Annexe DSN Data Manager (DDM)

Version 1.3 - Avril 2026

Préambule

Cette annexe vient compléter les informations présentes dans les Conditions Générales de Vente (CGV) d'Orisha Health & Safety accessibles sur le site internet à l'adresse suivante : https://insurance.orisha.com/cgv.

Elle vient préciser les conditions particulières et les traitements en lien avec la solution **D**SN**D**ata**M**anager (DDM) souscrite et s'applique de plein droit.

1. Conditions financières

Les montants facturés seront libellés en euros et seront payés dans cette monnaie.

Tous les prix indiqués dans le contrat et ses annexes sont indexés pour toute la durée du contrat conformément aux CGV accessibles sur notre site.

1.1. Redevance récurrente

Les conditions financières sont négociées sur la base d'un engagement ferme "Période initiale" de 3 ans sauf autre accord précisé à la Proposition Commerciale.

La première facturation est datée du 1er jour ouvré de la période de mise à disposition de la solution.

- En cas de Mise à Disposition entre le 1er et le 24 du mois M, la redevance est facturée à compter du premier jour du mois M,
- En cas de Mise à Disposition entre le 25 et le 31 du mois M, la redevance est facturée à compter du premier jour du mois M+1.

La date anniversaire du contrat est basée sur la date de la première facturation de l'abonnement.

Toute résiliation du Contrat par le Client avant la fin de la Période Initiale, pour une raison non imputable au Prestataire, donnera lieu à une facturation de 50% du montant de la redevance restant à facturer jusqu'au terme de la Période Initiale.

Après la Période Initiale, les contrats sont renouvelés tacitement et par période d'un (1) an sauf résiliation adressée 3 mois avant la date anniversaire en LRAR.

Toute résiliation intervenant en cours d'année sera facturée des échéances dues jusqu'à la date anniversaire.

1.2. Location maintenance évolutive

En contrepartie de la concession du droit d'utilisation des Progiciels décrits dans les Propositions Commerciales, de l'hébergement et de l'infogérance de la solution DDM, le licencié paiera une redevance annuelle, facturée trimestriellement à échoir, selon la tarification convenue dans la Proposition Commerciale.

La maintenance locative est facturée en fonction de la grille tarifaire précisée dans la Proposition Commerciale.

1.3. Transport et frais de vie

Les modalités seront convenues entre les Parties.

Les frais de vie et de transport seront facturés aux frais réels.

1.4. Tarif journalier des prestations

Les prestations complémentaires non définies dans la Proposition Commerciale donneront lieu, le cas échéant, à l'application des tarifs et conditions de règlement définis d'un commun accord entre les Parties selon la nature de la prestation concernée. Ces prestations complémentaires donneront lieu à une facture séparée.

Ces tarifs sont indexés pour toute la durée du contrat conformément aux CGV accessibles sur notre site.

Pour les Services concernant des « fonctions importantes ou critiques » au sens du Règlement (UE) 2022/2554 du 14 décembre 2022 dit « DORA » (ou « Règlement DORA »), le Prestataire s'engage, aux frais du Client et sur prise en charge par ce dernier de l'ensemble des coûts associés, notamment au titre de la mobilisation du personnel du Prestataire, à (i) s'assurer que son personnel participera au programmes de sensibilisation à la sécurité et aux formations à la résilience opérationnelle numérique que le Client peut être tenu d'organiser, et à (ii) participer et coopérer au test de résilience opérationnelle fondé sur la menace que le Client peut être tenu d'effectuer par une loi ou réglementation en vigueur.

1.5. Facturation en mode projet

Pour de nouveaux projets, la facturation à date de livraison en recette sera au minimum fixée à 90% du montant initial devisé. Les 10% restant seront facturés à réception du procès-verbal de recette définitif engageant la mise en production.

Les Parties peuvent convenir d'un autre échéancier de facturation sur la Proposition Commerciale signée. Sans précision d'un échéancier de facturation spécifique, l'échéancier préalablement cité s'appliquera.

Le Client dispose de 45 jours calendaires pour effectuer la recette, sauf dérogation écrite entre les Parties.

A l'issue du délai de 45 jours, la recette sera de facto « prononcée » et la facturation du montant restant dû du projet et du locatif associé (le cas échéant) seront engagés.

1.6. Prestation de formation

Le Prestataire propose des formations à l'utilisation de la solution DDM. Le catalogue des formations disponibles est accessible à l'adresse https://insurance.orisha.com/formation.

La formation peut se faire en présentiel ou en distanciel, selon le choix du Client.

- Prérequis technique en distanciel:
    - 1 ordinateur par participant
    - 1 connexion internet
- Maximum de participants à la formation : 7 participants par groupe

Un règlement sera remis à chaque participant à la formation.

1.7. Modalités de réversibilité

En cas de cessation de la relation contractuelle, le Client peut demander au Prestataire la mise en œuvre d'une prestation de réversibilité, en précisant les attendus en matière de restitution des Données du Client et, le cas échéant, la nature de l'assistance attendue durant la période de migration. Cette demande devra être adressée par lettre recommandée avec accusé de réception au plus tard trois (3) mois avant la cessation de la relation contractuelle.

La prestation de réversibilité fera l'objet d'une qualification et d'un chiffrage adapté au scénario retenu par les Parties, sauf disposition contractuelle contraire, et sera à régler à réception de la facture.

Il est entendu entre les Parties que la mise en œuvre de la réversibilité ne suspend pas l'exécution des obligations contractuelles des Parties. Par conséquent, le Prestataire continuera de facturer au Client les Services au titre du Contrat, le Client s'engageant corrélativement à les honorer.

Dans le cas où une prestation de réversibilité a été mise en œuvre, les Données du Client seront supprimées dans un délai maximal d'un mois à compter de la fin de ladite prestation.
À défaut de mise en œuvre d'une prestation de réversibilité, les Données du Client seront supprimées dans un délai maximal d'un mois à compter de la date de fin du contrat.
Dans tous les cas, le Prestataire s'engage à fournir au Client un certificat de destruction des Données du Client sur demande du Client.
Le Prestataire ne pourra être tenu responsable en cas d'absence de demande de prestation de réversibilité exprimée par le Client.

