilisateurs,
- (v) À l'absence de copies ou sauvegardes complémentaires effectuées par le Client, étant rappelé que le Prestataire assure les sauvegardes standard prévues à l'Article 13.4 des CGV,
- (vi) Plus largement, à tout Manquement constitutif d'un usage inapproprié, illégitime, illicite ou illégal, d'une divulgation d'Identifiants ou d'accès non autorisés.

11.4 Plafond de responsabilité

Le régime de responsabilité du Prestataire, y compris les plafonds applicables et les exclusions légales, est celui défini à l'Article 9 des CGV WakaStart, auquel les présentes CGU renvoient expressément.

Toute sanction prononcée en raison d'un Manquement du Client aux présentes CGU et tous les préjudices subis par le Prestataire ou par des Tiers et résultant directement ou indirectement de ce Manquement restent à la charge exclusive et entière du Client et devront être intégralement réparés par lui.

Article 12 – Modification des CGU

Le Prestataire se réserve le droit de modifier les présentes CGU à tout moment, notamment pour tenir compte de l'évolution de la réglementation applicable, de la Solution SaaS, des retours d'expérience opérationnels ou des bonnes pratiques de sécurité.

Toute modification substantielle fait l'objet d'une notification au Client, conformément à l'Article 18 des CGV WakaStart, avec un préavis raisonnable permettant au Client et aux Utilisateurs d'en prendre connaissance, sans qu'il soit nécessaire de procéder par voie d'Avenant au Contrat.

Les Utilisateurs sont invités à accepter la nouvelle version lors de leur connexion suivant l'entrée en vigueur, dans les conditions de l'Article 1.3 des présentes. À défaut d'acceptation, l'accès à la Solution SaaS pourra être restreint aux fonctionnalités compatibles avec la version antérieure ou suspendu, selon les cas.

Les modifications mineures ou rédactionnelles n'affectant pas les droits substantiels des Parties peuvent être publiées directement, sans préavis, avec mise à jour de la date d'entrée en vigueur portée en tête des présentes.

Article 13 – Dispositions survivant à la fin du Contrat

Les obligations du Client et des Utilisateurs au titre des présentes CGU, et notamment celles relatives à la propriété intellectuelle (Article 9), à la confidentialité des Identifiants, à la responsabilité pour Manquement (Article 11\) et aux effets d'un usage non conforme, survivent à la fin du Contrat pour toute la durée pendant laquelle elles demeurent utiles à la protection des droits du Prestataire et des Tiers, conformément aux dispositions des CGV et du droit applicable.

Article 14 – Langue, Loi applicable et Juridiction

La langue originale et faisant foi des présentes CGU est la langue française.

Les présentes CGU sont régies par le droit français. En cas de litige, les dispositions de l'Article 12 des CGV WakaStart relatives à la loi applicable et à la juridiction compétente s'appliquent.

Document contractuel \- JDS CONSEIL

DPA — WakaStart v1.0

dpa · Version 1.0 · en vigueur depuis le 28 avril 2026

Data Processing Agreement applicable aux traitements de données à caractère personnel réalisés par JDS CONSEIL en qualité de Sous-traitant pour le compte du Client Responsable de traitement

Entrée en vigueur le 15 avril 2026

Conclu en application de l'article 28 du Règlement (UE) 2016/679 (RGPD)

Identification des Parties

Sous-traitant

JDS CONSEIL — Société par Actions Simplifiée (SAS), opérant sous la marque commerciale WakaStellar pour l'ensemble de ses produits et modules de la gamme Waka (dont WakaStart, Waka HDS, WakaSign, WakaSeal, WakaInvoice).

- Capital social : 440 760 € (après réduction du 30/12/2024)
- Siège social : Parc d'Activité de Tournebride, 44118 LA CHEVROLIÈRE, France
- RCS : Nantes 529 773 368
- SIRET : 529 773 368 00012
- Code APE/NAF : 6420Z
- N° TVA intracommunautaire : FR45 529 773 368
- Présidente : Jannick SCHIRRA
- Directeur Général : Denis SCHIRRA
- Site web : www.wakastellar.com
- Contact contractuel : contact@wakastellar.com

Déléguée à la Protection des Données (DPO) :

- Florelle SCHIRRA, désignée auprès de la CNIL.
- Adresse postale : 17, rue de la Guillauderie, 44118 LA CHEVROLIÈRE, France
- Email dédié : dpo@wakastellar.com

Ci-après dénommée « JDS CONSEIL » ou le « Responsable de Traitement ». Le terme « WakaStellar » désigne la marque commerciale sous laquelle JDS CONSEIL opère ses produits ; il ne désigne aucune entité juridique distincte de JDS CONSEIL.

Responsable de Traitement

Le Client, tel qu'identifié dans le Devis signé avec JDS CONSEIL, agissant pour ses propres besoins et ceux de ses Utilisateurs finaux.

Ci-après dénommé le « Client » ou le « Responsable de Traitement » au sens du RGPD.

Les Parties sont ensemble dénommées les « Parties » et individuellement une « Partie ».

Article 1 – Préambule et Objet

1.1 Contexte contractuel

Les Parties sont liées par les Conditions Générales de Vente WakaStart (les « CGV ») portant sur la fourniture d'une Solution SaaS développée et hébergée par le Prestataire, selon la méthodologie définie à l'Article 7 des CGV et dans les conditions d'Hébergement, d'Infogérance et de Sécurité

définies aux Articles 3 et 13 des CGV.

Le Contrat est complété par les CGU (Conditions Générales d'Utilisation) qui encadrent les règles opérationnelles d'accès et d'utilisation de la Solution SaaS par le Client et les Utilisateurs, et par la Charte de Confidentialité qui encadre les traitements réalisés par le Prestataire agissant en qualité de Responsable de Traitement pour ses propres besoins de gestion. L'articulation entre ces documents est précisée à l'Article 8.5 des CGV.

Le Prestataire développe, dans le cadre de la plateforme WakaStart, des applications SaaS pour le compte de ses Clients. Ces applications sont de nature extrêmement variable et répondent à des besoins métier spécifiques propres à chaque Client : outils de gestion, plateformes collaboratives, progiciels sectoriels, solutions de facturation, applications métier verticales, etc. En conséquence, les catégories de Données Client hébergées peuvent varier significativement d'un Contrat à l'autre, tant en nature qu'en volume et en sensibilité.

1.2 Répartition des rôles RGPD

Dans le cadre de l'exécution du Contrat et de l'exploitation de la Solution SaaS :

- Le Client agit en qualité de Responsable de Traitement au sens de l'article 4.7 du RGPD pour l'ensemble des Données Client hébergées et traitées dans la Solution SaaS. Il détermine seul les finalités et les moyens des traitements mis en œuvre via la Solution SaaS et assume la pleine et entière responsabilité de la licéité, de la loyauté, de la transparence, de la minimisation, de l'exactitude, de la limitation de la conservation et de la sécurité des traitements qu'il met en œuvre.
- Le Prestataire agit en qualité de Sous-traitant au sens de l'article 4.8 du RGPD, traitant les Données Client pour le compte et selon les instructions documentées du Client.

Il est expressément rappelé que, parallèlement, le Prestataire agit en qualité de Responsable de Traitement pour les données à caractère personnel qu'il collecte directement auprès des interlocuteurs professionnels du Client (gestion contractuelle, facturation, support) dans les conditions définies par la Charte de Confidentialité annexée aux CGV. Le présent DPA ne couvre pas ces traitements.

1.3 Objet du DPA

Le présent Accord de Traitement des Données (ci-après le « DPA ») a pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à traiter les Données Client pour le compte du Responsable de Traitement, conformément à l'article 28 du RGPD.

Le DPA fait partie intégrante du Contrat au sens de l'Article 2 des CGV et prévaut, pour toutes les questions relatives à la protection des données à caractère personnel, sur toute disposition contradictoire des CGV ou du Devis.

Les termes employés avec une majuscule initiale dans le présent DPA ont la signification qui leur est donnée à l'Article 2 des CGV WakaStart, sauf définitions spécifiques introduites ci-après.

1.4 Définitions complémentaires

- « Données Client » ou « Données à Caractère Personnel » — Pour les besoins du présent DPA et par exception à la définition plus large figurant à l'Article 2 des CGV WakaStart, le terme désigne ici exclusivement les données à caractère personnel, au sens de l'article 4.1 du RGPD, traitées par le Sous-traitant pour le compte du Responsable de Traitement dans le cadre du Contrat, telles que décrites à l'Annexe 1\. Les données non personnelles hébergées par le Client dans la Solution SaaS demeurent régies par la définition générale des CGV et ne relèvent pas du présent DPA.
- « Traitement » — Toute opération ou ensemble d'opérations, au sens de l'article 4.2 du RGPD, effectuée(s) sur les Données Client, telles que décrites à l'Annexe 1\.
- « Personne Concernée » — Toute personne physique identifiée ou identifiable dont les Données Client font l'objet d'un Traitement.

- « Sous-traitant Ultérieur » — Tout tiers auquel le Sous-traitant fait appel pour exécuter tout ou partie des Traitements, conformément à l'Article 7 du présent DPA.
- « Violation de Données » — Violation de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Client ou l'accès non autorisé à celles-ci, au sens de l'article 4.12 du RGPD.

Article 2 – Description du Traitement

Les caractéristiques des Traitements réalisés par le Sous-traitant pour le compte du Responsable de Traitement sont décrites en Annexe 1 du présent DPA :

- Nature et finalité des Traitements,
- Catégories de Personnes Concernées,
- Catégories de Données Client,
- Durée des Traitements.

Responsabilité du Client sur le contenu hébergé — Le Client reconnaît et accepte expressément que, compte tenu du caractère hautement variable des applications SaaS développées par le Prestataire, il demeure seul et pleinement responsable du contenu des Données Client hébergées dans la Solution SaaS, de leur licéité, de leur pertinence au regard des finalités déclarées, et du respect des droits des Personnes Concernées. Le Sous-traitant n'exerce aucun contrôle éditorial ou de conformité a priori sur les Données Client saisies ou téléversées par le Client ou ses Utilisateurs dans la Solution SaaS.

Toute modification substantielle de la nature des Données Client ou des finalités poursuivies par le Client, en cours de Contrat, doit être portée à la connaissance du Sous-traitant conformément à l'Article 3 ci-après et peut, si elle impacte les conditions techniques ou organisationnelles du Traitement, donner lieu à un Avenant au présent DPA.

