Version en date du 05 Mars 2026

SERVICE RAINBOW HDS PAYANT EN MODE UCaaS – Hébergement de Données Santé Conditions particulières d'utilisation

Les présentes Conditions particulières d'utilisation (les « Conditions d'utilisation ») régissent l'utilisation du service Rainbow HDS payant (le « Service Rainbow HDS » ou « Service ») que vous avez acheté directement auprès d'ALE International ou d'un Revendeur Agréé (ci-après le « Fournisseur de Service »).

Le Service Rainbow est une solution de communication fournie par ALE International (« ALE »), une société française dont le siège social se situe au 32 avenue Kléber, 92700 Colombes, France, enregistrée à la Chambre de commerce de Nanterre sous le numéro 602 033 185 RCS Nanterre (pour plus d'informations veuillez cliquer sur le lien suivant https://www.al-enterprise.com). Le Service Rainbow HDS est décrit plus en détail en section 3.

Tous les termes commençant par une majuscule et utilisés, mais non définis dans les présentes Conditions Particulière ont le sens qui leur est attribué dans l'Annexe 1 Conditions Générales d'utilisation.

ARTICLE 1 : OBJET

Les présentes Conditions particulières, complétant les Conditions Générales d'utilisation du Service ont pour objet de définir les conditions techniques dans lesquelles le Fournisseur s'engage à rendre le Service au Client.

Les présentes Conditions Particulières prévaudront sur les Conditions Générales d'utilisation du Service payant Rainbow si une contradiction devait apparaître entre ces deux documents.

ARTICLE 2 : DEFINITIONS

En sus des termes définis dans le Glossaire, les termes suivants, tant au singulier qu'au pluriel, ont la signification suivante entre les Parties :

Certification HDS : certification nécessaire à l'exercice de traitement et d'hébergement de données de santé à caractère personnel sur support numérique telle que définie par l'article L 1111-14 à L 1111-24 du Code de la Santé Publique et son décret d'application N° 2018-137 du 26 février 2018.

Conditions Particulières : les présentes conditions.

Client : Personne, physique ou morale qui souscrit à l'offre « Service Rainbow HDS ». Il appartient au Client de s'assurer de son obligation de se faire certifier HDS si nécessaire pour sa propre activité. Dans le cadre de l'hébergement de données de santé, le Client est un professionnel ou un établissement de santé qui dépose des Données de santé par le biais du Service. Il appartient au Client de s'assurer de ses obligations relatives à la PGSSI-S.

Contrat : Ensemble des présentes Conditions Particulières et des Conditions Générales de Services.

Données : Ensemble des données saisies, transmises et/ou traitées par le Client, ses propres Utilisateurs et les Personnes concernées, lors de l'utilisation du Service. Ces données pouvant inclure des Données de santé.

Données de santé à caractère personnel (ou Données de santé) : toutes données relatives à la santé physique ou mentale d'une personne physique, identifiée ou qui peut être identifiée, directement ou indirectement, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soin ainsi que la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

Hébergeur de données de santé - Infogéreur (ou Hébergeur) : personne physique ou morale disposant d'une certification et pouvant, de ce fait, héberger des Données de santé.

Personnes concernées : personne physique à laquelle se rapportent les données à caractère Personnel.

Service : solution de communication, objet des Conditions particulières, par laquelle ALE ou le Revendeur de Service permet au Client de communiquer, partager et stocker des Données avec des Utilisateurs et des Personnes concernées.
UCaaS : Service de Communications Unifiées (Unified Communications As A Service).
Utilisateurs : utilisateurs finaux du Service mis à leur disposition par Vous en qualité de Client du Service ou vos propres utilisateurs, dans le cadre du Service Rainbow HDS. Il s'agit des membres du personnel du Client et des personnes que ce dernier autorise à accéder au Service.

ARTICLE 3 : SERVICE RAINBOW HDS

Dans le cadre de la fourniture du Service, ALE ou un Revendeur Agrée (dans le cadre d'une souscription via un Revendeur Agrée) met à votre disposition un Service de communication pour des échanges de Données conforme à la réglementation HDS.

ALE intervient au titre du Service en qualité d'Hébergeur – infogéreur de Données de Santé au sens des articles L1111-8 et R1111-9 du Code de la Santé Publique et assure dans le cadre du Service les activités suivantes mentionnées aux points 1,2,3,4,5 et 6 de l'article R 1111-9 précité :

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

2- mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de Données de santé ;

3- mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;

4- mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des Données de santé ;

5- administration et l'exploitation du système d'information contenant les Données ;

6- sauvegarde des Données.

Etant entendu que pour les activités 1,2,3 et partiellement l'activité 4 sont sous – traitées à OVH en qualité d'hébergeur de données santé certifié HDS LNE-35608-0

Concernant l'activité 6 Sauvegarde des Données :

- Le Service HDS Rainbow n'est pas un service d'archivage agréé par le Ministère de la culture. Le Service n'inclut pas les services d'archivage et de conservation des Données de Santé, tels que requis dans le cadre de la PGSSI-S (conservation des archives sur les Données des Personnes concernées / patients).
- Cependant, ALE fournit les outils et interfaces nécessaires pour que le Client puisse réaliser ou faire réaliser ces services d'archivage auprès d'un tiers de son choix.
- A cet égard, ALE fournit une extraction mensuelle/ trimestrielle ou annuelle des éléments échangés lors de l'utilisation du service (messages, fichiers) ainsi que des données d'identification du compte de l'Utilisateur (nom, prénom et profils utilisateurs,) soit à un archiveur certifié sur option de paiement supplémentaire, soit au Client si vous réalisez vous-même ledit archivage.

ALE met à disposition sur son site internet les preuves de certification HDS et de certification ISO27001. Tout changement lié à l'activité HDS réalisée par ALE ou par extension tout changement relatif aux normes associées (ISO27001) sera notifiée au Client sous 10 jours ouvrés

Le Service est à destination des établissements et professionnels de santé conformément aux dispositions légales et réglementaires en vigueur.