2. Condition d'accès et prérequis

Afin que la solution DDM soit utilisé dans les meilleures conditions, il est impératif d'avoir :

- Un navigateur internet à jour et supporté par l'éditeur
- Un accès internet

3. Hébergement et infogérance

Le Client a retenu le Prestataire comme partenaire pour assurer l'infogérance et l'hébergement de la solution DDM.

La présente description est donnée à titre indicatif par le Prestataire, qui pourra faire évoluer le datacenter en fonction de ses besoins et des progrès de la technique, sans que cela nécessite la régularisation d'un avenant.

Les seuls engagements du Prestataire sont, d'une part, de ne pas dégrader le niveau technique du datacenter et, d'autre part, la fourniture de ses prestations

au titre de l'hébergement et de l'infogérance conformément aux Indicateurs Qualité convenus.

L'offre du Prestataire s'appuie sur un hébergeur agréé Hébergement de Données de Santé et ISO 27001 (voir " Certifications & Labels").

Lorsque le Client importe et/ou stocke des Données du Client dans le Progiciel, le Client accorde au Prestataire, ainsi qu'à ses sous-traitants, une licence, pour la France, d'hébergement, de stockage, de reproduction desdites Données du Client uniquement en vue de l'exécution des Services. Cette autorisation demeure pour toute la durée du Contrat.

3.1. Périmètre

Le périmètre d'hébergement et d'infogérance est précisé dans la Proposition Commerciale selon les solutions souscrites.

3.2. Sauvegardes

Le Prestataire garantit au Client un plan de sauvegarde défini comme suit:

- Sauvegarde quotidienne sur 7 jours.
- Sauvegarde immuable mensuelle glissante pour le dernier mois calendaire écoulé (sauvegarde réalisée le premier jour calendaire du mois).
- Sauvegarde immuable annuelle conservée sur 3 ans glissants (sauvegarde réalisée le premier jour calendaire de l'année).

3.3. PCA / PRA

Toutes les composantes de l'infrastructure de l'hébergeur technique du Prestataire, dédiées à la plateforme, sont redondées et développées pour être résilientes au travers de 2 instances situées en France ou Union Européenne, qui assurent la Continuité d'Activité (Multi Availability Zone).

Cela signifie que les moyens techniques et organisationnels sont mis en œuvre avec pour mission d'assurer une très haute disponibilité répartie sur deux instances et qu'un incident majeur sur l'une des instances n'aura pas d'impact fonctionnel sur le service rendu et la disponibilité de la donnée en respect des accords fixés entre les Parties.

Une prise d'engagement sur cette continuité sera appuyée sur les garanties fournies par l'hébergeur technique du Prestataire et sur les mécanismes de réplication certifiés par ses soins (garantie d'intégrité et de confidentialité sur les données)

4. Support et Maintenance

La Documentation associée à la solution DDM est mise à disposition du Client par le Prestataire.

Il appartient aux utilisateurs de se reporter à cette Documentation avant chaque demande.

Avant de signaler un incident, le Client s'assure qu'il ne se situe pas sur ses équipements ou ceux sous sa responsabilité.

Le Client devra décrire de façon précise et exhaustive les symptômes du problème rencontré avant de les adresser.

Le niveau de gravité est établi d'un commun accord entre le Client et le service support du Prestataire. En cas de désaccord, l'avis de ce dernier prévaudra jusqu'à éventuelle requalification entre les Parties.

Dans l'attente d'une solution définitive, le Prestataire pourra préconiser une solution provisoire, dans les meilleurs délais compatibles avec la nature de la difficulté.

4.1. Procédure Support

Les demandes sont adressées par mail à l'adresse du Support DDM mise à disposition des Clients.

A partir des informations, le Prestataire procède au diagnostic et le cas échéant à la correction des Anomalies en indiquant au Client par téléphone ou par courriel la procédure à suivre.

L'adresse mail du Support DDM est accessible 7 jours sur 7, 24 heures sur 24. Elle constitue le point d'entrée à privilégier qui assure l'accueil, la notification, la prise en compte, l'aiguillage et le suivi des demandes du Client. Les demandes sont récupérées en temps réel par le Support aux horaires ouvrés.

Le Client s'engage à utiliser, en toutes hypothèses, cet outil de communication pour signaler les difficultés rencontrées, y compris pour confirmer d'éventuels signalements effectués par mail. Toute demande d'intervention réalisée sur cet outil reçoit un numéro d'identifiant unique. Ce numéro de référence sera nécessaire au suivi.

Toute remontée d'Anomalie qui ne suivrait pas ce canal obligatoire ne pourra être prise en compte pour l'appréciation des indicateurs "Délai d'intervention et suivi" du Prestataire.

Le Support DDM assure les services suivants :

- Identifier l'utilisateur, vérifier son habilitation, identifier le Client et le Contrat
- Qualifier la nature de sa demande
- Le cas échéant, classifier l'Anomalie selon son niveau de sévérité
- Assurer le traitement de l'Anomalie et sa traçabilité jusqu'à sa clôture
- Assister si besoin le Client à distance
- Transmettre la demande au service compétent, si celle-ci ne relève pas de son périmètre

4.2. Délai d'intervention et suivi

La réception par le Prestataire de l'ensemble des informations requises à l'ouverture du ticket constitue le point de départ des délais de traitement de l'Anomalie.

Les délais sont mentionnés en Heures / Jour Ouvrés.

Anomalie	Délai d'Intervention	Délai pour solution de contournement	Délai de Résolution d'Anomalie ou clôture du ticket
Bloquante	2 heures ouvrables	1 jour ouvrable	5 jours ouvrables
Majeure	4 heures ouvrables	2 jours ouvrables	10 jours ouvrables
Mineure			Version mineure suivante, ou subséquente

4.3. Maintenance

Maintenance corrective

La prestation de maintenance corrective consiste en la correction de toute Anomalie reproductible ou avérée qui apparaît dans l'utilisation de l'accès distant du Progiciel.