Article 3 – Instructions Documentées du Responsable de Traitement

3.1 Principe

Le Sous-traitant ne traite les Données Client que sur instruction documentée du Responsable de Traitement, y compris en ce qui concerne les transferts de Données Client vers un pays tiers ou une organisation internationale, sauf obligation légale contraire applicable au Sous-traitant.

3.2 Instructions initiales

Les instructions initiales du Responsable de Traitement résultent :

- Des dispositions du Contrat (CGV, Devis, présent DPA),
- Du paramétrage fonctionnel de la Solution SaaS validé lors de la Phase d'Audit & Cadrage et formalisé dans les Spécifications,
- Des configurations et paramètres opérationnels définis par le Client dans la Solution SaaS (droits d'accès, règles de rétention, paramètres de notification, etc.).

3.3 Instructions complémentaires

Toute instruction complémentaire doit être transmise par le Responsable de Traitement au Sous-traitant par écrit, conformément aux modalités de l'Article 18 des CGV (email avec confirmation de réception).

Le Sous-traitant se réserve le droit de refuser ou de suspendre l'exécution d'une instruction qui :

- Lui paraîtrait manifestement contraire au RGPD ou à toute autre disposition légale applicable à la protection des données,

- Excéderait le périmètre fonctionnel du Contrat ou les capacités techniques de la Solution SaaS,
- Relèverait d'une prestation supplémentaire facturable au titre de la TMA.

Dans ce cas, le Sous-traitant informe le Responsable de Traitement par écrit des motifs de son refus ou de sa réserve dans un délai raisonnable.

Article 4 – Obligations du Sous-traitant

4.1 Confidentialité

Le Sous-traitant s'engage à :

- Traiter les Données Client dans le strict respect des finalités définies au présent DPA et aux instructions du Responsable de Traitement,
- Garantir que les personnes autorisées à traiter les Données Client s'engagent au respect de la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
- Limiter l'accès aux Données Client aux seules personnes dont l'intervention est strictement nécessaire à l'exécution du Contrat, selon le principe du « besoin d'en connaître » (need-to-know).

4.2 Sécurité des Traitements

Le Sous-traitant met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, conformément à l'article 32 du RGPD, dans le cadre de son SMSI certifié ISO 27001.

Les mesures techniques et organisationnelles mises en œuvre sont détaillées en Annexe 2 du présent DPA.

Dans l'hypothèse où le Contrat porte sur un périmètre HDS activé au sens de l'Article 3.2 des CGV, les dispositions de l'Annexe 4 du présent DPA (Conditions particulières HDS) s'appliquent de plein droit et prévalent, pour toute question relative aux DSCP, sur les dispositions du présent DPA.

4.3 Durée de conservation des logs de sécurité

Les logs de sécurité associés aux Traitements (logs d'accès, logs d'activité, traces techniques de connexion) sont conservés par le Sous-traitant pour une durée de douze (12) mois glissants à compter de leur enregistrement, conformément aux recommandations de la CNIL et aux exigences du référentiel ISO 27001 en matière de traçabilité.

4.4 Assistance du Responsable de Traitement

Le Sous-traitant assiste le Responsable de Traitement, dans la mesure du possible et compte tenu de la nature des Traitements, dans :

- La réponse aux demandes d'exercice de droits des Personnes Concernées (Article 6),
- La notification des Violations de Données (Article 5),
- La réalisation des analyses d'impact relatives à la protection des données (AIPD) le concernant, en fournissant les informations techniques pertinentes,
- La consultation préalable de l'autorité de contrôle, le cas échéant.

Les prestations d'assistance excédant les diligences standard prévues au présent DPA peuvent être facturées au taux journalier de la TMA défini au Devis, sur bon de commande spécifique.

4.5 Documentation et registre

Le Sous-traitant tient à jour un registre des catégories d'activités de Traitement effectuées pour le compte du Responsable de Traitement, conformément à l'article 30.2 du RGPD. Ce registre est tenu à la disposition du Responsable de Traitement sur simple demande écrite.

Article 5 – Notification des Violations de Données

5.1 Obligation de notification

Le Sous-traitant notifie au Responsable de Traitement toute Violation de Données affectant les Données Client dans un délai maximum de quarante-huit (48) heures après en avoir pris connaissance.

Par dérogation, lorsque la Violation de Données affecte des DSCP dans le cadre d'un périmètre HDS activé, le délai est ramené à vingt-quatre (24) heures, conformément aux exigences renforcées du référentiel HDS et à l'Article 6.4 de l'Annexe 4 du présent DPA.

Cette notification est adressée par email à l'adresse contractuelle du Responsable de Traitement, conformément à l'Article 18 des CGV, avec demande de confirmation de réception.

5.2 Contenu de la notification

La notification doit comprendre, dans la mesure des informations disponibles au moment de l'envoi et sans préjudice de compléments ultérieurs :

- La nature de la Violation de Données, incluant, dans la mesure du possible, les catégories et le nombre approximatif de Personnes Concernées et les catégories et le nombre approximatif d'enregistrements de Données Client concernés,
- Le nom et les coordonnées de la Déléguée à la Protection des Données (DPO) ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues,
- Les conséquences probables de la Violation de Données,
- Les mesures prises ou proposées par le Sous-traitant pour remédier à la Violation de Données, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

5.3 Coopération et documentation

Le Sous-traitant assiste le Responsable de Traitement, dans la mesure de ses moyens, pour lui permettre de respecter ses propres obligations de notification auprès de la CNIL (dans un délai de 72 heures) et, le cas échéant, de communication aux Personnes Concernées, conformément aux articles 33 et 34 du RGPD.

Le Sous-traitant documente toute Violation de Données, ses effets et les mesures prises pour y remédier. Cette documentation est tenue à la disposition du Responsable de Traitement et de la CNIL.

Article 6 – Droits des Personnes Concernées

Le Sous-traitant, tenant compte de la nature des Traitements, assiste le Responsable de Traitement par des mesures techniques et organisationnelles appropriées, dans la mesure du possible, pour s'acquitter de son obligation de donner suite aux demandes dont les Personnes Concernées le saisissent en vue d'exercer leurs droits RGPD (accès, rectification, effacement, limitation, portabilité, opposition, directives post-mortem).

6.1 Transmission des demandes

Si une Personne Concernée adresse directement au Sous-traitant une demande d'exercice de droits portant sur des Données Client, le Sous-traitant :

- Ne répond pas directement à la demande, sauf instruction contraire du Responsable de Traitement,
- Transmet la demande au Responsable de Traitement sans délai et au plus tard dans un délai de cinq (5) Jours Ouvrés à compter de sa réception,

- Accompagne cette transmission, le cas échéant, de tout élément de contexte utile à son traitement.

6.2 Moyens techniques mis à disposition

Le Sous-traitant met à disposition du Responsable de Traitement, dans l'interface d'administration de la Solution SaaS, les fonctionnalités techniques nécessaires pour permettre au Responsable de Traitement de traiter lui-même les demandes d'exercice de droits des Personnes Concernées (export des données, rectification, suppression, etc.), dans la mesure du périmètre fonctionnel prévu aux Spécifications.

Article 7 – Sous-traitance Ultérieure

7.1 Autorisation générale

Le Responsable de Traitement autorise de manière générale le Sous-traitant à recourir à des Sous-traitants Ultérieurs pour l'exécution de tout ou partie des Traitements, dans les conditions prévues par l'Article 16 des CGV et par le présent Article 7\.

7.2 Liste initiale des Sous-traitants Ultérieurs

La liste des Sous-traitants Ultérieurs principaux à la date d'entrée en vigueur du présent DPA figure en Annexe 3. Cette liste inclut notamment OVH (OVHcloud) en qualité de fournisseur d'hébergement et d'infrastructure cloud.

La liste actualisée est tenue à la disposition du Responsable de Traitement sur simple demande écrite.

7.3 Notification des nouveaux Sous-traitants Ultérieurs

Le Sous-traitant informe par écrit le Responsable de Traitement de tout projet de recours à un nouveau Sous-traitant Ultérieur ou de remplacement d'un Sous-traitant Ultérieur existant, avec un préavis minimum de trente (30) jours calendaires.

Pendant ce préavis, le Responsable de Traitement peut émettre une objection motivée à ce changement, par écrit, conformément à l'Article 18 des CGV. L'objection doit être fondée sur des motifs raisonnables liés à la protection des données.

En cas d'objection :

- Les Parties s'efforcent de bonne foi de trouver une solution alternative dans un délai raisonnable,
- À défaut de solution, le Sous-traitant peut renoncer au recours au nouveau Sous-traitant Ultérieur, ou, à défaut, le Responsable de Traitement dispose d'un droit de résiliation anticipée du Contrat limitée à la partie des prestations impactées, sans pénalité.

7.4 Garanties exigées des Sous-traitants Ultérieurs

Le Sous-traitant s'engage à ne recourir qu'à des Sous-traitants Ultérieurs présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière à ce que les Traitements répondent aux exigences du RGPD.

À cet effet, le Sous-traitant conclut avec chaque Sous-traitant Ultérieur un contrat écrit imposant les mêmes obligations en matière de protection des données que celles figurant dans le présent DPA, conformément à l'article 28.4 du RGPD.

7.5 Responsabilité

Le Sous-traitant demeure pleinement responsable devant le Responsable de Traitement de l'exécution, par ses Sous-traitants Ultérieurs, de leurs obligations en matière de protection des données.

Article 8 – Transferts hors Union Européenne

Le Sous-traitant déclare et certifie que les Données Client ne font l'objet d'aucun transfert hors du territoire de l'Union Européenne, ni d'aucun Traitement en dehors du territoire de l'Union Européenne, cohérent avec le choix d'un hébergement souverain auprès d'OVHcloud en France et avec le référentiel ISO 27001 du Sous-traitant.

Toute évolution future de cette situation ferait l'objet d'une notification préalable au Responsable de Traitement conformément à l'Article 7.3 du présent DPA et d'une mise à jour du DPA, accompagnée de la mise en place des garanties appropriées prévues aux articles 45 à 49 du RGPD (décision d'adéquation, clauses contractuelles types de la Commission Européenne, règles d'entreprise contraignantes, etc.).

Article 9 – Droit d'Audit du Responsable de Traitement

9.1 Principe

Le Sous-traitant met à la disposition du Responsable de Traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues par l'article 28 du RGPD.