Les Données à caractère personnel ne sont utilisées que pour servir la finalité du Service (Service de communication, de partage et de stockage des Données). Le traitement des Données mis en œuvre par ALE a pour objectif exclusif de permettre la délivrance du Service de communication que vous avez en qualité de Client avec vos Utilisateurs et/ou les Personnes concernées dans le cadre du domaine de la santé et de permettre le partage et le stockage des Données.

Le Service permet à vos Utilisateurs de soumettre, de partager, d'envoyer et d'afficher des contenus vers et avec d'autres Utilisateurs. À ce titre, vous reconnaissez et convenez (pour vous-même et vos Utilisateurs) que ces contenus ne peuvent être vus que par les participants à la conversation.

Dans le cadre de l'utilisation de ce Service, Vous confirmez en qualité de Client posséder l'ensemble des connaissances de la Réglementation et des référentiels de la PGSSI-S pour utiliser vous-même le Service et uniquement par le personnel habilité à administrer les Données de santé.

En qualité de Client et en qualité de responsable des traitements vous êtes responsable du respect des dispositions réglementaires en vigueur de la PGSSI-S dans le cadre de l'utilisation de ce Service.

3.1 : GESTION DES DONNEES DE SANTE

Les Données que vous stockez sur le Service peuvent comporter des données à caractère personnel ainsi que des Données de Santé. En qualité de Client et responsable des traitements, vous assurez le contrôle du traitement de ces données. Les Parties s'engagent à traiter les Données de santé en conformité avec les dispositions légales et réglementaires en vigueur, notamment en matière de protection des données à caractère personnel et d'hébergement de données de santé. ALE, et toute personne intervenant dans le cadre du Service, n'agissent que sur instruction du Client.

En tant que sous-traitant de données, ALE s'engage à ne pas accéder aux données traitées par ALE pour le compte du Client sauf (i) dans les cas les cas prévus par la loi, (ii) ou dans les cas de maintenance correctives qui seront toutes journalisées et associées à un ticket de support.

ALE assure la sensibilisation de son personnel au respect des exigences légales et réglementaires applicables à la sécurité des Données de santé, en particulier à leur confidentialité et au respect du secret professionnel. À ce titre, ALE fournit à ses employés intervenant dans le cadre du Service une note spécifique dans le cadre de leur contrat de travail concernant la confidentialité des Données.

ALE atteste au travers de son hébergeur OVH, que les Données du Service sont exclusivement localisées en France et donc dans l'Espace Economique Européen (EEE) Cela inclut les environnements de production, de sauvegarde, de journaux et métadonnées.

ALE précise que dans la cadre du Service, il n'y a aucun transfert de Données de santé à caractère personnel vers un pays tiers à l'espace économique européen;

Dans le cadre du Service, le Client est responsable de la conformité des Données traitées aux exigences légales et réglementaires en vigueur, notamment en matière de protection des données personnelles et d'hébergement de données de santé. A ce titre et en sa qualité de responsable des traitements, il est notamment responsable de l'exactitude des Données et de leur mise à jour, de la détermination d'une durée de conservation, de la suppression des données, de l'information préalable des personnes concernées, du recueil des consentements auprès des Personnes concernées requis en application de la réglementation en vigueur, de la gestion des accès des Utilisateurs finaux aux Données de santé, et de la sécurité de ces dernières. Les Parties s'engagent à coopérer avec les autorités de protection des données à caractère Personnel ou de santé compétentes.

Aucun accès aux Données de santé à caractères personnels « DSCP » depuis un pays hors EEE n'est autorisé : Tout accès aux données réalisé par le client en dehors de l'Espace Economique Européen

(EEE) relève de la responsabilité unique du client. A cet égard, ALE recommande au Client en qualité de data contrôleur de mettre en place une politique de sécurité adaptée.

En cas de réception d'une requête provenant d'une autorité administrative ou judicaire par l'une des Parties, ALE sera tenue de transmettre lesdites Données aux autorités compétentes. ALE notifiera le Client d'une demande des autorités excepté dans le cas où la réquisition judiciaire l'interdit.

3.2 : DROIT DES PERSONNES CONCERNEES

3.2.1 : INFORMATION ET CONSENTEMENT

En qualité de Client, vous devez vous assurer de l'information préalable des Personnes concernées concernant l'utilisation du Service, conformément aux dispositions légales et réglementaires en vigueur. Cette information doit comporter les mentions obligatoires en matière de protection des données à caractère personnel, ainsi que les mentions relatives à l'hébergement de données de santé et aux modalités d'accès et de transmission de ces données. L'information préalable des Personnes concernées relative à l'hébergement de Données de santé ne relèvent en aucun cas de la responsabilité d'ALE. Le cas échéant, il revient au Client de s'assurer des modalités d'information préalable auprès des Personnes concernées. Le Client devra transmettre à ses propres Utilisateurs les modalités d'utilisation du Service.

3.2.2 : EXERCICE DES DROITS DES PERSONNES CONCERNEES

Conformément aux dispositions légales et réglementaires en vigueur, notamment en matière de gestion des droits sur les données personnelles et d'hébergement de Données de santé, tout Utilisateur du Service ou Personne Concernée dispose de droits sur ses Données pour autant que ces derniers ne soient pas contraints par d'autres disposition légales prévalentes (par exemple, une Personne Concernée ne devra pas voir une demande de suppression de ses Données de santé aboutir car le Code de la Santé Publique prévoit une durée de conservation réglementée de telles données (à titre d'exemple pendant 20 ans à compter de date du dernier séjour ou de la dernière consultations du patient et réduite à 10 ans à compter de la date du décès du patient dans les établissements publics ou privés ; 10 ans à compter de la stabilisation de la santé du Patient pour les praticiens libéraux).