Maintenance évolutive

Des mises à jour du Progiciel pourront être installées par le Prestataire sur son Environnement, au fur et à mesure de leur disponibilité. Ces mises à jour, qui sont décidées unilatéralement par le Prestataire, seront mises à disposition du Client depuis son Environnement sans coût supplémentaire.

Maintenance réglementaire

Les différentes mises à jour auront pour objet de procéder à l'ensemble des modifications rendues nécessaires par les évolutions légales ou réglementaires correspondant aux traitements relatifs à la mise en œuvre du Progiciel.

Exclusions à la Maintenance

Le Prestataire n'assurera pas le service de maintenance dans les cas suivants :

- Utilisation non conforme à la documentation de l'accès distant ;
- Intervention non autorisée réalisée par le Client ou par un tiers agissant pour le compte du Client ;
- Anomalie générée par le matériel du Client ou ses équipements d'accès ;
- Toute modification, révision, changement ou entretien du Progiciel non autorisée par le Prestataire ;
- Refus du Client d'accepter une nouvelle Version proposée par le Prestataire, ne modifiant pas les fonctionnalités, ne dégradant pas le fonctionnement général du Progiciel et permettant d'éviter la rencontre d'Anomalies.

Le Prestataire n'assurera pas le service d'assistance corrective, ou pourra le cas échéant les assurer à des conditions financières à déterminer, dans les cas suivants :

- Changement des logiciels du constructeur implanté sur la configuration des postes de travail, difficilement, peu, ou non compatible avec le Progiciel objet du contrat de fourniture. A ce titre, les parties conviennent de se tenir mutuellement informées d'un éventuel changement, et le

Prestataire avertit le Client, des délais et des conditions de mise à niveau présumés ;

- Changement de tout ou partie du matériel compatible ou incompatible avec les Progiciels, objet des présentes ;
- Exploitation sur le système du Client, par cette dernière ou par un tiers, de tout produit, programme (logiciels, progiciels) non fourni par le Prestataire, et pouvant être à l'origine d'anomalies, du fait de ses interférences éventuelles avec le Progiciel objet du présent contrat ;
- Mauvaise manipulation du Progiciel.

5. Plan d'Assurance Sécurité

L'ensemble des informations relatives aux garanties de sécurité des prestations figure dans le document « Plan d'Assurance Sécurité » du Prestataire, communicable au Client sur demande écrite de ce dernier.

Le Prestataire se réserve le droit de modifier, à tout moment, les mesures définies dans le Plan Assurance Sécurité, lesquelles sont par nature évolutives dans la mesure où elles s'inscrivent dans une démarche d'amélioration continue.

En cas d'incident avéré lié aux Services TIC ("Technologies de l'Information et de la Communication") fournis par le Prestataire concernant des « fonctions importantes ou critiques » au sens du Règlement DORA, le Prestataire pourra fournir au Client, sur demande écrite de ce dernier, les informations dont il dispose permettant de classer les incidents liés aux TIC selon les critères définis à l'article 18 du Règlement DORA.

En cas d'incident avéré lié aux Services TIC fournis par le Prestataire concernant des « fonctions importantes ou critiques » au sens du Règlement DORA et hors Anomalie couverte par les présentes conditions, le Prestataire s'engage, sous réserve d'acceptation par le Client d'un devis sur la base des tarifs en vigueur du Prestataire, à fournir une assistance sur le/les Services TIC concerné(s). Dans ce cas, le Client s'engage à coopérer activement, dans le cadre de son obligation de collaboration et de bonne foi, avec le Prestataire dans la réalisation de l'assistance qu'il fournit. Cette assistance n'implique en aucun cas une obligation de résultat quant à la résolution de l'incident visé.

6. Description des traitements de données

6.1. Traitements réalisés par le Prestataire

Dans le cadre de la relation commerciale et contractuelle, le Prestataire est amené à traiter des données personnelles de ses clients et collaborateurs en tant que Responsable de traitement.

Objet -Finalité	Personnes concernées	Catégories Données	Sous-traitant & logiciel	Sécurité & garanties
Projet & échanges	Participant au projet, Direction, Administratif …	Identité, coordonnées de contact	Google Workspace	Compte nominatif sécurisé par authentification Boîte mail sécurisée
Contrat et commandes	Direction, Administratif, Projet, Commercial	Identité, coordonnées de contact	Google Workspace	Compte nominatif sécurisé par authentification Boîte mail sécurisée Chiffrement
Comptabilité	Administratif Direction Commercial	Identité adresse mail	SAGE CashOnTime	Compte nominatif sécurisé par authentification
Newsletter & communication actualité	Participant au contrat ou au projet	Identité adresse mail	Salesforce	Compte nominatif sécurisé par authentification Clauses contractuelles type 2021 Chiffrement des données
Accès aux locaux	Visiteur	Identité	Non	Conservation 1 an Habilitation limitée
Enquête de satisfaction Client	Clients de la Solution	Données d'identification	Survicate	Certifié ISO 27001

6.2. Traitements DDM sur instruction du Client

Traitement	Finalité	Catégories Données	Sous-traitant	Transfert hors UE
Comptes-rendus métiers DSN	Générer les Comptes-Rendus Métiers (CRM) Mettre à disposition les CRM auprès des Concentrateurs Valider la qualité et la bonne réception du flux	Norme NEODES		Non
Consolidation des flux DSN	Contrôler la conformité des données en lien avec la fiche de paramétrage Garantir l'intégrité Assurer la cohérence	Norme NEODES		Non
Exports	Exports standards -Formatés aux normes réglementaires	Norme NEODES		Non
Hébergement DDM	Mettre à disposition les informations nécessaires au fonctionnement des solutions pour nos Clients Hébergés	Norme NEODES	AWS	Non
Intégration des flux DSN	Intégrer les fichiers DSN Historiser les données DSN	Norme NEODES		Non
Hébergement API DDM	Mise à disposition des données au travers de l'API pour les Clients Lecture- Export	Norme NEODES	AWS	Non
Support et Maintenance	Assurer la maintenance et l'Assistance auprès de nos Clients	Identité collaborateur Client et potentielles données adhérent si besoin	JIRA	Non

6.3. Liste des sous-traitants

Sous-traitant	Finalité	Localisation des données	Garanties
AWS	Cloud Provider (sans accès aux données)	France	Contrat Certifié HDS; ISO 27001;...