À cet effet, le Responsable de Traitement dispose d'un droit d'audit des Traitements effectués par le Sous-traitant, dans les conditions suivantes.

9.2 Fréquence et préavis

Le Responsable de Traitement peut diligenter un audit au maximum une (1) fois par année civile, sauf en cas de Violation de Données avérée affectant les Données Client, auquel cas un audit supplémentaire peut être diligenté sans délai.

L'audit est programmé avec un préavis écrit minimum de trente (30) jours calendaires, adressé par le Responsable de Traitement au Sous-traitant conformément à l'Article 18 des CGV.

9.3 Modalités

L'audit peut prendre la forme, au choix du Responsable de Traitement :

- Audit documentaire : transmission par le Sous-traitant de ses rapports de conformité ISO 27001, certificats, politiques de sécurité, registres, et autres documents pertinents,
- Audit sur site : visite des locaux du Sous-traitant par le Responsable de Traitement ou un auditeur tiers mandaté par lui, pendant les heures ouvrées et dans le respect des règles de sécurité du site.

L'auditeur tiers éventuellement mandaté par le Responsable de Traitement doit être indépendant du Sous-traitant et de ses concurrents directs, et signer préalablement un accord de confidentialité avec le Sous-traitant.

9.4 Coûts

Les coûts de l'audit sont à la charge du Responsable de Traitement, sauf si l'audit révèle un manquement significatif du Sous-traitant à ses obligations contractuelles, auquel cas les coûts raisonnables et justifiés de l'audit sont pris en charge par le Sous-traitant.

Les prestations d'accompagnement du Sous-traitant lors de l'audit (mobilisation d'équipes, ouverture d'environnements, analyse conjointe) sont facturées au taux journalier de la TMA défini au Devis, sur bon de commande spécifique, à l'exception des prestations documentaires standard qui demeurent gratuites.

9.5 Restitution

Au terme de l'audit, le Responsable de Traitement remet au Sous-traitant une copie du rapport d'audit dans un délai raisonnable, afin de permettre la mise en œuvre des éventuelles mesures correctives.

Article 10 – Durée, Fin du Traitement et Sort des Données

10.1 Durée

Le présent DPA entre en vigueur à la date de signature du Contrat et s'applique pendant toute la durée de celui-ci.

10.2 Fin du Traitement

Au terme du Contrat, pour quelque cause que ce soit (expiration normale, résiliation anticipée, etc.), le Sous-traitant cesse tout Traitement des Données Client, sous réserve des opérations nécessaires à la restitution ou à la destruction des données conformément au présent Article 10\.

10.3 Restitution par défaut, puis destruction

Conformément à l'article 28.3.g du RGPD et au principe défini à l'Article 11 des CGV WakaStart (Réversibilité), les Données Client font, par défaut, l'objet d'une restitution au Responsable de Traitement, selon les modalités suivantes :

- Activation de la Réversibilité — Sous réserve du paiement intégral des sommes dues et de la fin de la période d'engagement initiale, conformément à l'Article 11 des CGV, le Sous-traitant met à disposition du Responsable de Traitement l'ensemble des Données Client sous un format structuré et couramment utilisé (export base de données, fichiers standard), téléchargeable via Internet.
- Période de disponibilité — Les Données Client restent disponibles à la restitution pendant une période de trente (30) jours calendaires à compter de la fin effective du Contrat.
- Destruction à l'issue de la période de restitution — À l'expiration de ce délai de trente (30) jours, le Sous-traitant procède à la destruction sécurisée et irréversible de l'ensemble des Données Client, ainsi que de leurs copies, conformément aux bonnes pratiques de son SMSI ISO 27001\.

10.4 Option de destruction immédiate

Le Responsable de Traitement peut, par demande écrite expresse adressée au Sous-traitant avant la fin du Contrat, renoncer à la restitution et demander la destruction immédiate des Données Client à la date de fin du Contrat. Cette demande est irrévocable.

10.5 Attestation de destruction

Le Sous-traitant délivre au Responsable de Traitement, sur simple demande écrite, une attestation de destruction des Données Client dans un délai de trente (30) jours ouvrés suivant la destruction effective.

10.6 Obligations légales de conservation

Par exception aux dispositions qui précèdent, le Sous-traitant est autorisé à conserver certaines Données Client au-delà des délais fixés ci-dessus lorsque la loi applicable l'y oblige (obligations comptables, réquisitions judiciaires, etc.). Dans ce cas, le Sous-traitant garantit la confidentialité des Données Client ainsi conservées et s'interdit tout Traitement ultérieur à des fins autres que celles requises par la loi.

Article 11 – Responsabilité

11.1 Renvoi aux CGV

La responsabilité des Parties au titre du présent DPA est régie par les dispositions de l'Article 9 des CGV WakaStart, sous réserve des précisions ci-après.

11.2 Exception au plafond de responsabilité

Conformément à l'Article 9.4 des CGV, les plafonds de responsabilité ne s'appliquent pas aux dommages résultant d'une violation des obligations du Sous-traitant en matière de protection des données à caractère personnel, sans préjudice des dispositions de l'article 82 du RGPD qui fixent le régime autonome de responsabilité en matière de protection des données.

11.3 Répartition des responsabilités

- Le Responsable de Traitement demeure seul responsable de la licéité, de la loyauté et de la transparence des Traitements qu'il met en œuvre via la Solution SaaS, de la pertinence et de la qualité des Données Client, de l'information et de la collecte du consentement éventuel des Personnes Concernées, du respect de la durée de conservation définie pour ses propres traitements, et de la licéité du contenu hébergé.
- Le Sous-traitant est responsable de la sécurité et de la confidentialité des Traitements qu'il met en œuvre pour le compte du Responsable de Traitement, du respect de ses instructions documentées, et des obligations spécifiques mises à sa charge par l'article 28 du RGPD et par le présent DPA.

Article 12 – Modification du DPA

Le présent DPA peut être modifié à tout moment par voie d'Avenant signé des deux Parties, notamment pour tenir compte :

- De l'évolution de la réglementation applicable à la protection des données,
- De l'activation du périmètre HDS en cours de Contrat (donnant lieu à une annexe HDS spécifique),
- De l'évolution substantielle des Traitements, des catégories de Données Client ou des finalités,
- De l'évolution des Sous-traitants Ultérieurs.

Les modifications mineures ou rédactionnelles n'affectant pas les droits substantiels des Parties peuvent être notifiées par le Sous-traitant au Responsable de Traitement, avec un préavis raisonnable, conformément à l'Article 18 des CGV, sans qu'il soit nécessaire de procéder par voie d'Avenant.

Article 13 – Langue et Juridiction

La langue originale et faisant foi du présent DPA est la langue française.

Le présent DPA est régi par le droit français. En cas de litige, les dispositions de l'Article 12 des CGV relatives à la loi applicable et à la juridiction compétente s'appliquent.

Annexe 1 – Description du Traitement

A.1.1 Nature et finalité des Traitements

Le Sous-traitant effectue, pour le compte du Responsable de Traitement, les opérations de Traitement suivantes :

- Hébergement des Données Client sur son infrastructure cloud sous-traitée auprès d'OVH,

- Stockage, sauvegarde et restauration des Données Client conformément aux niveaux de service définis à l'Article 13 des CGV,
- Mise à disposition et consultation des Données Client par les Utilisateurs autorisés par le Responsable de Traitement, via l'interface de la Solution SaaS,
- Transmission des Données Client entre les composants techniques de la Solution SaaS et, le cas échéant, avec des systèmes tiers connectés selon les Spécifications,
- Support technique et opérations de maintenance (corrective, évolutive, adaptative) de la Solution SaaS,
- Enregistrement des logs d'accès, d'activité et de sécurité aux fins de traçabilité.

Finalité principale — Permettre au Responsable de Traitement l'exploitation de la Solution SaaS développée et hébergée pour son compte, dans les conditions prévues au Contrat.

A.1.2 Catégories de Personnes Concernées

Compte tenu de la nature hautement variable des applications SaaS développées par le Sous-traitant, les catégories de Personnes Concernées dépendent de l'usage métier spécifique du Responsable de Traitement. Elles peuvent notamment inclure, selon les cas :

- Les Utilisateurs finaux de la Solution SaaS (employés, collaborateurs, prestataires du Responsable de Traitement),
- Les clients et prospects du Responsable de Traitement,
- Les partenaires commerciaux du Responsable de Traitement,
- Toute autre catégorie de personnes physiques concernée par l'activité métier du Responsable de Traitement.

Le Responsable de Traitement assume la pleine responsabilité de l'identification précise des catégories de Personnes Concernées au titre de son propre registre des traitements.

A.1.3 Catégories de Données Client

Les catégories de Données Client hébergées varient selon la nature fonctionnelle de la Solution SaaS commandée et peuvent notamment inclure :

- Données d'identification : nom, prénom, civilité, identifiants,
- Données de contact : email, téléphone, adresse postale,
- Données professionnelles : fonction, organisation d'appartenance, secteur d'activité,
- Données de connexion et de navigation : adresse IP, identifiants de session, horodatage, logs d'accès et d'activité,
- Données métier spécifiques saisies ou téléversées par le Responsable de Traitement et ses Utilisateurs dans la Solution SaaS selon l'usage fonctionnel prévu aux Spécifications,
- Données financières le cas échéant (identifiants bancaires, factures), hors données de paiement sensibles qui ne sont pas hébergées dans la Solution SaaS.

Données sensibles — Le Sous-traitant ne procède pas, par défaut, au Traitement de données sensibles au sens de l'article 9 du RGPD. Le Traitement de Données de Santé est strictement conditionné à l'activation du périmètre HDS prévue à l'Article 3.2 des CGV.

A.1.4 Durée des Traitements

Les Traitements sont effectués pendant toute la durée du Contrat, puis cessent conformément à l'Article 10 du présent DPA.

Annexe 2 – Mesures Techniques et Organisationnelles

Le Sous-traitant met en œuvre les mesures techniques et organisationnelles suivantes, dans le cadre de son SMSI certifié ISO 27001, pour garantir la sécurité des Traitements au sens de l'article 32 du RGPD.

A.2.1 Mesures organisationnelles

- Politique de sécurité de l'information formalisée et révisée périodiquement,
- Désignation d'un Responsable de la Sécurité des Systèmes d'Information (RSSI) et d'une Déléguée à la Protection des Données (DPO),
- Sensibilisation et formation régulières du personnel aux enjeux de sécurité et de protection des données,
- Engagements de confidentialité signés par l'ensemble des collaborateurs ayant accès aux Données Client,
- Politique de gestion des droits d'accès selon le principe du besoin d'en connaître (need-to-know),
- Procédures de gestion des incidents de sécurité et des Violations de Données, documentées et testées.