Il s'agit des droits à la transparence sur les finalités de traitements sur les Données, les droits d'accès et de rectification ou de suppression des Données, les droits d'objection ou d'opposition à toutes ou partie des finalités de traitement des Données, le droit de notification des événements intervenus sur ou ayant affecté les Données, du droit de restriction de traitement ou du droit à la portabilité.

L'Utilisateur du Service responsable de traitement demeure seul responsable du traitement de ces demandes conformément à la réglementation en vigueur notamment les articles L1110-4 et L1111-7 du Code de la Santé Publique et le chapitre III du Règlement 2016/679 du Parlement européen et du Conseil en date du 27 avril 2016.

A cet effet, il revient au Client de traiter ou faire traiter les demandes d'exercice de droits qui lui sont adressées par les Personnes concernées, conformément aux dispositions légales et réglementaires en vigueur. A réception d'une Demande d'exercice de droit par une Personnes Concernée, le Client s'engage à i) authentifier le demandeur, ii) valider la recevabilité de la demande et notamment vérifier que la demande n'entre pas en conflit avec d'autres dispositions légales prévalentes, iii) répondre à la demande dans la mesure de ses possibilités et des moyens mis à sa disposition par ALE dans le cadre du Service (outils d'administration du Service).

ALE fait suivre au Client toutes demandes des Personnes concernées qui voudraient exercer leurs droits.

ALE fournit au Client responsable de traitement l'assistance et la coopération pour le traitement de telles demandes et ce de la manière suivante.

Si le Client démontre n'être pas parvenu à répondre à la demande de la Personne Concernée au regard de ses moyens, alors il pourra transmettre la demande à son revendeur Agréé (dans le cas où ALE n'est pas le Fournisseur) ou à ALE après transmission de la demande du Client par le Revendeur Agréé à ALE (si ALE n'est pas le Fournisseur), ou après la réception de la demande du Client par ALE, ALE s'engage à répondre à cette demande conformément aux dispositions légales et réglementaires en vigueur avec l'accord préalable du Client et dans le respect des délais légaux, dans la mesure où la requête a été reçue par ALE dans les deux jours suivant la demande initiale.

À cet effet :

• Le Client devra identifier le ou les personnes référentes et leur délégués dûment habilitées pour demander au Revendeur Agréé (si ALE n'est pas le Fournisseur) de réaliser ou faire réaliser les actions permettant de répondre aux demandes d'exercice des droits de la Personnes Concernée.
• Le Client devra identifier et adjoindre à la requête un moyen de communication permettant de répondre directement à la Personne Concernée : par exemple, un email de la Personne Concernée demanderesse.
ALE ne pouvant pas identifier les Données de Santé d'une Personne concernée (exemple : échange texte ou de fichiers entre deux médecins concernant un patient), en conséquence il appartient au Client et son responsable de traitement de fournir ses informations à la Personne concernée conformément à la réglementation en vigueur.

Le Client pourra sur demande, soit via son Revendeur Agréé (dans le cas ou ALE n'est pas le Founisseur) ou à ALE demander à consulter les traces d'accès de DSCP portées par des personnels sous son contrôle.

3.2.4 : SECURITE

Dans le cadre de la fourniture du Service, ALE s'engage à prendre toutes précautions utiles, en regard de la nature des Données et des risques présentés par le traitement, pour préserver la sécurité des Données.

ALE s'engage notamment, à mettre en place des mesures de protection ainsi que les mesures techniques et organisationnelles telles qu'elles figurent en Annexe 1 afin d'assurer la confidentialité, l'intégrité et la disponibilité du Service et des Données de santé conformément aux politiques de sécurité et directives du services Rainbow HDS reliées à la déclaration d'applicabilité issue des certification ISO 27001 et HDS.

La Déclaration d'Applicabilité (DDA) relative à la certification HDS d'ALE est disponible sur demande et en français au support Rainbow par email à support@openrainbow.com.

Les Parties s'engagent, en particulier, à respecter les principes fondateurs de la PGSSI-S
(Politique générale de sécurité des systèmes d'information de santé) et à se conformer aux référentiels techniques et aux guides associés.

Il incombe à ALE de :

- Fournir au Client, tout au long du Service et par le biais d'une interface, un accès, individuel et sécurisé, reposant sur des moyens d'authentification forte, aux Données hébergées chez ALE dans le cadre du Service.
- Formaliser une politique de sécurité dont le champ d'application couvre le Service et les Données ;
- Assurer la sécurité de l'architecture réseau et des services liés au Service En particulier, ALE s'engage à ce qu'en aucun cas des Données ne transitent en clair sur un réseau public.
- Maintenir la confirmité HDS et ISO 27001:2022
- Sensibiliser son personnel à la confidentialité et au respect du secret professionnel, et plus particulièrement concernant les Données de santé à caractère personnel déposées dans le cadre du service conformément à la clause de confidentialité telle qu'elles figurent dans leur contrat de travail.

• Assurer la mise en place contractuelle d'accord de non divulgation avec ses sous-traitants ayant possiblement accès à des données personnelles. Il est précisé que lesdits sous-traitants ne peuvent accéder qu'a des données d'identification des personnes dans le cadre du support mais en aucun cas au contenu des échanges dès lors que le Client à bien veillé à ne pas inclure des Données de Santé dans ses tickets de support.
• Assurer la traçabilité des accès et des opérations réalisées sur le Service et les Données, tant par son personnel que par les Utilisateurs conformément à la loi LCEN;
- Sauvegarder pendant une durée de douze (12) mois les journaux de connexion et mettre en œuvre les moyens techniques permettant l'extraction des données permettant l'archivage des Données
- Gérer les Incidents de sécurité et informer le Revendeur Agréé qui en informera le Client en cas en cas d'atteinte à la sécurité des Données selon la réglementation en cours
- Mettre en œuvre un plan de continuité et de reprise d'activité.