7. Audits

7.1. Généralités

i. Sur demande expresse du Client, ce dernier pourra diligenter une procédure d'audit, à tout moment, dans le but d'évaluer le respect par le Prestataire des obligations souscrites par elle au titre du présent contrat, selon les modalités suivantes :

- Cet audit ne pourra porter que sur les éléments données et justificatifs relatifs aux prestations effectuées pour le Client conformément aux conditions prévues au Contrat ;
- Il ne pourra être effectué que dans la limite d'une (1) fois par année contractuelle ;
- La demande d'audit sera notifiée par le Client au Prestataire par lettre recommandée avec accusé de réception au moins trente (30) Jours Ouvrés avant la réalisation de l'audit. Cette demande devra détailler ce que le Client envisage en termes de périmètre d'audit ;
- Les Parties disposeront d'un délai de trente (30) Jours Ouvrés suivant la demande pour convenir du protocole d'audit qui sera déroulé, les méthodes utilisées et les données auditées.
- Cet audit pourra être effectué par les soins soit d'une structure d'audit interne du Client ; soit par un cabinet extérieur à la triple condition que ce tiers ne soit pas un concurrent direct ou indirect du Prestataire ou un ancien salarié de celui-ci, qu'il soit soumis au secret professionnel et qu'il est conclu un accord de confidentialité dont copie sera remise au Prestataire pour approbation ; soit, si l'audit porte sur des Services TIC concernant des « *fonctions importantes ou critiques* » au sens du Règlement DORA, par l'autorité compétente, y compris les personnes nommées par cette autorité. Le Prestataire dispose de la faculté de s'opposer à la nomination d'un auditeur proposé par le Client, cette décision devant être motivée et dûment justifiée ;

- Le Client vérifie que les auditeurs, qu'il s'agisse d'auditeurs internes ou externes ou d'un groupe d'auditeurs, possèdent les compétences et les connaissances requises pour réaliser efficacement les évaluations et les audits pertinents communément admises et conformément à toute instruction de surveillance relative à l'utilisation et à l'incorporation de ces normes d'audit ;
- Cet audit ne devra pas perturber les activités du Prestataire.

ii. Le Prestataire s'engage à coopérer avec l'auditeur ou, le cas échéant s'agissant des audits portant sur le respect du Règlement DORA, l'autorité compétente ou le superviseur principal au sens du Règlement DORA, et à lui fournir les informations et, le cas échéant, documents tels que définis dans le protocole d'audit.

iii. Les frais d'audit restent à la charge du Client, ainsi que les éventuels frais engagés et temps passés par le Prestataire ou ses sous-traitants ultérieurs.

iv. Le Client sera responsable de tout dommage qui résulterait de l'exercice de l'audit, subi par le Prestataire ou par tout tiers au contrat (y compris les autres clients du Prestataire). Il ne pourra donc obtenir l'indemnisation par le Prestataire des dommages subis par le Client et résultant directement de l'exercice de cet audit, notamment si l'audit entraîne l'indisponibilité des Services ou une perte, altération ou divulgation de données.

v. Les résultats d'audit feront l'objet d'un débat contradictoire et d'une validation par les Parties. Les informations contenues dans le rapport d'audit, ainsi que tout document remis par le Prestataire, sont soumis à la même obligation de confidentialité que celle prévue au contrat.

Au cas où le rapport d'audit ferait apparaître un non-respect des obligations du Prestataire visées au contrat, non contesté et reconnu par le Prestataire, ce dernier s'engage à mettre en œuvre, à ses frais, les mesures correctives nécessaires dans un délai convenu entre les Parties, à l'exclusion de toute autre indemnisation.

Dans l'hypothèse où le Prestataire contesterait le non-respect d'une obligation ou son impact sur le résultat attendu, les Parties se réuniront pour décider des répartitions de la prise en charge des coûts liés à cet audit.

7.2. Tests de résilience opérationnelle

Sous réserve que les Services TIC concernent des « *fonctions importantes ou critiques* » au sens du Règlement DORA, le Client est habilité à faire réaliser des tests de résilience opérationnelle fondés sur la menace, dans la limite d'une (1)

fois par année contractuelle, par des personnes habilitées selon les conditions précisées ci-après, et à condition que cette prestation soit encadrée par un contrat.

Ces tests ne pourront porter que sur les éléments, données et justificatifs relatifs aux Services TIC effectués pour le Client au titre du contrat concernant des « *fonctions importantes ou critiques* » au sens du Règlement DORA.

Le prestataire testeur doit :

- Posséder l'aptitude et la réputation les plus élevées, le Prestataire pourra solliciter du Client tout document permettant de justifier de l'expertise technique du prestataire testeur ;
- Ne pas être un concurrent direct ou indirect du Prestataire ou un ancien salarié de celui-ci;
- Être soumis au secret professionnel et avoir conclu un accord de confidentialité dont copie sera remise au Prestataire pour approbation ;
- Posséder les capacités techniques et organisationnelles et justifier d'une expertise spécifique en matière de renseignement sur les menaces et de tests de pénétration et de tests en mode red team ;
- Être certifié par un organisme d'accréditation dans un état membre ou adhérent à des codes de conduite ou des cadres éthiques formels ;
- Fournir une assurance indépendante ou un rapport d'audit ayant trait à la bonne gestion des risques associés à la réalisation de tests de pénétration fondés sur la menace, y compris la protection adéquate des informations confidentielles du Client et la couverture des risques opérationnels du Client ;
- Être dûment et entièrement couvert par les assurances de responsabilité civile professionnelle pertinentes, y compris contre les risques de mauvaise conduite et de négligence.

Le Prestataire dispose de la faculté de s'opposer à la nomination du prestataire testeur proposé par le Client, cette décision devant être motivée et dûment justifiée.