A.2.2 Mesures techniques

- Chiffrement des Données Client au repos et en transit (protocoles TLS en vigueur, chiffrement de la base de données),
- Authentification forte des comptes d'administration et des accès privilégiés,
- Cloisonnement logique des environnements entre Clients dans l'architecture mutualisée SaaS,
- Supervision et détection d'intrusion sur les infrastructures hébergeant les Données Client,
- Sauvegardes quotidiennes avec rétention minimale de 30 jours glissants, conformément à l'Article 13.4 des CGV,
- Plan de continuité et de reprise d'activité (PCA/PRA) testé périodiquement,
- Tests d'intrusion (Pentests) réalisés conformément à l'Article 7.3 des CGV.

A.2.3 Mesures applicables au périmètre HDS

Dans l'hypothèse où le périmètre HDS est activé au sens de l'Article 3.2 des CGV, les mesures ci-dessus sont complétées par les exigences spécifiques du référentiel HDS en vigueur, notamment :

- Hébergement chez un hébergeur certifié HDS,
- Mesures renforcées de traçabilité et d'auditabilité,
- Procédures spécifiques de gestion des incidents impliquant des Données de Santé,
- Formation spécifique des personnels amenés à intervenir sur les Données de Santé.

Le détail des mesures HDS applicables est formalisé dans un avenant HDS au présent DPA, signé concomitamment à l'activation du périmètre HDS.

A.2.4 Documentation complémentaire

Le détail complet et actualisé des mesures techniques et organisationnelles mises en œuvre par le Sous-traitant est consigné dans son SMSI ISO 27001 et est tenu à la disposition du Responsable de Traitement dans le cadre du droit d'audit prévu à l'Article 9 du présent DPA.

Annexe 3 – Liste des Sous-traitants Ultérieurs

A.3.1 Sous-traitant Ultérieur principal

| Sous-traitant Ultérieur | Rôle | Localisation | Garanties |

| ----- | ----- | ----- | ----- |
| OVH (OVHcloud) | Fournisseur d'hébergement et d'infrastructure cloud | France / Union Européenne | ISO 27001, ISO 27017, ISO 27018, HDS (selon offre), contrat DPA OVH conforme à l'article 28 RGPD |

A.3.2 Autres Sous-traitants Ultérieurs

Les partenaires et prestataires directs de JDS CONSEIL intervenant ponctuellement sur l'exécution de prestations techniques (développement, support, maintenance, surveillance de sécurité) sont tous liés par un contrat sécurisé intégrant :

- Des engagements de confidentialité,
- Des obligations conformes à l'article 28 du RGPD,
- Des engagements de sécurité de l'information alignés sur le référentiel ISO 27001 de JDS CONSEIL.

La liste actualisée et nominative des Sous-traitants Ultérieurs est tenue à la disposition du Responsable de Traitement sur simple demande écrite adressée à dpo@wakastellar.com.

Annexe 4 – Conditions particulières HDS (conditionnellement activable)

L'Annexe 4 — Conditions particulières HDS s'applique de plein droit lorsque le périmètre HDS est expressément activé au Devis conformément à l'Article 3.2 des CGV WakaStart.

Cette annexe précise notamment :

- Les engagements de l'Hébergeur au titre de la Certification HDS de JDS CONSEIL,
- Les mesures de protection et de sécurisation renforcées des DSCP,
- Le délai de notification des Violations de Données renforcé à vingt-quatre (24) heures pour les DSCP,
- Les Sous-Traitants Ultérieurs certifiés HDS (dont OVH Gravelines et Strasbourg),
- Les modalités spécifiques de réversibilité et de destruction (dont le crypto-shredding),
- Les SLO HDS (disponibilité 99,9 %, RTO/RPO PCA/PRA spécifiques),
- Le plafond de responsabilité spécifique au périmètre HDS.

En cas de contradiction entre les dispositions générales du présent DPA et l'Annexe 4 pour toute question portant sur les DSCP, les dispositions de l'Annexe 4 prévalent.

L'Annexe 4 fait l'objet d'un document séparé (Annexe-HDS-WakaStart.md), joint au Contrat lors de l'activation du périmètre HDS et tenu à disposition sur simple demande écrite.

Document contractuel — JDS CONSEIL

DPA HDS — WakaStart v1.0

dpa-hds · Version 1.0 · en vigueur depuis le 28 avril 2026

Annexe conditionnellement activable au Data Processing Agreement (DPA) WakaStart, applicable lorsque le périmètre HDS est expressément activé au Devis conformément à l'Article 3.2 des CGV WakaStart

Entrée en vigueur le 15 avril 2026

Conclu en application des articles L.1111-8 et R.1111-8-8 à R.1111-9-11 du Code de la Santé Publique, de la Réglementation Applicable HDS en vigueur et de l'article 28 du RGPD

Identification du Prestataire certifié HDS

JDS CONSEIL — Société par Actions Simplifiée (SAS), opérant sous la marque commerciale WakaStellar pour l'ensemble de ses produits et modules de la gamme Waka (dont WakaStart, Waka HDS, WakaSign, WakaSeal, WakaInvoice).

- Capital social : 440 760 € (après réduction du 30/12/2024)
- Siège social : Parc d'Activité de Tournebride, 44118 LA CHEVROLIÈRE, France
- RCS : Nantes 529 773 368
- SIRET : 529 773 368 00012
- Code APE/NAF : 6420Z
- N° TVA intracommunautaire : FR45 529 773 368
- Présidente : Jannick SCHIRRA
- Directeur Général : Denis SCHIRRA
- Site web : www.wakastellar.com
- Contact contractuel : contact@wakastellar.com

Déléguée à la Protection des Données (DPO) :

- Florelle SCHIRRA, désignée auprès de la CNIL.
- Adresse postale : 17, rue de la Guillauderie, 44118 LA CHEVROLIÈRE, France
- Email dédié : dpo@wakastellar.com

Ci-après dénommée « JDS CONSEIL » ou le « Responsable de Traitement ». Le terme « WakaStellar » désigne la marque commerciale sous laquelle JDS CONSEIL opère ses produits ; il ne désigne aucune entité juridique distincte de JDS CONSEIL..

Article 1 – Préambule et Objet

1.1 Contexte

Les Parties sont liées par les CGV WakaStart (Article 3.2 — Périmètre de certification applicable), qui prévoient que la certification HDS ne s'applique à la Solution SaaS que si elle est expressément mentionnée au Devis ou formalisée par un Avenant ultérieur signé des deux Parties.

La présente Annexe constitue les conditions particulières applicables au traitement de Données de Santé à Caractère Personnel (DSCP) dans la Solution SaaS, lorsque le périmètre HDS a été activé conformément aux CGV.

Elle s'ajoute aux dispositions du DPA principal et aux autres documents contractuels sans les remplacer, tout en introduisant les obligations spécifiques imposées par la Réglementation Applicable HDS.

1.2 Activation conditionnelle

La présente Annexe ne produit ses effets qu'à compter de l'activation effective du périmètre HDS au Devis ou par Avenant. En l'absence d'activation HDS, l'hébergement de DSCP dans la Solution SaaS est strictement interdit conformément à l'Article 3.2 des CGV, et la présente Annexe demeure inopérante.

1.3 Objet

La présente Annexe a pour objet :

- (i) De préciser les conditions particulières dans lesquelles JDS CONSEIL, agissant en qualité d'Hébergeur de DSCP et de Sous-traitant RGPD, met à disposition du Client la Solution SaaS dans son périmètre HDS,
- (ii) De satisfaire aux exigences spécifiques du référentiel HDS en vigueur et du Code de la Santé Publique,
- (iii) De définir les mesures de protection et de sécurisation renforcées des DSCP, ainsi que les objectifs de performance et de niveau de service applicables au périmètre HDS.

1.4 Articulation avec les autres documents contractuels

La présente Annexe s'articule avec les autres documents composant le Contrat, conformément à l'Article 8.5 des CGV WakaStart, avec la précision suivante :

En cas de contradiction portant sur le traitement de DSCP dans le périmètre HDS activé, les dispositions de la présente Annexe prévalent, sans préjudice des dispositions impératives de la Réglementation Applicable HDS et du RGPD.

Pour toute autre question non spécifiquement régie par la présente Annexe, les dispositions du DPA principal, des CGU, de la Charte de Confidentialité et des CGV s'appliquent dans leur priorité normale.

1.5 Définitions complémentaires

Les termes employés avec une majuscule initiale dans la présente Annexe ont la signification qui leur est donnée à l'Article 2 des CGV WakaStart et à l'Article 1.4 du DPA principal, complétés par les définitions spécifiques suivantes :

- « API » — Application Programming Interface. Ensemble des méthodes et protocoles permettant au Client d'interagir par programme avec la Solution SaaS, notamment via une interface de type S3 pour le Service de Stockage Objet.
- « Certification HDS » — Certification Hébergeur de Données de Santé délivrée selon les exigences et les critères du Code de la Santé Publique (article L.1111-8) afférents à la prestation d'hébergement de DSCP sur support numérique, ainsi que de ses textes d'application.
- « Clés d'Accès » — Identifiants fournis par l'Hébergeur au Client permettant au Client de s'authentifier auprès de l'API de la Solution SaaS. Ces identifiants personnels, sécurisés et uniques prennent la forme d'une clé d'accès combinée à une clé secrète.
- « DSCP » (Données de Santé à Caractère Personnel) — Toute donnée à caractère personnel relative à la santé physique ou mentale, passée, présente ou future, d'une personne physique, recueillie à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social, au sens de l'article 4.15 du RGPD et de l'article L.1111-8 du Code de la Santé Publique. Les DSCP constituent une sous-catégorie des Données Client au sens du DPA.
- « Données Sources » — Données que le Client téléverse dans la Solution SaaS dans le cadre spécifique du périmètre HDS. Les Données Sources sont des DSCP.
- « Hébergeur » — JDS CONSEIL agissant en qualité d'hébergeur de DSCP au sens du Code de la Santé Publique, titulaire de la Certification HDS pour la Solution SaaS. L'Hébergeur est également Sous-traitant au sens du RGPD.