Il est précisé au Client que l'ensemble des Données et des fichiers échangés dans le cadre du Service ALE sont conservées pendant la durée du Contrat.

Toutefois, Le Client reconnait expressément qu'ALE reporte la couverture de certaines obligations légales et réglementaires vers le Client. A cet effet, les obligations suivantes dans le cadre du Service relèvent exclusivement de votre responsabilité en qualité de Client :

• S'assurer que ses propres Utilisateurs intervenant dans le cadre du Service, gèrent les Données de santé dans le respect de la PGSSI-S ;

• Formaliser une politique de sécurité dont le champ d'application couvre les Données de santé ;

• Assurer la sécurité des postes de travail et des équipements à partir desquels ses Utilisateurs, et toute personne autorisée par le Client, accèdent aux applications et aux Données de santé ;

• Gérer finement les habilitations, l'identification, l'authentification et le contrôle d'accès de son personnel et des utilisateurs aux applications et aux Données de santé ;

- Veiller à ne pas inclure de Données de santé dans les tickets ouverts vers le support du Revendeur.

• Contrôler l'utilisation des moyens d'authentification forte par les personnes habilitées à accéder aux Données de santé ;

- Sensibiliser et former votre personnel à la sécurité des systèmes d'information ;
- Sensibiliser son personnel à la confidentialité et au respect du secret professionnel, et plus particulièrement concernant les Données de santé à caractère personnel déposées dans le cadre du service, et identifier les Utilisateurs seuls habilités à accéder aux Données de santé;
- Archiver et conserver les Données de Santé conformément à la réglementation PGSSI-S
- Transmettre et mettre à jour la Liste des Points de contacts telle qu'elle figure en Annexe 2.

3.2.5 : GESTION DES ACCES AUX DONNEES DE SANTE

Conformément aux dispositions légales et réglementaires en vigueur, l'accès aux Données de santé est réservé aux personnels de santé et aux personnes placées sous l'autorité du Client.

Le Client est responsable de la gestion des habilitations des Utilisateurs finaux du Service, de toute personne qu'il aurait individuellement autorisée à accéder aux Données de Santé et, le cas échéant, des Patients. Il est également responsable de la mise en œuvre des accès correspondants et du contrôle de l'utilisation des moyens d'accès, dans le respect des dispositions légales et réglementaires en vigueur.

S'agissant du personnel technique, le Client s'engage à n'accorder un droit d'accès aux Données de santé qu'aux personnes, individuellement identifiées, ayant strictement besoin de les connaître et qui sont liées contractuellement au Client. Il est rappelé au Client que, conformément aux

dispositions légales et réglementaires en vigueur, ces personnes sont soumises au secret professionnel.

Il revient au Client de s'assurer que les personnels techniques accédant aux Données de santé :

• sont qualifiés pour réaliser les opérations sur les Données de santé et pour assurer la sécurité de ces données ;
• sont sensibilisés à la gestion des Données de santé et au respect de la vie privée des Personnes concernées ;
• sont sensibilisés au respect du secret professionnel ;
• disposent d'une clause de confidentialité dans leur contrat de travail ;
• maîtrisent les mesures de sécurité renforcées spécifiques aux Données de santé ;
• utilisent des comptes d'accès individuels ;
• sont dotés de moyens d'authentification conformes à l'état de l'art, à savoir unidentifiant/mot de passe conforme aux recommandations de la CNIL et des moyens d'authentification forte, comme, par exemple, l'utilisation des cartes de professionnels de santé (CPS) comme deuxième facteur d'authentification.

S'agissant des Utilisateurs, le Client a seul la responsabilité de veiller à ce qu'ils :
• soient juridiquement autorisés à accéder aux Données de santé et à intervenir sur les traitements de Données de santé ;
• soient soumis au respect du secret professionnel, et notamment du secret médical ;
• accèdent aux Données de santé dans le respect des dispositions légales et réglementaires en vigueur.

Le Client est responsable de la gestion des accès délivrés aux Personnes concernées. Il s'assure notamment que la qualité de l'identité des Personnes concernées sont fiables et de l'utilisation de moyens d'authentification forte conformes à l'état de l'art.

Dès lors que le Client utilise le Service, il lui revient, conformément aux dispositions légales et réglementaires en vigueur, de vérifier les accès directs de la Personne concernée au Service.

ALE et/ou le Revendeur Agréé ne sauraient en aucun cas être tenus pour responsables de toute conséquence d'une utilisation erronée par les Utilisateurs du Client ou par toute personne à laquelle le Client aura fourni un accès.

3.2.6 : EVOLUTION MAJEURE DU SERVICE

Toute évolution majeure du Service, étant à l'initiative d'ALE, n'entrainera pas de régression, ni de non-conformité quant aux exigences concernant la protection des Données de santé et la protection des Données à caractère personnel. ALE s'engage à assurer la continuité de service au cours des évolutions majeures. ALE s'engage à informer le Client de toute évolution majeure, conformément aux exigences légales et réglementaires en vigueur en matière d'hébergement de données de santé.

3.2.7 : SUPPORT DE LA LANGUE FRANCAISE

L'application est disponible dans son intégralité en langue française. Le support de premier niveau est lui aussi accessible en langue française.

3.2.8 : GESTION DES INCIDENTS

Les Parties s'engagent à coopérer dans la gestion de tout Incident (à l'exclusion de tous les incidents liés à une mauvaise utilisation du Service, un non-respect de l'état de l'art sur la sécurité des actifs du périmètre du Déposant ou du Prestataire, etc.). ALE s'engage à informer de tout incident dont il a eu connaissance et qui est susceptible d'affecter les Données de santé dans les meilleurs délais avec un objectif de 48 Heures le Revendeur Agréé qui en informera le Client,

La communication est assurée via le Service Client Rainbow. Une cellule de crise est organisée pour identifier les causes et les actions correctives à mettre en place. Pendant cette période de gestion

de crise, le Service peut passer en mode dégradé (par exemples par confinement du système impacté, filtrage ou surveillance active, etc.). La remise en ligne du service peut notamment être effectuée grâce au Plan de Continuité d'Activité. Le cas échéant, le Client s'assure de l'information des autorités compétentes concernées, des Utilisateurs et des Personnes concernées dans les délais règlementaires. Dans le cas où ALE détecterait que le Service est corrompu, ou subit un dysfonctionnement, ALE se réserve le droit de limiter le service jusqu'à la résolution du problème, sous réserve qu'elle estime qu'une telle résolution est possible.