Le Client, lorsqu'il a recours à des testeurs internes, s'engage à ce que, outre les exigences prévues ci-dessus, les conditions suivantes soient remplies :

- Le recours à ces testeurs internes a été approuvé par l'autorité compétente concernée ou par l'autorité publique unique désignée conformément à l'article 26, paragraphes 9 et 10 du Règlement DORA ;
- L'autorité compétente concernée a vérifié que le Client dispose des ressources suffisantes et a veillé à éviter les conflits d'intérêts pendant les phases de conception et d'exécution du test ;
- L'absence de conflit d'intérêts des testeurs et l'alternance périodique entre le recours à des testeurs internes et à des testeurs externes (tous les trois tests) ;
- Le fournisseur de renseignements sur les menaces est externe au Client.

En cas de recours à des testeurs externes, le Client s'engage à veiller à ce que les contrats conclus avec des testeurs externes requièrent une gestion efficace des résultats des tests de pénétration fondés sur la menace, et à ce que le traitement de données correspondant, y compris la génération, le stockage, l'agrégation, l'élaboration, le projet, le rapport, la communication ou la destruction, ne fasse pas courir de risques au Client ni au Prestataire.

Le Client doit préalablement communiquer au Prestataire, et en respectant un délai de prévenance de 30 Jours Ouvrés au minimum :

- Le périmètre du test (Liste des URL, matériels, réseaux, logiciels…) ;
- Les dates et délais de réalisation des tests ;
- Les lieux de réalisation des tests ;
- Les coordonnées de contacts pour l'audit côté Client et côté prestataire testeur ;
- Ainsi que la désignation des outils et techniques utilisés.

Le rapport incluant la synthèse des résultats, le détail des vulnérabilités et les préconisations identifiées, sera remis et partagé avec le Prestataire et ses éventuels sous-traitants ultérieurs afin de convenir des éventuelles actions correctives à mettre en place dès lors que les résultats du rapport ne sont pas contestés et sont reconnus par le Prestataire.

Les tests de résilience opérationnelle ne devront en aucun cas perturber l'activité du Prestataire.

Le Client reste responsable des éventuelles dégradations ou interruptions de service durant ou par suite de la réalisation de ces tests.

8. Résiliation au titre de la résilience opérationnelle (DORA)

Conformément aux exigences du Règlement (UE) 2022/2554, le Client dispose de la faculté de résilier le présent Contrat dans les circonstances spécifiques et limitatives suivantes :

- Le Prestataire présente une ou plusieurs violation(s) grave(s) et caractérisée(s) aux dispositions législatives, réglementaires ou contractuelles relatives à la sécurité des TIC.
- Le suivi des risques révèle des changements substantiels et objectifs affectant la capacité du Prestataire à exécuter les fonctions prévues par le présent Contrat, y compris des changements significatifs qui affectent le Contrat ou la situation du Prestataire. Les Parties conviennent que de tels changements doivent avoir un impact direct et matériellement démontrable sur la fourniture ou la sécurité des Services pour ouvrir droit à résiliation.
- Le Prestataire présente des faiblesses significatives liées à sa gestion globale du risque TIC, compromettant durablement la disponibilité, l'authenticité, l'intégrité ou la confidentialité des Données du Client. L'existence de ces faiblesses doit être établie de manière contradictoire et documentée entre les Parties.
- Les conditions contractuelles ou les circonstances liées au Prestataire empêchent l'autorité de contrôle compétente d'exercer sa mission de surveillance du Client de manière efficace.

Sauf injonction de l'autorité de contrôle exigeant une cessation immédiate ou un délai plus court, la résiliation du présent Contrat ne peut intervenir qu'après mise en demeure par le Client au Prestataire, notifiée par lettre recommandée avec accusé de réception, précisant le manquement en cause, et non réparé au terme d'un délai de trente (30) jours à compter de sa date de réception.

En cas de résiliation au titre du présent article, le Client reste tenu au paiement de tous Services fournis jusqu'à la date d'effet de la résiliation, et plus généralement au paiement de toutes factures dues et restées impayées nonobstant la prise

d'effet de la résiliation. Une prestation de réversibilité pourra également être déclenchée sur demande du Client, selon les modalités prévues au Contrat.

9. SLA - Objectifs de service

Objet	Indicateur	Valeur
Taux de disponibilité des services de la solution DDM	Taux de disponibilité effectif (mesure mensuelle)	99% sur les plages d'ouverture des services, hors plages de maintenances programmées et annoncées (ex : mise en production d'une nouvelle version de la solution).
Plage d'ouverture du service DDM CORE (front-office) et Plage d'ouverture du service DDM SEPA (front-office)		Du lundi au vendredi, de 7h00 à 20h00 (GMT+1) (*)
Plage d'ouverture du service DDM API		Disponibilité 24/7, hors redémarrage quotidien du service (durée de redémarrage ≤ 2 minutes)
Gestion de comptes Administrateur Client	Réception de la demande durant les plages horaires d'ouverture du Support DDM	12 h ouvrées pour la création d'un compte Administrateur Client 4 h ouvrées pour réinitialisation ou déverrouillage d'un compte Administrateur Client
Disponibilité du Support DDM		9h00-12h30 et 14h-18h00 du lundi au jeudi (GMT+1) 9h00-12h30 et 14h-17h00 le vendredi (GMT+1)