- « Objet » — Unité de base de stockage de la Donnée Source gérée par l'Hébergeur par l'intermédiaire de la Solution SaaS. L'Objet est généré lors du téléversement de la Donnée Source dans la Solution SaaS et correspond à une entité unique chiffrée donnant accès à la Donnée Source par l'intermédiaire d'une clé d'identification unique.
- « Réglementation Applicable HDS » — Ensemble des textes législatifs et réglementaires applicables en France à l'activité d'hébergement de DSCP, incluant notamment les articles L.1111-8, R.1111-8-8 et R.1111-9 à R.1111-11 du Code de la Santé Publique, les référentiels de Certification HDS en vigueur, le RGPD, la loi n° 78-17 du 6 janvier 1978 modifiée, ainsi que leurs textes d'application et doctrines de l'Agence du Numérique en Santé (ANS) et de la CNIL.
- « Service de Stockage Objet » — Infrastructure virtuelle sécurisée, certifiée HDS, consistant en la mise à disposition de la Solution SaaS au Client, lui permettant de stocker et gérer les Données Sources sous la forme d'Objets via une API de type S3.
- « SLO » (Service Level Objective) — Objectif de niveau de service, tel que défini à l'Annexe 4-Bis de la présente Annexe.
- « Sous-traitant Ultérieur RGPD certifié HDS » — Sous-traitant Ultérieur au sens de l'Article 7 du DPA principal, disposant de sa propre Certification HDS pour les activités qui lui sont déléguées.
- « Utilisateurs Finaux » — Personnes physiques destinataires finales des services développés par le Client sur la base de la Solution SaaS, typiquement des professionnels de santé ou des patients, sous la responsabilité exclusive du Client.

Article 2 – Certificat HDS

2.1 Titulaire et périmètre de la Certification

La Certification HDS est délivrée à JDS CONSEIL (RCS Nantes 529 773 368), qui en est l'unique titulaire. Elle couvre le Système de Management de la Sécurité de l'Information (SMSI) mis en œuvre par JDS CONSEIL pour l'ensemble de ses produits de la gamme Waka, dont WakaStart.

2.2 Périmètre couvert par la certification

Le périmètre de certification couvre directement, pour JDS CONSEIL, les activités HDS suivantes (citation du référentiel de Certification HDS) :

- Activité n° 4 — Mise à disposition et maintien en condition opérationnelle de l'infrastructure logicielle,
- Activité n° 5 — Administration et exploitation du système d'information contenant les données de santé,
- Activité n° 6 — Sauvegarde des données de santé.

Les activités complémentaires sont assurées par des Sous-Traitants Ultérieurs certifiés HDS (cf. Article 8 de la présente Annexe) :

- Activité n° 1 — Mise à disposition et maintien en condition opérationnelle de sites physiques hébergeant l'infrastructure matérielle,
- Activité n° 2 — Mise à disposition et maintien en condition opérationnelle de l'infrastructure matérielle,
- Activité n° 3 — Mise à disposition et maintien en condition opérationnelle de l'infrastructure virtuelle.

L'ensemble de la chaîne d'hébergement des DSCP est ainsi couvert par des certifications HDS contractuellement chaînées.

2.3 Coordonnées du certificat

À la date d'entrée en vigueur de la présente Annexe, la Certification HDS de JDS CONSEIL est en cours d'obtention. Les coordonnées du certificat (numéro, date de délivrance, date de renouvellement, organisme certificateur) seront renseignées au Client dès la délivrance effective par un complément à la présente Annexe, sans qu'il soit nécessaire de procéder par voie d'Avenant.

Jusqu'à la délivrance effective de la Certification HDS, l'activation du périmètre HDS dans un Devis demeure conditionnée à la confirmation par JDS CONSEIL de la capacité opérationnelle à accueillir des DSCP dans les conditions de la présente Annexe, par recours à des Sous-Traitants Ultérieurs déjà certifiés HDS.

2.4 Accès à la documentation

Le Client reconnaît expressément avoir accès, à tout moment :

- Au certificat HDS dès sa délivrance, dans la base documentaire accessible sur le site internet de l'Hébergeur à l'adresse : https://www.wakastellar.com/nos-modules/waka-hds,
- Aux documents internes en lien avec l'activité ou la Certification HDS, via l'interface d'administration de la Solution SaaS, accessible avec des identifiants d'administration.

2.5 Maintien, veille et notification en cas de perte de certification

Maintien — Pendant toute la durée du Contrat, l'Hébergeur déploie ses meilleurs efforts pour maintenir en vigueur la Certification HDS conformément au périmètre énoncé au 2.2. L'Hébergeur réalise une veille trimestrielle du statut de sa propre certification et de celle de ses Sous-Traitants Ultérieurs certifiés HDS, auprès de l'Agence du Numérique en Santé (ANS).

Procédure en cas de non-renouvellement, perte ou suspension — En cas de non-renouvellement, perte ou suspension de la Certification HDS de l'Hébergeur ou de l'un de ses Sous-Traitants Ultérieurs certifiés HDS critiques, l'Hébergeur s'engage à :

- (a) Information immédiate : notifier le Client par écrit dans un délai maximum de quarante-huit (48) heures suivant la connaissance de la perte ou suspension, avec mention de la nature de l'événement, du périmètre concerné, et de l'impact potentiel sur les DSCP du Client,
- (b) Plan de remédiation : communiquer au Client un plan de remédiation dans les quinze (15) jours calendaires suivant la notification, précisant les actions correctives envisagées et le délai estimé de rétablissement,
- (c) Migration vers Hébergeur alternatif : si le délai de rétablissement est supérieur à trois (3) mois, ou si la certification est définitivement retirée, l'Hébergeur active son plan de migration vers un hébergeur HDS alternatif certifié, identifié préalablement dans son dispositif de continuité. Les frais de migration sont à la charge exclusive de l'Hébergeur,
- (d) Continuité de service : pendant toute la durée de la procédure de remédiation ou de migration, l'Hébergeur maintient des mesures techniques et organisationnelles équivalentes aux exigences HDS,
- (e) Transmission à l'ANS : l'Hébergeur transmet sans délai à l'Agence du Numérique en Santé la liste des Clients HDS concernés, conformément aux exigences réglementaires.

Résiliation — En cas de perte définitive de la Certification HDS, le Client est en droit de résilier le Contrat relatif au périmètre HDS, sans pénalité, avec un préavis de trente (30) jours calendaires à compter de la notification prévue au (a) ci-dessus. Dans ce cas, l'Hébergeur met en œuvre la procédure de réversibilité définie à l'Article 7 à ses frais exclusifs.

Article 3 – Référent contractuel et points de contact HDS

Le Client désigne, dès l'entrée en vigueur du périmètre HDS, un référent contractuel HDS chargé du traitement des incidents ayant un impact sur les DSCP. Le référent est renseigné et tenu à jour par le Client dans l'interface d'administration de la Solution SaaS, et communiqué à l'Hébergeur

conformément à l'Article 4.2 des CGU.

L'Hébergeur tient une liste active et à jour des référents contractuels HDS, afin de garantir, en cas de suspension ou de retrait de la Certification HDS, sa capacité à la transmettre sans délai à l'autorité compétente (ANS, CNIL), conformément aux exigences réglementaires.

Article 4 – Descriptif du Service HDS

4.1 Finalité

Lorsque le périmètre HDS est activé, la Solution SaaS fournit au Client :

- (a) Un Service de Stockage Objet permettant de stocker et gérer les Données Sources sous forme d'Objets via des appels à une API de type S3,
- (b) Le support technique associé tel que décrit à l'Annexe 4-Bis.

La Solution SaaS, dans son périmètre HDS, accepte les Données Sources aux formats natifs définis au Devis (notamment PDF).

Les capacités techniques comprennent : la scalabilité dans la limite du volume maximum défini au Contrat, l'accès aux Objets par des méthodes sécurisées d'authentification et d'autorisation, la durabilité et la résilience des Objets par un mécanisme de redondance et de réplication.

La Solution SaaS, dans son périmètre HDS, n'a pas vocation à constituer un service d'archivage électronique au sens de la norme NF Z42-013 ou équivalent.

4.2 Traitements opérés

Étape 1 — Pseudonymisation et indexation des Données Sources

Le Client transmet les Données Sources en clair à l'API de l'Hébergeur. Avant leur dépôt dans le Service de Stockage Objet, l'API effectue les opérations suivantes :

- Chiffrement : les Données Sources sont chiffrées au moyen d'une clé AES-256-GCM unique et dédiée à chaque Client, gérée par le KMS interne de l'Hébergeur (Infisical / OpenBao Transit Engine selon les modules),
- Pseudonymisation des identifiants pour l'indexation : des index de métadonnées non sensibles sont générés pour garantir la confidentialité et l'efficacité de la recherche. Aucune donnée nominative brute n'est conservée en clair dans le moteur de recherche externe.

Étape 2 — Stockage des Objets

Une fois l'Étape 1 accomplie, les Données Sources sont converties en Objets et versées dans le Service de Stockage Objet. Le Service de Stockage Objet ne contient ou ne conserve aucune information afférente au contenu sensible, notamment nominatif, des Données Sources.

Étape 3 — Gestion des Objets

Le Client dispose d'un accès aux Objets pour les besoins de mise en œuvre de son propre service à destination des Utilisateurs Finaux.

Les traitements opérés par l'Hébergeur portent uniquement sur les Objets et les métadonnées techniques générées à l'Étape 1, nécessaires au fonctionnement de la Solution SaaS et à la conformité à ses obligations en matière de continuité et reprise d'activité, de journalisation, de traçabilité et d'audit.

À titre d'information, les métadonnées techniques se présentent sous la forme d'identifiants uniques GUID, client_id, horodatages, ou identifiants pseudonymisés/hachés.