Sont exclus de ce processus tous les Incidents liés à une mauvaise utilisation du Service par le Client, un non-respect de l'état de l'art par le Client sur la sécurité des actifs de leur périmètre.

3.2.9 : POINT DE CONTACT

Les Parties (ALE, le Revendeur Agréé du Service et le Client), s'engagent à désigner chacune un interlocuteur principal et un interlocuteur secondaire, en charge de la bonne exécution du Service, et notamment des problématiques de sécurité. Ce point de contact doit être en mesure de désigner à ALE un professionnel de santé lorsque cela est nécessaire (exemple : Accès aux Données de santé, gestion des relations avec le patient).

Le Client s'assure de la désignation au minimum d'un interlocuteur principal et secondaire, en charge des problématiques sur le traitement des Données de santé sur le Service. Le Client transmet au Revendeur Agréé ses points de contact et s'assure de la connaissance des interlocuteurs par le Revendeur Agréé (au cas où ALE ne soit pas le revendeur du Service). A cet égard, le Client s'engage à remplir la Fiche Point de Contact en Annexe 2 et s'assurer de sa régulière mise à jour, cette fiche devant être transmise à ALE via son Revendeur Agréé. Le Revendeur Agréé soumet pour cela un eService Request (eSR) avec cette Fiche Point de Contact attachée en indiquant les mots clés suivants dans le eSR : « HDS » et « Contact ».

L'ensemble de ces interlocuteurs doivent permettre une prise de contact entre les Parties.

ARTICLE 4 : SOUS-TRAITANCE

Le Client est informé qu'ALE fait appel à des sous-traitants dans le cadre de l'exécution du Service dont la liste figure en Annexe 3.

1. Le Service est hébergé chez un hébergeur certifié HDS.

Etant entendu qu'en cas de multiplicité d'offres d'Hébergeur et/ou de localisation de Data center par ALE dans la liste de ses sous-traitants en Annexe 3, le Client aura le choix de la localisation de ses Données.

ALE est susceptible de modifier la liste de ses sous-traitants à tout moment telle qu'elle figure en Annexe 3, sous réserve d'en informer le Client au préalable.
ALE s'engage à reporter, dans les engagements qu'il contractera avec le sous-traitant les obligations qui lui incombent au titre dispositions légales et réglementaires en vigueur, à cet égard ALE a conclu un accord sur la sous-traitance des données conformément au RGPD.

ARTICLE 5 : RESPONSABILITE

TOUTES LES DISPOSITIONS DE L'ARTICLE 9 DES CONDITIONS GENERALES D'UTILISATION DU SERVICE RAINBOW PAYANT S'APPLIQUENT DANS SON INTEGRALITE.

EN OUTRE, TOUTE RESPONSABILITÉ DU FOURNISSEUR DE SERVICE, DE SES SOCIÉTÉS AFFILIÉES, TOUT FOURNISSEUR TIERS AYANT ÉTÉ IMPLIQUÉ DANS LA FOURNITURE DU SERVICE HDS (Y COMPRIS SANS LIMITATION, ALE DANS LES CAS OU VOUS AVEZ ACHETÉ LE SERVICE AUPRÈS D'UN REVENDEUR AGRÉÉ), LEURS ADMINISTRATEURS, DIRIGEANTS, SALARIÉS ET AGENTS RESPECTIFS DANS LEUR ENSEMBLE, NE PEUT ETRE ENGAGEE (i) EN CAS DE NON RESPECT LE CLIENT DE SES

PROPRES OBLIGATIONS LEGALES (ii) DE LA DIVULGATION OU DE L'UTILISATION ILLICITE DU MOT DE PASSE REMIS CONFIDENTIELLEMENT AU CLIENT (iii) DESTRUCTION PARTIELLE OU TOTALE DES INFORMATIONS TRANSMISES OU STOCKEES A LA SUITE D'ERREURS IMPUTABLES DIRECTEMENT OU INDIRECTEMENT AU CLIENT (IV) EN CAS DE PERTE OU DE DETERIORATION DES DONNEES CONFIEES A ALE DANS LE CADRE DU SERVICE.

ETANT RAPPELE QU'ALE ASSURE DES SAUVEGARDES DES DONNEES DANS LE CADRE DU SERVICE, MAIS CELA NE SAURAIT DISPENSER LE CLIENT D'EFFECTUER UNE SAUVEGARDE COMPLETE DE SES DONNEES A DES FINS D'ARCHIVAGE. IL EST RAPPELE A CET EGARD QU'IL EST DE LA RESPONSABILITE DU CLIENT DE S'ASSURER REGULIEREMENT DE L'ARCHIVAGE DES DONNEES DE SANTE ET DE LEUR CONSERVATION SUR UN SUPPORT INFALSIFIABLE CONFORMEMENT A LA REGLEMENTATION EN VIGUEUR.

ARTICLE 6 : PLAN DE REPRISE D'ACTIVITE ET PLAN DE CONTINUITE D'ACTIVITE

Des mécanismes et fonctionnalités permettent d'assurer la disponibilité et la continuité du Service. ALE rappelle que le Service établie et maintient un plan de continuité d'activité (PCA) ainsi qu'un plan de reprise d'activité (PRA).
Ces documents décrivent la nature des dispositifs, les activités de test des dispositifs réalisés par ALE ainsi que les conditions de déclenchement du PCA et du PRA.
Les valeurs de RTO (Objectif de délai de récupération) et RPO (Objectif de point de récupération) sont respectivement fixé à 48 heures et 24 heures.