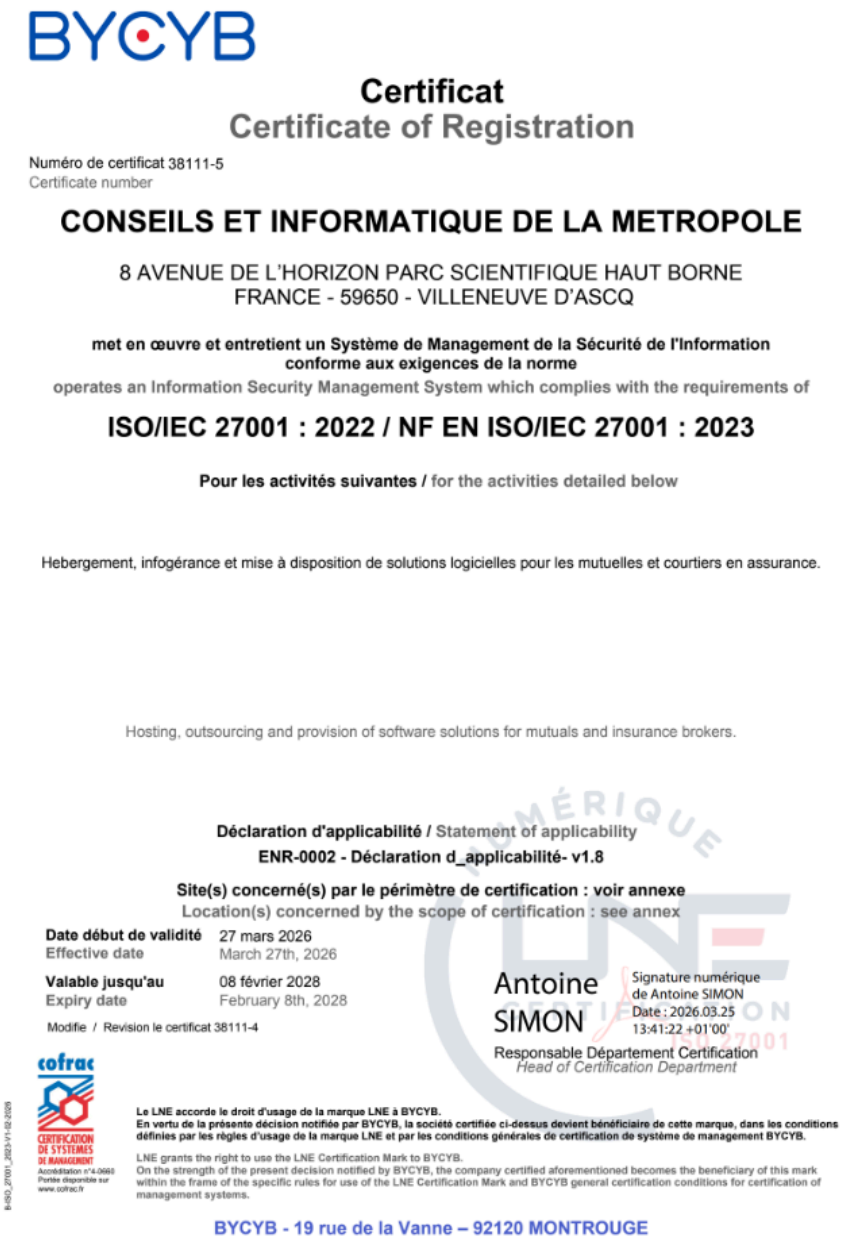
**À la demande du Client et sous réserve d'acceptation préalable du Prestataire, la plage horaire d'ouverture du service peut être ajustée, dans la limite d'une durée maximale de*

13 heures consécutives par jour. Une extension de cette durée maximale peut être mise en place, sous réserve de validation d'une proposition commerciale spécifique.

10. Labels & Certifications

<u>Orisha Insurance - CIM</u> :

- **Rapport ISAE 3402 de type 1** pour son système de contrôle interne. Réalisé par les auditeurs de la société Grant Thornton.
- **Certification ISO 27001**



BYCYB

Certificat
Certificate of Registration

Numéro de certificat 38111-5
Certificate number

CONSEILS ET INFORMATIQUE DE LA METROPOLE

8 AVENUE DE L'HORIZON PARC SCIENTIFIQUE HAUT BORNE
FRANCE - 59650 - VILLENEUVE D'ASCQ

met en œuvre et entretient un Système de Management de la Sécurité de l'Information conforme aux exigences de la norme
operates an Information Security Management System which complies with the requirements of

ISO/IEC 27001 : 2022 / NF EN ISO/IEC 27001 : 2023

Pour les activités suivantes / for the activities detailed below

Hebergement, infogérance et mise à disposition de solutions logicielles pour les mutuelles et courtiers en assurance.

Hosting, outsourcing and provision of software solutions for mutuals and insurance brokers.

Déclaration d'applicabilité / Statement of applicability
ENR-0002 - Déclaration d_applicabilité- v1.8

Site(s) concerné(s) par le périmètre de certification : voir annexe
Location(s) concerned by the scope of certification : see annex

Date début de validité / Effective date : 27 mars 2026 / March 27th, 2026
Valable jusqu'au / Expiry date : 08 février 2028 / February 8th, 2028

Modifie / Revision le certificat 38111-4

Antoine SIMON
Signature numérique de Antoine SIMON
Date : 2026.03.25 13:41:22 +01'00'
Responsable Département Certification
Head of Certification Department

cofrac
CERTIFICATION DE SYSTEMES DE MANAGEMENT
Accréditation n°4-0683
Portée disponible sur www.cofrac.fr

Le LNE accorde le droit d'usage de la marque LNE à BYCYB.
En vertu de la présente décision notifiée par BYCYB, la société certifiée ci-dessus devient bénéficiaire de cette marque, dans les conditions définies par les règles d'usage de la marque LNE et par les conditions générales de certification de système de management BYCYB.