4.3 Mesures de protection et de sécurisation des DSCP

Conformément à la Réglementation Applicable HDS, la mise à disposition de la Solution SaaS dans le périmètre HDS comporte les mesures spécifiques suivantes :

- Sécurité de l'infrastructure : chiffrement en transit (TLS) et au repos, mise en œuvre des mesures techniques et organisationnelles du référentiel ISO 27001 en vigueur,
- Localisation du stockage : les Objets sont stockés exclusivement sur des sites physiques situés en France métropolitaine,
- Continuité et reprise d'activité : réplication des Objets stockés sur un site de secours situé en France métropolitaine, dans le cadre du Plan de Continuité et de Reprise d'Activité (PCA/PRA) dont les objectifs RTO et RPO sont définis à l'Annexe 4-Bis,
- Traçabilité et journalisation : conservation dans des journaux consultables par le Client sur demande de l'ensemble des appels effectués à l'API (horodatage, identifiant client, identifiant utilisateur, adresse IP source, type d'opération : dépôt, récupération, suppression),
- Souveraineté et transparence : l'Hébergeur et ses Sous-Traitants Ultérieurs listés à l'Article 8 ne sont soumis à aucune législation d'un pays tiers à l'Espace Économique Européen susceptible d'imposer un accès aux DSCP non autorisé par le droit français,
- Réversibilité : la Solution SaaS inclut la fonctionnalité correspondante permettant d'extraire les Données Sources, dans les conditions de l'Article 7,
- Sensibilisation des personnels : les personnels de l'Hébergeur impliqués dans la mise en œuvre de la Solution SaaS dans son périmètre HDS font l'objet d'actions de sensibilisation régulières, notamment sur le caractère sensible des DSCP et la criticité associée,
- Encadrement des Sous-Traitants Ultérieurs : l'Hébergeur établit un cahier des charges, contractualise et opère le suivi de la sous-traitance conformément à la Réglementation Applicable HDS,
- Traçabilité des accès administrateurs : l'Hébergeur communique au Client, à sa demande et dans le cadre des audits prévus à l'Article 9 ou en cas de suspicion d'accès non autorisé, les traces spécifiques d'accès aux systèmes de traitement des Objets effectuées par le personnel de l'Hébergeur dûment habilité (accès administrateurs), conformément à l'exigence EXI15 du référentiel HDS.

4.4 Évolutions de la Solution SaaS dans le périmètre HDS

Les mises à jour de la Solution SaaS (techniques ou réglementaires) sont réalisées conformément à l'Article 3.3 des CGV (Évolution des référentiels) et sous réserve du devoir d'information défini à l'Article 6.6 de la présente Annexe.

En cas d'évolution ayant pour effet (a) de dégrader le niveau de service, (b) de réduire les garanties définies au Contrat, ou (c) d'augmenter le Prix applicable au périmètre HDS, l'Hébergeur recueille l'accord écrit et préalable du Client conformément à la Réglementation Applicable HDS.

Article 5 – Engagements réciproques des Parties

Pendant toute la durée du Contrat, les Parties s'engagent à fournir leurs meilleurs efforts pour :

- (a) Collaborer, et
- (b) Déployer tous moyens raisonnables, dans l'objectif de maintenir l'intégrité de la chaîne de sécurité définie pour protéger les DSCP, chacune dans le respect et la limite de ses obligations et responsabilités afférentes aux termes du Contrat.

Article 6 – Engagements et obligations de l'Hébergeur

D'une manière générale, l'Hébergeur s'engage à garantir la disponibilité, l'intégrité, la confidentialité et l'auditabilité des DSCP hébergées, dans les conditions et limites définies au Contrat, dans le cadre d'une obligation générale de moyens, sans préjudice de toute disposition impérative de la loi française

mettant à sa charge une obligation de résultat.

6.1 Mise à disposition de la Solution SaaS

La prestation de l'Hébergeur consiste à mettre la Solution SaaS à la disposition du Client dans son périmètre HDS conformément aux termes du Contrat.

En conséquence, le Client demeure seul responsable tant vis-à-vis de l'Hébergeur que des Utilisateurs Finaux et des tiers de :

- (a) Le développement,
- (b) La mise en œuvre,
- (c) La gestion et
- (d) La sécurité des applications de santé ou des services métier qu'il choisit de faire interagir avec la Solution SaaS.

6.2 Sous-traitance

L'Hébergeur est autorisé à recourir aux Sous-Traitants Ultérieurs certifiés HDS listés à l'Article 8 de la présente Annexe, conformément à l'Article 7 du DPA principal.

Le Client autorise expressément et sans réserve ce recours. Tout nouveau Sous-Traitant Ultérieur certifié HDS ou modification substantielle de la chaîne de sous-traitance HDS est soumis à la procédure de notification et d'opposition prévue à l'Article 7.3 du DPA principal.

6.3 Accès aux Données Sources et traitements autorisés

L'Hébergeur, en qualité de Sous-traitant RGPD et d'Hébergeur HDS, effectue uniquement les traitements confiés par le Client dans le cadre du Contrat, strictement nécessaires à l'exécution de l'activité d'hébergement des DSCP et à leur sécurisation :

- Chiffrement des Données Sources (AES-256-GCM) et pseudonymisation des identifiants pour l'indexation,
- Stockage des Objets,
- Réplication des Objets conformément au PCA/PRA,
- Extraction des Objets dans les cas prévus à l'Article 7 ou en cas de Force Majeure.

L'Hébergeur s'interdit formellement :

- D'accéder, traiter ou visualiser le contenu nominatif en clair des DSCP,
- Tout usage des Objets à des fins autres que celles indispensables à l'exécution du Contrat,
- Toute cession à titre onéreux des Objets ou des Données Sources, même sur instruction du Client.

Il est expressément convenu que le Client demeure le Responsable de Traitement au sens du RGPD, conservant la pleine responsabilité de la finalité et des moyens du traitement, y compris pour les demandes d'exercice des droits des Personnes Concernées.

6.4 Notification renforcée des violations de données DSCP

Par dérogation à l'Article 5.1 du DPA principal qui prévoit un délai de notification de quarante-huit (48) heures pour les Violations de Données ordinaires, le délai de notification est ramené à vingt-quatre (24) heures pour les Violations de Données affectant des DSCP, conformément à l'article 33 du RGPD et aux exigences renforcées du référentiel HDS.

Cette notification est adressée par écrit au référent contractuel HDS désigné à l'Article 3 et au DPO du Client, par email sécurisé, et comprend obligatoirement :

- (a) La nature de la violation (accès non autorisé, perte, destruction, altération),
- (b) Les catégories et le volume approximatif de DSCP concernées,

- (c) L'identifiant des Objets ou vaults potentiellement impactés, si disponible,
- (d) Les coordonnées du DPO de l'Hébergeur,
- (e) Les mesures déjà prises ou envisagées pour remédier à la violation et en limiter les conséquences,
- (f) Les éléments de preuve disponibles (traces d'audit, logs d'accès).

Si toutes les informations ne sont pas disponibles dans ce délai, l'Hébergeur communique une notification provisoire dans les 24 heures et complète les informations au fur et à mesure sans délai injustifié.

Le délai de 48 heures du DPA principal demeure applicable aux Violations de Données portant sur des données à caractère personnel qui ne seraient pas des DSCP.

6.5 Devoir de conseil et de mise en garde

Le devoir de conseil et de mise en garde de l'Hébergeur se limite exclusivement aux sujets techniques standards relatifs à l'utilisation de la Solution SaaS en mode SaaS par le Client.

L'Hébergeur n'est tenu à aucun devoir de conseil ou de mise en garde vis-à-vis du Client dans les domaines suivants :

- Dans le cadre de l'activité métier propre du Client (applications de santé développées par le Client),
- Sur les plans juridique et réglementaire relatifs à l'activité de soins ou aux obligations des professionnels de santé.

6.6 Devoir d'information et de transparence

Publication des garanties HDS — Conformément à la Réglementation Applicable HDS, l'Hébergeur publie, tient à jour et rend accessible au public, dans la base documentaire accessible sur son site internet à l'adresse https://www.wakastellar.com/nos-modules/waka-hds, le tableau standard des « garanties » tel que défini dans le référentiel de Certification HDS.

Information sur les évolutions — L'Hébergeur informe le Client par tout moyen de toute évolution de la Solution SaaS définie à l'Article 4.4 dans les seuls cas où ladite évolution aurait pour effet :

- (a) De dégrader le niveau de service,
- (b) De réduire les garanties définies au Contrat, et/ou
- (c) D'augmenter le Prix applicable au périmètre HDS.

Accord préalable requis — Dans les cas prévus par la Réglementation Applicable HDS, l'Hébergeur s'engage à obtenir l'accord écrit et préalable du Client avant toute mise en œuvre d'évolution au titre de (a) ou (b) ci-dessus, d'intégration d'un nouveau Sous-Traitant Ultérieur certifié HDS, ou de transfert de données hors de France.

En l'absence d'accord du Client transmis à l'Hébergeur dans un délai de quinze (15) jours calendaires à compter de l'information préalable, les Parties pourront se référer aux dispositions de réversibilité de l'Article 7\.

Notification des violations de données — La notification des violations de données affectant des DSCP est régie par l'Article 6.4 ci-dessus.

Article 7 – Réversibilité des Données Sources et destruction

7.1 Principe et champ d'application

L'Hébergeur s'engage à restituer au Client l'intégralité des Données Sources stockées sous forme d'Objets dans la Solution SaaS à la fin du Contrat, y compris en cas de rupture anticipée, quel qu'en soit le motif.

La restitution porte exclusivement sur les Objets effectivement stockés dans le Service de Stockage Objet à la date de fin du Contrat ou de rupture anticipée, à l'exclusion des Objets effacés ou détruits par le Client antérieurement.

Articulation avec l'Article 11 des CGV — La présente Article 7 constitue le mécanisme de Réversibilité spécifique applicable aux Données Sources dans le périmètre HDS. Il complète les dispositions générales de l'Article 11 des CGV (Réversibilité des Données Client) et prévaut en cas de contradiction pour les Données Sources relevant du périmètre HDS.

7.2 Mise en œuvre standard

La Solution SaaS, dans son périmètre HDS, est dotée d'une fonctionnalité de réversibilité autonome permettant au Client d'effectuer lui-même l'extraction des Données Sources dans un format standard, lisible et exploitable.

À compter de la date de fin du Contrat ou de rupture anticipée :

- L'Hébergeur restreint de plein droit les droits d'accès et d'utilisation de la Solution SaaS conférés au Client, qui ne bénéficiera plus que d'un droit en lecture seule,
- Le Client bénéficie d'un délai maximum de trente (30) jours calendaires pour effectuer l'intégralité de l'extraction.

Au plus tard au terme de ce délai, le Client fait parvenir à l'Hébergeur un procès-verbal de récupération attestant de l'accomplissement de l'opération de réversibilité.

7.3 Formats de restitution

Les Données Sources sont restituées dans les formats suivants, au choix du Client :

- Documents : format natif d'origine (PDF ou autre défini au Devis),
- Métadonnées et index : format JSON ou CSV (standard, lisible, exploitable sans logiciel propriétaire),
- Export complet : archive chiffrée au format standard, accompagnée d'une clé de déchiffrement communiquée séparément via canal sécurisé.