ARTICLE 7 : Indicateur de qualité et performance

ALE fournit un service continu permettant d'avoir une vue de l'état du service et des opérations en cours via la site https://status.openrainbow.health/. Ces mesures sont prises en continu.

Le taux de disponiblité du service proposé est de 99,5%.

ALE ne propose pas de système de pénalités applicable en cas de non respect des objectifs de disponibilité.

ARTICLE 8 : AUDIT – CERTIFICATION HDS

8.1 Dans le cadre de l'organisation du Service, ALE a mis en place un système de management de la sécurité de l'information certifié HDS. ALE s'engage à maintenir cette certification (ou toute certification équivalente) pendant la durée du Contrat, et dans ce cadre, mandate chaque année un organisme accrédité pour réaliser un audit de suivi et tous les trois ans afin de délivrer la certification HDS. Cet organisme accrédité mandate un auditeur reconnu dans ce domaine, afin d'auditer le Service conformément aux dispositions du référentiel HDS.

8.2 Dans le cadre du référentiel HDS, le Client peut dans les conditions prévues de la procédure d'audit du Service réaliser ou faire réaliser à leur propre charge un audit portant sur le respect du référentiel HDS.
8.3 En cas de perte de sa Certification, ALE en informe sans délai le Revendeur Agréé qui en informe le Client. Dans une telle circonstance, le Client peut résilier de plein droit le Contrat et ce sans indemnité. Le Service étant conditionné à la certification HDS d'ALE, le Client reconnaît que toute perte de certification par ALE implique l'obligation pour lui de récupérer les Données de santé qu'il aurait échangées dans le cadre du Service.

Dans cette hypothèse, ALE s'engage à accompagner le Client pour la pleine récupération des Données de santé, dans les conditions prévues à l'article 8. Réversibilité.

8.4 ALE s'engage fournir, sur demande le dernier rapport d'audit de certification HDS par email à support@openrainbow.com

8.5 Le client peut demander à ALE de founir une synthèse managériale d'un rapport d'audit technique portant sur les ressources mutualisées dans le cadre du service. Le rapport d'audit ne devra pas dater de plus de 3 ans.

ARTICLE 9: REVERSIBILITE

ALE assurera la restitution des Données au Client dans les trente (30) jours suivant la réception d'un ticket demandant la restitution des données, suite à une fin du Service c'est à dire la fin de votre Contrat d'Abonnement et ce quelle que soit la cause.
Pour la demande de restitution, le Revendeur Agréé s'engage à ouvrir un ticket auprès d'ALE sur le Business Portal afin de demander la restitution des données. Ce ticket aura pour objet « Reversibility HDS ». Les données seront restituées par ALE au Client dans les trente (30) jours.
A compter de la demande de la fin de Service pour le Client concerné, le Revendeur Agréé s'engage à ne modifier aucune des données et configurations de ce Client et à ne pas détruire la compagnie Rainbow créée dans l'environnement HDS.
Les modalités de récupération de leurs Données par le Client se fera dans un format de fichier numérique défini par ALE, lisible par le Client. Les DSCP et metadonnées seront fournies dans des formats ouvert. Les documents attachés conserveront leur format d'origine.
A cet effet, le Client mettra à disposition d'ALE un espace d'accueil sécurisé des données et définira avec ALE et le Revendeur Agréé les médias sécurisés à utiliser (courriel, texto, ..) afin d'échanger les informations de contrôle d'intégrité et de droits d'accès.
Le Client est informé qu'ALE procédera à la suppression de l'ensemble des Données que le Client aurait déposé sur le Service soixante (60) jours suivant la fin du Service.
A l'issue de cette période de soixante (60) jours, les données seront supprimées et ni ALE, ni le Revendeur Agréé ne pourront être tenus pour responsable d'un défaut de réconciliation des Données qui n'aurait pas été dûment détecté par le Client lors de la réversibilité. La vérification de la complète restitution des Données est sous la seule responsabilité du Client.
Sous réserve des données qu'ALE se doit de conserver conformément à la réglementation en vigueur et des données nécessaires à la défense de ses droits, ALE s'engage, à la fin des opérations de réversibilité, à ne conserver aucune copie des données concernées.
ALE ne facture pas de coûts en regard de la réversibilité dans la mesure ou les extractions et échanges ne prennent pas plus de trois (3) jours travaillés. Si la durée devait être étendue du fait des volumes de données ou des ralentissements du fait du Client, ALE pourrait demander un paiement au temps passé au-delà des 3 jours. Cette règle ne s'appliquera pas dans le cas ou ALE serait responsable de la perte de sa certification HDS.

Liste des Annexes :
ANNEXE 1 – MESURES TECHNIQUES ET ORGANISATIONNELLES
ANNEXE 2 – FICHE POINT DE CONTACTS SERVICE RAINBOW HDS – CLIENT
ANNEXE 3 – LISTE DES SOUS-TRAITANTS
ANNEXE 4 – CERTIFICATS HDS

Annexe 1
Mesures techniques et organisationnelles
ALE Rainbow

Contenu

1. Confidentialité

Contrôle d'accès aux installations

Contrôle d'accès aux ressources informatiques

Contrôle d'accès aux processus et aux données

Contrôle de séparation – séparation des tâches

Pseudonymisation

2. Intégrité

Contrôle des transferts

Contrôle des entrées

3. Disponibilité et capacité de charge de l'

Contrôle de la disponibilité

Contrôle de la capacité de charge

4. Procédures de révision, d'analyse et d'évaluation régulières

Gestion de la protection des données

Délégué à la protection des données

Gestion des incidents

Paramètres par défaut respectueux de la vie privée – protection de la vie privée dès la conception