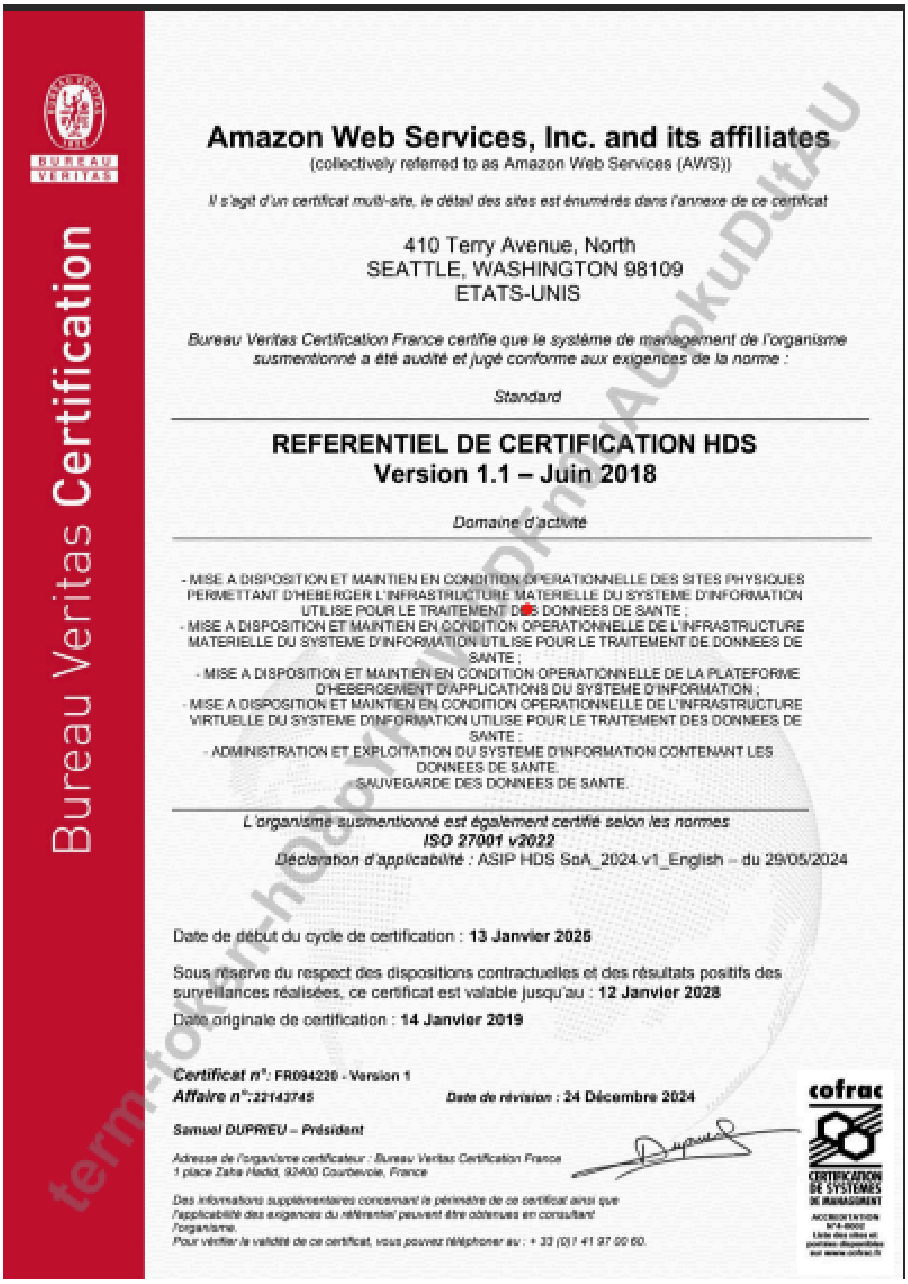
LNE grants the right to use the LNE Certification Mark to BYCYB.
On the strength of the present decision notified by BYCYB, the company certified aforementioned becomes the beneficiary of this mark within the frame of the specific rules for use of the LNE Certification Mark and BYCYB general certification conditions for certification of management systems.

BYCYB - 19 rue de la Vanne – 92120 MONTROUGE

AWS :

- **HDS - Hébergeur certifié :**
  Liste des hébergeurs certifiés | Agence du Numérique en Santé

- **AWS dispose de certifications de conformité aux normes ISO/IEC** 27001:2022, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 et CSA STAR CCM v4.0
  https://aws.amazon.com/compliance/iso-certified/



Bureau Veritas Certification

Amazon Web Services, Inc. and its affiliates
(collectively referred to as Amazon Web Services (AWS))

Il s'agit d'un certificat multi-site, le détail des sites est énumérés dans l'annexe de ce certificat

410 Terry Avenue, North
SEATTLE, WASHINGTON 98109
ETATS-UNIS

Bureau Veritas Certification France certifie que le système de management de l'organisme susmentionné a été audité et jugé conforme aux exigences de la norme :

Standard

REFERENTIEL DE CERTIFICATION HDS
Version 1.1 – Juin 2018

Domaine d'activité

- MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DES SITES PHYSIQUES PERMETTANT D'HEBERGER L'INFRASTRUCTURE MATERIELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DES DONNEES DE SANTE ;
- MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DE L'INFRASTRUCTURE MATERIELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DE DONNEES DE SANTE ;
- MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DE LA PLATEFORME D'HEBERGEMENT D'APPLICATIONS DU SYSTEME D'INFORMATION ;
- MISE A DISPOSITION ET MAINTIEN EN CONDITION OPERATIONNELLE DE L'INFRASTRUCTURE VIRTUELLE DU SYSTEME D'INFORMATION UTILISE POUR LE TRAITEMENT DES DONNEES DE SANTE ;
- ADMINISTRATION ET EXPLOITATION DU SYSTEME D'INFORMATION CONTENANT LES DONNEES DE SANTE.
- SAUVEGARDE DES DONNEES DE SANTE.

L'organisme susmentionné est également certifié selon les normes
ISO 27001 v2022
Déclaration d'applicabilité : ASIP HDS SoA_2024.v1_English – du 29/05/2024

Date de début du cycle de certification : **13 Janvier 2025**

Sous réserve du respect des dispositions contractuelles et des résultats positifs des surveillances réalisées, ce certificat est valable jusqu'au : **12 Janvier 2028**