7.4 Traitement des Données Sources répliquées

À réception du procès-verbal de récupération et sauf demande spécifique du Client formulée par écrit au plus tard à la date de fin du Contrat, l'Hébergeur procède à l'effacement irréversible de l'intégralité des Données Sources répliquées sur le site de secours dans le cadre du PCA/PRA.

Au terme de cette opération, l'Hébergeur fournit une attestation de destruction au Client, attestant également de la fin du processus de réversibilité.

7.5 Destruction logique par crypto-shredding (droit à l'oubli RGPD)

Dans le cadre d'une demande d'exercice du droit à l'effacement d'un Utilisateur Final (article 17 RGPD), et lorsque les Données Sources concernées sont soumises à des obligations légales de rétention (notamment les obligations de conservation des données de santé), l'Hébergeur met en œuvre un mécanisme de crypto-shredding consistant en la révocation de la clé de chiffrement propre à l'Utilisateur Final concerné, gérée par le KMS interne de l'Hébergeur.

Ce mécanisme rend les Données Sources définitivement inaccessibles et inutilisables sans suppression physique des Objets chiffrés, conciliant ainsi le droit à l'oubli RGPD avec les obligations légales de conservation HDS.

La révocation de clé est irréversible et journalisée.

7.6 Procès-verbal de destruction

À l'issue de toute opération de destruction définitive des Données Sources (fin de Contrat, résiliation anticipée, crypto-shredding sur demande), l'Hébergeur fournit au Client un procès-verbal de

destruction signé par le RSSI de l'Hébergeur, comprenant :

- La date et l'heure de l'opération,
- L'identité de l'intervenant ayant réalisé l'opération,
- La liste des Objets ou vaults détruits (par identifiants techniques, sans contenu sensible),
- Le mécanisme de destruction utilisé (suppression physique ou crypto-shredding),
- L'attestation que toutes les copies répliquées ont également été détruites ou rendues inaccessibles.

Ce procès-verbal est fourni dans un délai maximum de quinze (15) jours ouvrés suivant la destruction effective.

7.7 Prix et prestations complémentaires

L'extraction standard des Données Sources est incluse dans les fonctionnalités de la Solution SaaS. Aucun supplément n'est facturé en cas de mise en œuvre conforme au présent Article.

Toutefois, si l'opération nécessite l'intervention de l'Hébergeur — notamment demande d'assistance complémentaire, fourniture d'un support spécifique, restitution dans un format non standard —, l'Hébergeur soumettra au Client un devis préalable au taux journalier de la TMA défini au Devis, sous réserve de faisabilité technique.

7.8 Défaut de mise en œuvre par le Client

Si le Client ne s'exécute pas conformément au présent Article ou n'est pas en mesure de s'y conformer, et après relance écrite restée infructueuse sous trente (30) jours calendaires à compter de l'envoi d'une mise en demeure, l'Hébergeur pourra prendre toutes les mesures utiles aux frais exclusifs du Client ou de ses ayants-droits dans l'intérêt de la préservation des Données Sources.

Ces mesures pourront inclure, sous l'autorité de la DPO de l'Hébergeur et après notification à l'autorité compétente (CNIL), le dépôt des Données Sources chiffrées chez un tiers séquestre ou un organisme d'entiercement désigné par l'Hébergeur, afin de garantir la pérennité du traitement pour les ayants-droits du Client ou les Utilisateurs Finaux, aux frais exclusifs du Client.

Article 8 – Sous-Traitants Ultérieurs HDS

8.1 Liste des Sous-Traitants Ultérieurs certifiés HDS

L'Hébergeur fait appel aux Sous-Traitants Ultérieurs suivants, tous certifiés HDS, ce que le Client reconnaît et accepte expressément :

Rôle	Sous-Traitant Ultérieur	Localisation	Activités HDS
Datacenter de Production	OVH / GRAVELINES — OVH GROUPE, siège 2 rue Kellermann 59100 ROUBAIX	ZI des Huttes — Route de la ferme Masson, 59820 GRAVELINES	Activités n° 1, 2, 3
Datacenter de Secours	OVH / STRASBOURG — OVH GROUPE, siège 2 rue Kellermann 59100 ROUBAIX	9 rue du Bassin de l'Industrie, 67000 STRASBOURG	Activités n° 1, 2, 3
Opérateurs Réseau	OVH GROUPE, siège 2 rue Kellermann 59100 ROUBAIX	France	Réseau

8.2 Évolution de la liste

En cas de déménagement sur le territoire français ou de modification des coordonnées des Sous-Traitants Ultérieurs, l'Hébergeur en informe le Client par écrit sans nécessité de procéder par Avenant et sans accord préalable écrit du Client.

Tout changement substantiel de Sous-Traitant Ultérieur certifié HDS (remplacement d'OVH par un autre hébergeur HDS, ajout d'un nouveau Sous-Traitant Ultérieur) est soumis à la procédure de notification avec préavis de trente (30) jours calendaires et droit d'objection motivée du Client,

conformément à l'Article 7.3 du DPA principal.

8.3 Responsabilité

L'Hébergeur demeure pleinement responsable devant le Client de l'exécution, par ses Sous-Traitants Ultérieurs certifiés HDS, de leurs obligations en matière de protection des DSCP, conformément à l'article 28 du RGPD et au référentiel HDS.

Article 9 – Audit

9.1 Audits internes de l'Hébergeur

L'Hébergeur met en œuvre des audits internes visant à vérifier que les mesures mises en place pour protéger et garantir l'intégrité des Données Sources sont conformes aux exigences de la Certification HDS, efficacement mises en œuvre et maintenues.

L'Hébergeur audite les journaux d'accès par les personnes opérant pour son compte aux Objets et aux systèmes utilisés pour leur traitement.

9.2 Rapport d'audit technique mutualisé et traces spécifiques

9.2.1 Rapport d'audit mutualisé — L'Hébergeur met à la disposition du Client, sur demande écrite et sous couvert d'un accord de confidentialité, la synthèse managériale d'un rapport d'audit technique, datant de moins de trois (3) ans et réalisé par un auditeur indépendant, portant sur les ressources mutualisées. Ce rapport couvre a minima la conformité aux exigences du référentiel HDS v2 et de la norme ISO 27001 en vigueur.

9.2.2 Traces d'accès spécifiques aux DSCP (EXI15) — Sur demande écrite du Client, dans le cadre d'un incident suspecté, d'un audit ou d'une demande de contrôle, l'Hébergeur communique au Client, dans un délai de quinze (15) jours ouvrés :

- (a) Les traces spécifiques d'accès aux systèmes de traitement des Objets du Client effectuées par le personnel de l'Hébergeur dûment habilité (accès administrateurs), exportées depuis le module d'audit de l'Hébergeur,
- (b) Ces traces distinguent explicitement les accès des utilisateurs du Client (client_user) des interventions du personnel de JDS CONSEIL (jds_admin), conformément à l'exigence EXI15 du référentiel HDS,
- (c) Tout accès d'urgence au vault du Client (procédure break-glass) fait l'objet d'une notification automatique et immédiate au référent contractuel HDS du Client désigné à l'Article 3, avec mention de l'identité de l'intervenant, la justification documentée, la date et l'heure d'accès, et la durée d'accès (accès en lecture seule limité à 24 heures),
- (d) Les traces sont fournies dans un format standard lisible et exploitable (CSV ou JSON). Elles sont conservées pendant douze (12) mois glissants.

9.2.3 Rapport HDS annuel — L'Hébergeur met à disposition du Client, sur demande, un rapport annuel de conformité HDS synthétisant : le statut de la Certification HDS, les incidents de sécurité survenus sur la période, les résultats des tests de restauration PCA/PRA, et les évolutions de la Solution SaaS ayant un impact sur la sécurité des DSCP.

9.3 Audit par le DPO du Client

Principe et périmètre — L'Hébergeur autorise le DPO du Client, ou un auditeur tiers non-concurrent mandaté par lui et soumis à un accord de confidentialité, à réaliser des audits documentaires portant sur la conformité de l'Hébergeur aux exigences d'assistance au Responsable de Traitement (exercice des droits des Personnes Concernées).

Modalités — L'audit s'effectue dans la limite d'une (1) session par année civile, aux frais exclusifs du

Client, sous forme d'audit documentaire réalisé à distance. La demande est notifiée par écrit à la DPO de l'Hébergeur avec un préavis minimum de trente (30) jours ouvrés, précisant le périmètre détaillé et les points de contrôle.

Preuves accessibles — Dans le cadre de cet audit, l'Hébergeur fournit au DPO du Client, sous couvert de confidentialité :

- Documentation de conformité : Politique RGPD en vigueur, extrait pertinent du Registre des Traitements, procédure interne de gestion des demandes d'exercice de droits,
- Preuves d'assistance technique et organisationnelle : extrait anonymisé du registre des demandes, exemples de journaux d'accès à l'API, documentation technique des fonctionnalités de l'API pour localiser, récupérer et supprimer les données.

9.4 Audit par le Client

Droit d'audit — L'Hébergeur autorise le Client, une (1) fois par année calendaire et à ses propres frais, à auditer la conformité de la Solution SaaS aux engagements de sécurité, aux exigences du référentiel HDS et à la Réglementation Applicable HDS. Cet audit doit être mené par un auditeur tiers indépendant et qualifié, non concurrent direct de l'Hébergeur, préalablement validé par l'Hébergeur et soumis à un accord de confidentialité.

Modalités — La demande est notifiée par écrit à l'Hébergeur avec un préavis minimum de trente (30) jours ouvrés, précisant le périmètre, l'identité de l'auditeur et les méthodologies envisagées. L'audit se déroule, au choix de l'Hébergeur :

- (a) En fournissant au Client les documents pertinents démontrant la conformité (rapports d'audit HDS et ISO 27001, politiques, procédures, rapports de tests d'intrusion synthétiques),
- (b) En organisant des sessions d'audit à distance avec le personnel compétent de l'Hébergeur,
- (c) En fournissant un extrait des traces d'accès aux DSCP du Client sur la période auditée, conformément à l'Article 9.2.2.

Tests d'intrusion — Le Client n'est pas autorisé à effectuer des tests d'intrusion, scans de vulnérabilités ou toute autre forme de test technique offensif sur l'infrastructure de l'Hébergeur sans autorisation écrite et expresse préalable. Si une telle autorisation est accordée, le périmètre, les horaires et les adresses IP sources des tests sont strictement définis dans un protocole sur mesure, conformément à l'Article 7.3 des CGV (Pentests par tiers auditeur).