Gestion des contrats

Avant-propos
L'objectif du présent document est de répertorier les mesures techniques et organisationnelles mises en place chez ALE, qui concourent à protéger de manière adéquate non seulement les données en général, mais aussi et surtout les données à caractère personnel.
Ces mesures visent à répondre aux objectifs de contrôle standard en matière de confidentialité, d'intégrité et de disponibilité, qui constituent une méthodologie standard permettant de démontrer qu'un niveau adéquat de protection des données existe et est efficace.
Identification des responsabilités :
Dans le cadre du service Rainbow, ALE est le responsable du traitement et le sous-traitant dans toutes les situations, sauf lorsque le service est fourni à partir d'un cloud privé exploité par une entité autre qu'ALE. Ainsi, sauf dans ce dernier cas, ALE est le sous-traitant et sous-traite l'hébergement et la connectivité du centre de données ainsi que la sécurité de celui-ci.
Sécurité certifiée
Rainbow est certifié selon les normes DIN ISO 27001:2013, ISO 27017 et ISO 27018, qui peuvent être consultées à tout moment sur https://support.openrainbow.com/hc/fr/articles/360003802400-ISO-Certification-EN-

Hébergement chez OVH

OVH s'engage à garantir la sécurité optimale de ses infrastructures, notamment par la mise en œuvre d'une politique de sécurité des systèmes d'information. De plus, les infrastructures d'OVH sont conformes à de nombreuses normes internationales et certifiées selon les normes PCI DSS, ISO/IEC 27001, SOC 1 TYPE II et SOC 2 TYPE II, etc.
Pour plus d'informations sur la protection et la sécurité des données chez OVH, rendez-vous sur https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml#accordion_1872-1.

1. Confidentialité

1.1 Contrôle d'accès physique et sécurité

Protection de l'accès physique ; centre de données (OVH

Le centre de données est exploité par le fournisseur OVH. Vous trouverez plus de détails sur les mesures de sécurité à l'adresse https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml.

Mesures de sécurité générales des sites physiques
L'accès physique repose sur une sécurité contextuelle restrictive, qui s'applique dès la zone d'entrée. Chaque site est divisé comme suit :

- Zones de circulation privées
- Bureaux accessibles à tous les employés et aux visiteurs enregistrés
- Bureaux privés accessibles uniquement au personnel autorisé
- Zones abritant les équipements du centre de données
- Zones privées du centre de données
- Zones du centre de données abritant des services critiques
- Mesures de sécurité générales des sites physiques

Les mesures de sécurité suivantes sont mises en œuvre pour contrôler l'accès aux sites physiques d'OVH :

- Une politique d'autorisation d'accès
- Des cloisons (ou installations similaires) entre chaque zone
- Caméras aux entrées et sorties des locaux et dans les salles de serveurs
- Accès sécurisé, contrôlé par des lecteurs de badges
- Barrières laser sur les parkings
- Système de détection de mouvement
- Mécanismes anti-effraction aux entrées et sorties des centres de données
- Mécanismes de détection des intrusions non autorisées (service de sécurité et vidéosurveillance 24 heures sur 24)
- Centre de surveillance permanent qui surveille l'ouverture des portes d'entrée et de sortie

Le contrôle d'accès physique est assuré par un système de badges. Chaque badge est lié à un compte OVH, lui-même lié à une personne spécifique. Grâce à ce système, chaque personne présente dans les locaux peut être identifiée et les mécanismes de contrôle authentifiés :

- Toute personne entrant sur les sites d'OVH doit disposer d'un badge personnel lié à son identité.
- Chaque identité doit être vérifiée avant la délivrance d'un badge.
- Le badge doit toujours être porté de manière visible dans les locaux.
- Les badges ne doivent pas indiquer le nom de leur propriétaire ni le nom de l'entreprise.
- Il doit être possible d'identifier immédiatement la catégorie de personnes présentes à l'aide du badge (employés, tiers, accès temporaire, visiteurs).
- Le badge sera désactivé dès que son titulaire ne sera plus autorisé à accéder aux locaux.
- Les badges des employés d'OVH sont activés pour la durée du contrat de travail ; pour les autres catégories,
- le badge est automatiquement désactivé après une période déterminée. Les badges qui ne sont pas utilisés pendant trois semaines sont automatiquement désactivés.

Accès aux portes par badge. Il s'agit du système de contrôle d'accès standard dans les locaux d'OVH :

- La porte est reliée au système central de gestion des autorisations d'accès.
- La personne doit présenter son badge devant le lecteur spécial pour déverrouiller la porte.
- Chaque accès est vérifié lors de la lecture afin de s'assurer que la personne dispose de l'autorisation appropriée.
- En cas de défaillance du système central de gestion des autorisations d'accès, les autorisations configurées au moment de la défaillance restent valables pendant toute la durée de l'incident.

- Les serrures des portes sont protégées contre les coupures de courant et restent fermées dans ces situations.

Accès aux portes par clé. Certaines zones ou certains équipements sont équipés de serrures pouvant être verrouillées à l'aide de clés :

- Les clés de chaque site sont conservées dans un lieu centralisé à accès restreint et répertoriées dans un inventaire.
- Chaque clé est munie d'une étiquette d'identification.
- Un inventaire des clés est tenu à jour. Chaque utilisation des clés peut être suivie au moyen d'un mécanisme de gestion ou d'un registre papier.
- La liste d'inventaire des clés est vérifiée quotidiennement par rapport à l'inventaire.

Accès aux centres de données via des sas à une personne. L'accès à nos centres de données se fait exclusivement via des sas à une personne :

- Chaque sas se compose de deux portes et d'une zone fermée entre les commandes afin de garantir qu'une seule personne passe à la fois.
- Une porte ne peut être ouverte que lorsque l'autre est fermée (sas).
- Les sas utilisent le même système de badges que les autres portes et les mêmes règles s'appliquent.
- Des mécanismes de détection vérifient qu'une seule personne se trouve dans le sas (anti-piggybacking).
- La configuration du système empêche l'utilisation du badge plus d'une fois dans le même sens (anti-passback).
- Grâce à une caméra installée dans la zone du sas, les accès peuvent être surveillés.