Date originale de certification : **14 Janvier 2019**

***Certificat n°*: FR094220 - Version 1**
***Affaire n°*:22143745** ***Date de révision* : 24 Décembre 2024**

Samuel DUPRIEU – Président

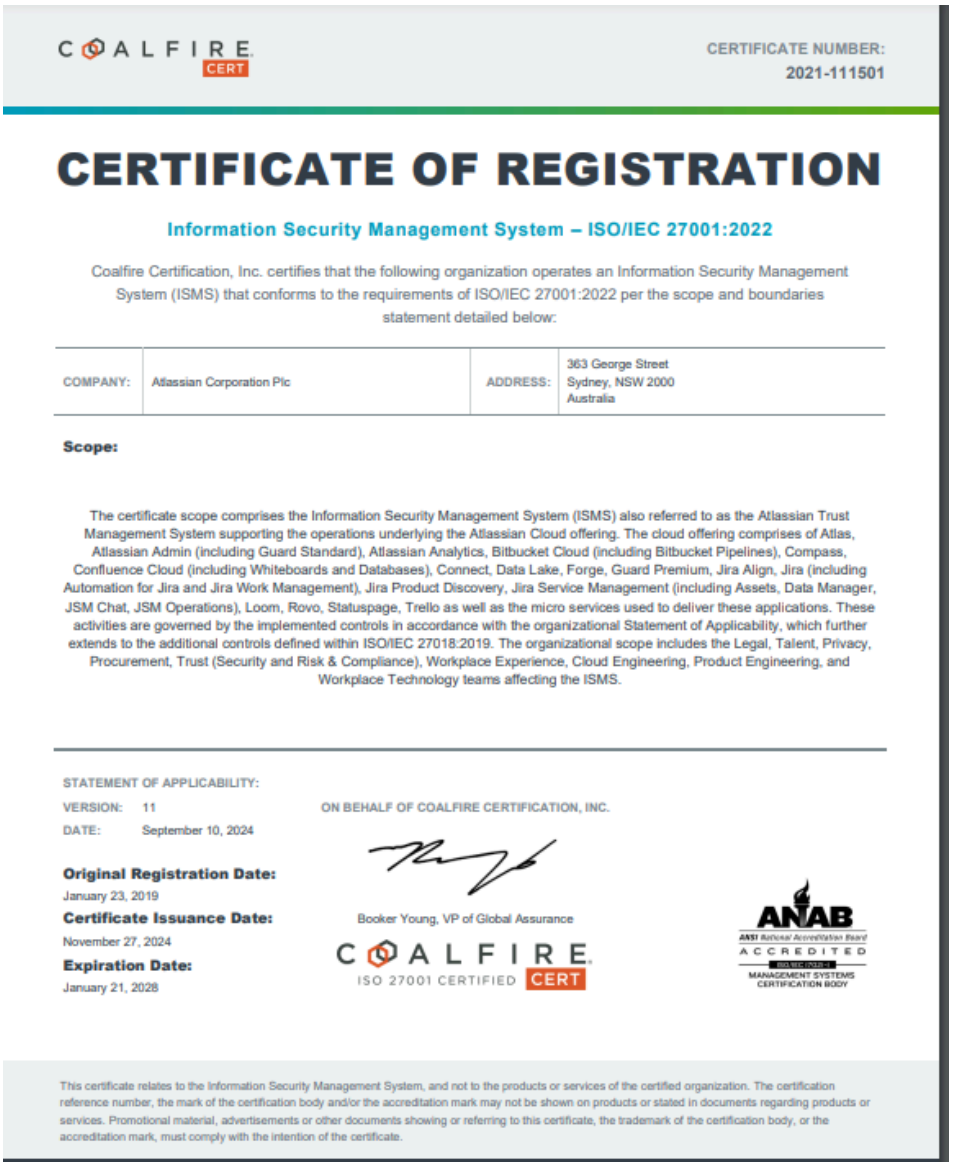
Adresse de l'organisme certificateur : Bureau Veritas Certification France
1 place Zaha Hadid, 92400 Courbevoie, France

Des informations supplémentaires concernant le périmètre de ce certificat ainsi que l'applicabilité des exigences du référentiel peuvent être obtenues en consultant l'organisme.
Pour vérifier la validité de ce certificat, vous pouvez téléphoner au : + 33 (0)1 41 97 00 60.

cofrac CERTIFICATION DE SYSTEMES DE MANAGEMENT

ATLASSIAN (JIRA) :

- Certification ISO 27001
- DPA



COALFIRE CERT

CERTIFICATE NUMBER: 2021-111501

CERTIFICATE OF REGISTRATION

Information Security Management System – ISO/IEC 27001:2022

Coalfire Certification, Inc. certifies that the following organization operates an Information Security Management System (ISMS) that conforms to the requirements of ISO/IEC 27001:2022 per the scope and boundaries statement detailed below:

COMPANY:	Atlassian Corporation Plc	ADDRESS:	363 George Street Sydney, NSW 2000 Australia

Scope:

The certificate scope comprises the Information Security Management System (ISMS) also referred to as the Atlassian Trust Management System supporting the operations underlying the Atlassian Cloud offering. The cloud offering comprises of Atlas, Atlassian Admin (including Guard Standard), Atlassian Analytics, Bitbucket Cloud (including Bitbucket Pipelines), Compass, Confluence Cloud (including Whiteboards and Databases), Connect, Data Lake, Forge, Guard Premium, Jira Align, Jira (including Automation for Jira and Jira Work Management), Jira Product Discovery, Jira Service Management (including Assets, Data Manager, JSM Chat, JSM Operations), Loom, Rovo, Statuspage, Trello as well as the micro services used to deliver these applications. These activities are governed by the implemented controls in accordance with the organizational Statement of Applicability, which further extends to the additional controls defined within ISO/IEC 27018:2019. The organizational scope includes the Legal, Talent, Privacy, Procurement, Trust (Security and Risk & Compliance), Workplace Experience, Cloud Engineering, Product Engineering, and Workplace Technology teams affecting the ISMS.

STATEMENT OF APPLICABILITY:
VERSION: 11
DATE: September 10, 2024

Original Registration Date:
January 23, 2019
Certificate Issuance Date:
November 27, 2024
Expiration Date:
January 21, 2028

ON BEHALF OF COALFIRE CERTIFICATION, INC.

Booker Young, VP of Global Assurance

COALFIRE ISO 27001 CERTIFIED CERT

ANAB ACCREDITED MANAGEMENT SYSTEMS CERTIFICATION BODY

This certificate relates to the Information Security Management System, and not to the products or services of the certified organization. The certification reference number, the mark of the certification body and/or the accreditation mark may not be shown on products or stated in documents regarding products or services. Promotional material, advertisements or other documents showing or referring to this certificate, the trademark of the certification body, or the accreditation mark, must comply with the intention of the certificate.