Rapport d'audit — Le Client communique à l'Hébergeur une copie du rapport final d'audit. Les non-conformités identifiées font l'objet d'un plan d'action contradictoire entre les Parties.

Prestations d'accompagnement — Les prestations d'accompagnement de l'Hébergeur lors de l'audit (mobilisation d'équipes, ouverture d'environnements, analyse conjointe) sont facturées au taux journalier de la TMA défini au Devis, à l'exception des prestations documentaires standard qui demeurent gratuites.

Article 10 – Responsabilité spécifique au périmètre HDS

10.1 Nature de l'obligation

L'Hébergeur fournit la Solution SaaS dans son périmètre HDS dans le cadre d'une stricte obligation de moyens, sous réserve des dispositions impératives de la Réglementation Applicable HDS mettant à sa charge une obligation de résultat.

10.2 Responsabilité du fait de la Sous-Traitance Ultérieure

Conformément au RGPD, l'Hébergeur reste responsable de l'exécution conforme du Contrat vis-à-vis du Client, y compris pour les prestations déléguées à ses Sous-Traitants Ultérieurs. Les défaillances de ses Sous-Traitants Ultérieurs certifiés HDS sont couvertes par les PCA/PRA de l'Hébergeur, dont

les objectifs RTO et RPO sont définis à l'Annexe 4-Bis.

10.3 Plafond de responsabilité spécifique au périmètre HDS

Par dérogation à l'Article 9.3 des CGV (double plafond), la responsabilité de l'Hébergeur au titre des dommages résultant de la mise en œuvre du périmètre HDS — sous réserve des dispositions impératives de la Réglementation Applicable HDS et du RGPD — est plafonnée, tous préjudices et formes d'indemnisation confondus, au montant total Hors Taxes des redevances effectivement payées par le Client à l'Hébergeur au titre de la Solution SaaS dans son périmètre HDS sur les douze (12) mois précédant l'événement engageant la responsabilité.

Ce plafond unique et simplifié constitue la contrepartie acceptée par les Parties de la répartition des risques inhérents à l'hébergement de DSCP et à la nature des services fournis.

10.4 Exceptions légales

Les exclusions du plafond prévues à l'Article 9.4 des CGV (faute lourde ou dolosive, dommage corporel, violation RGPD au sens de l'article 82 du RGPD, violation des obligations de confidentialité, atteinte aux droits de propriété intellectuelle de tiers) demeurent applicables au périmètre HDS.

10.5 Exclusion des pénalités forfaitaires

Aucune pénalité forfaitaire n'est prévue au titre de la présente Annexe. L'indemnisation éventuelle repose exclusivement sur la réparation de dommages démontrés, dans la limite du plafond défini au 10.3.

Article 11 – Prix et conditions associées

Le prix et les conditions tarifaires applicables au périmètre HDS sont précisés au Devis ou à l'Avenant d'activation du périmètre HDS.

Ils tiennent compte de la répartition des responsabilités et des risques entre les Parties eu égard aux spécificités de mise en œuvre (niveau de service, mesures spécifiques imposées par la Réglementation Applicable HDS) en l'état des connaissances au moment de la signature.

Les dispositions de l'Article 15 des CGV relatives à la Révision Tarifaire s'appliquent également au périmètre HDS, sous réserve des ajustements rendus nécessaires par l'évolution de la Réglementation Applicable HDS.

Article 12 – Modification de la présente Annexe

L'Hébergeur se réserve le droit de modifier la présente Annexe conformément aux évolutions de la Réglementation Applicable HDS.

Les Parties sont autorisées à inclure des clauses supplémentaires à condition qu'elles ne contredisent pas, directement ou indirectement, les engagements pris au titre de la Réglementation Applicable HDS ou qu'elles ne portent atteinte aux libertés et droits fondamentaux des Utilisateurs Finaux.

Toute modification substantielle fait l'objet d'une notification au Client, conformément à l'Article 18 des CGV WakaStart, avec un préavis raisonnable.

Annexe 4-Bis — Objectifs de performance et de niveau de service (SLO) HDS

A.4-Bis.1 Objet et interprétation

La présente Annexe précise les indicateurs de référence en matière de performance et de niveau de service applicables au périmètre HDS, conformément à l'obligation légale d'information mise à la

charge de l'Hébergeur dans le cadre de la Réglementation Applicable HDS.

A.4-Bis.2 Engagement et garantie

L'Hébergeur s'engage à respecter les modalités énoncées dans la présente Annexe dans le strict cadre d'une obligation de moyens et sous réserve de l'exécution conforme du Contrat par le Client.

En aucun cas la présente Annexe ne saurait être interprétée comme sous-tendant une obligation de résultat, une pénalité forfaitaire ou un versement automatique de dommages et intérêts.

A.4-Bis.3 Classification du service

Les systèmes d'information mis à disposition dans le cadre du service d'hébergement de DSCP sont classifiés comme critiques, conformément au référentiel HDS.

Cette classification se traduit par des mesures renforcées de protection et de sécurité.

A.4-Bis.4 Disponibilité

Taux de disponibilité mensuel — Le taux de disponibilité mensuel de référence du Service de Stockage Objet est de 99,9 %, mesuré tous les mois sur la base d'un mois calendaire.

Note : ce taux est plus élevé que le taux de 99 % défini à l'Article 13 des CGV pour la Solution SaaS standard, en raison de la criticité propre aux DSCP.

Mises à jour planifiées — Les opérations de mise à jour sont réalisées, dans la mesure du possible, en dehors des heures ouvrables, à savoir entre 20h00 et 6h00 heure française en semaine et le week-end. L'Hébergeur s'efforce de notifier le Client au moins 48 heures à l'avance de toute maintenance planifiée.

Calcul de la disponibilité — Le taux est calculé selon la formule :

Disponibilité (%) \= \[(TMT " TI) / TMT\] × 100

Où :

- TMT \= Temps Maximum Théorique (en minutes) sur la période considérée,
- TI \= Temps d'Indisponibilité (en minutes) sur la période considérée.

Événements non comptabilisés comme indisponibilité :

- Mises à jour planifiées,
- Cas de Force Majeure au sens de l'Article 20 des CGV,
- Indisponibilités causées par des éléments hors du contrôle de l'Hébergeur (configuration logicielle/matérielle du Client, qualité du réseau et de la connexion Internet),
- Indisponibilités résultant d'actions du Client, des Utilisateurs Finaux ou de tiers non autorisés.

A.4-Bis.5 Support technique

Classification des requêtes — Les objectifs de niveau de service pour le support technique sont les suivants :

Priorité	Descriptif	Délai de prise en charge	Délai de résolution	Procédure
P4/P5 — Impact mineur	Demande d'assistance ou conseil	16 heures ouvrées	10 jours ouvrés	Plateforme de signalement ou email
P3 — Impact modéré	Incident dégradant les services, fonctionnement normal possible	8 heures ouvrées	5 jours ouvrés	Plateforme de signalement ou email
P2 — Impact majeur	Impact significatif affectant une partie des fonctionnalités ou fonctionnalité spécifique indisponible	4 heures ouvrées	2 jours ouvrés	Plateforme de signalement ou email
P1 — Impact bloquant	Service majoritairement indisponible ou impossibilité d'accéder à l'environnement	2 heures ouvrées	1 jour ouvré	Téléphone

Plages de support :

Plage	Horaires
Lundi au jeudi	9h00 – 12h00 et 14h00 – 17h00
Vendredi	9h00 – 12h00 et 14h00 – 16h30

Hors jours fériés en France et fermetures exceptionnelles de l'Hébergeur avec information préalable au Client.

Canaux de contact :

- Plateforme de signalement : disponible en ligne dans l'interface d'administration,
- Email : contact@wakastellar.com (ticket qualifié HDS),
- Téléphone (P1 uniquement) : numéro communiqué au Client à l'activation du périmètre HDS.

Qualification de la priorité — Le Client qualifie la priorité dans sa requête. L'Hébergeur la confirme ou, le cas échéant, la requalifie lors de la prise en charge.

Fréquence de mesure de conformité : une fois par semestre sur une année civile.

A.4-Bis.6 Continuité et reprise d'activité (PCA/PRA)

Scénario A — Mode dégradé nominal (panne partielle, défaillance d'un composant, redémarrage de service)

Service	RTO	RPO
Service de Stockage Objet (documents DSCP S3)	\< 15 minutes	Temps réel — réplication live managée OVH (Gravelines !’ Strasbourg)
Base de données PostgreSQL (métadonnées applicatives)	\< 15 minutes	Quasi-temps-réel — PITR OVH managé
Base de données MongoDB (index DSCP)	\< 15 minutes	"d 24 heures — sauvegarde quotidienne

Scénario B — Sinistre complet (perte totale du datacenter de production, indisponibilité prolongée OVH Gravelines)

Service	RTO	RPO
Service de Stockage Objet (documents DSCP S3)	"d 24 heures	Temps réel — données disponibles sur site Strasbourg
Base de données PostgreSQL	"d 24 heures	Quasi-temps-réel — PITR OVH managé
Base de données MongoDB (index DSCP)	"d 24 heures	"d 24 heures — sauvegarde quotidienne chiffrée

Limitation assumée RPO MongoDB — L'absence de Point-in-Time Recovery sur la base MongoDB constitue une limitation documentée. Elle porte uniquement sur les métadonnées et index de documents de santé. Les documents DSCP eux-mêmes (Objets S3) bénéficient d'un RPO temps réel. Cette limitation est prise en compte dans la tarification du service.

Information du Client en cas de déclenchement du PCA/PRA — En cas d'activation du Plan de Continuité ou de Reprise d'Activité, l'Hébergeur informe le référent contractuel HDS désigné à l'Article 3 dans les meilleurs délais et au plus tard dans un délai de deux (2) heures suivant la déclaration formelle du sinistre, avec :

- La nature et l'étendue de l'incident,
- L'impact estimé sur l'accès aux DSCP du Client,
- Le délai estimé de rétablissement,
- Les mesures prises pour préserver l'intégrité et la confidentialité des DSCP.

Fréquence des tests : à chaque incident nécessitant la mise en œuvre du PCA/PRA, et au minimum

une fois par an lors d'un test de restauration documenté.

Document contractuel — JDS CONSEIL