Accès aux sas de marchandises. Les marchandises sont réceptionnées dans les centres de données exclusivement via des passages spécialement conçus :

- La zone de livraison est configurée de la même manière qu'un sas pour une seule personne, mais avec plus d'espace, sans contrôle de volume ni de poids, et avec des lecteurs de badges situés uniquement à l'extérieur du sas.
- Seul l'article livré passe par la zone de livraison ; les personnes doivent entrer par les sas à une personne.
- Dans la zone de livraison, une caméra sans angle mort est installée.

Protection des accès aux installations ALE

Sur les sites ALE, des équipes disposent d'un accès à distance à l'instance Rainbow.

Mesures de protection de l'accès physique

Systèmes de verrouillage

ALE utilise généralement des systèmes de contrôle d'accès électroniques. Les autorisations d'accès correspondantes sont attribuées sur le plan organisationnel et technique par du personnel autorisé. Il existe des règles relatives à l'utilisation des systèmes de verrouillage électroniques, par exemple sur la manière dont les employés doivent se comporter en cas de perte d'un transpondeur.

Des systèmes de verrouillage manuels sont parfois encore utilisés pour les sites ALE de plus petite taille.

Cartes d'identité / badges ALE

Les badges ALE sont obligatoires et indiquent le statut (employé, visiteur, invité ou non-employé). Ils restent la propriété de l'entreprise et doivent être portés de manière visible.

Politique relative aux visiteurs

Les visiteurs sont enregistrés et toujours accompagnés par un employé d'ALE.

Zones sensibles

L'accès aux zones sensibles (par exemple, le centre de données) est autorisé et enregistré selon le principe du strict nécessaire. Les zones sensibles sont également surveillées en dehors des heures de bureau habituelles.

Zones de livraison et de chargement

Les zones de livraison et de chargement utilisées pour la réception ou la distribution des biens d'ALE sont équipées d'une porte extérieure et d'une porte intérieure qui ne s'ouvrent pas simultanément.

Vidéosurveillance

La vidéosurveillance / télévision en circuit fermé (CCTV) couvre les principaux points d'entrée, le hall principal, la rampe de chargement et les parkings des grands sites.

Politique du bureau rangé

Chaque bureau doit être rangé à la fin de la journée de travail, les ordinateurs doivent être éteints.

Fenêtres de sécurité

Des limiteurs d'ouverture sont installés sur les fenêtres du rez-de-chaussée.

1.2 Contrôle d'accès aux ressources informatiques

Contrôle d'accès aux ressources d'infrastructure (hébergeur OVH)

- Tous les employés utilisent des comptes utilisateurs nominatifs.
- Les sessions de connexion ont systématiquement une durée d'expiration adaptée à chaque application.
- Avant toute modification des méthodes d'authentification, l'identité des utilisateurs est vérifiée.
- L'utilisation de comptes standard, génériques et anonymes est interdite.
- Tous les accès aux ressources sont gérés via une authentification par clé SSH individuelle. La validité des clés SSH individuelles doit être renouvelée tous les 3 jours.
- Tous les accès sont enregistrés, stockés et examinés régulièrement

Contrôle d'accès aux ressources d'infrastructure dans les locaux d'ALE

Gestion des identités et des accès
La gestion des identités et des accès est fondée sur la fonction ou la tâche à accomplir et reflète les principes de séparation des tâches et du principe du moindre privilège.

Identifiant utilisateur unique et accès
Chaque personne se voit attribuer un **identifiant utilisateur** unique pour accéder aux ressources d'information d'ALE.
Les noms de compte doivent permettre de distinguer les comptes utilisateur, administrateur (privilégié) et de service.

Identifiant utilisateur / compte de service Authentification et gestion des mots de passe

Les mécanismes d'authentification peuvent être :
i) mot de passe / code PIN ou
ii) à deux facteurs (tels qu'un mot de passe ou un code PIN associé à un dispositif matériel, un jeton logiciel ou un certificat numérique).

Politique relative aux mots de passe
Les mots de passe doivent comporter au moins huit (8) caractères pour les comptes d'utilisateurs et vingt (20) caractères pour les comptes de service. Les mots de passe doivent contenir au moins trois des quatre catégories suivantes : lettres majuscules, lettres minuscules, chiffres, caractères spéciaux.

Surveillance de l'utilisation des systèmes d'information de l'ALE
- Veiller au respect des lois et réglementations applicables ;
- Détecter toute violation des lois et réglementations applicables ;
- Garantir l'utilisation efficace des systèmes d'information et leur fonctionnement normal ;
- Garantir la confidentialité et l'intégrité effectives des données d'ALE ainsi que le respect par les employés de leurs obligations en matière de sécurité ;
- Garantir la sécurité effective des systèmes d'information d'ALE en mettant en œuvre des fonctionnalités de détection des menaces de sécurité, notamment les virus, chevaux de Troie, vers, logiciels malveillants et spams (messages indésirables), ainsi que la protection contre ceux-ci et les enquêtes judiciaires.
- Assurer la maîtrise des coûts.

(sans s' limiter à ce qui précède)

Mesures organisationnelles

- Directives en matière d'authentification
- Directive relative à la sécurité de l'information
- Directives relatives à l'utilisation de l'intranet et d'Internet
- Directive relative à la communication par courrier électronique

Autres mesures techniques

- Utilisation de pare-feu professionnels
- Utilisation de logiciels antivirus
- Utilisation de systèmes de détection d'intrusion
- Gestion des proxys Internet
- SSO/SAML
- Restriction de l'accès aux serveurs

Contrôle d'accès des utilisateurs dans Rainbow

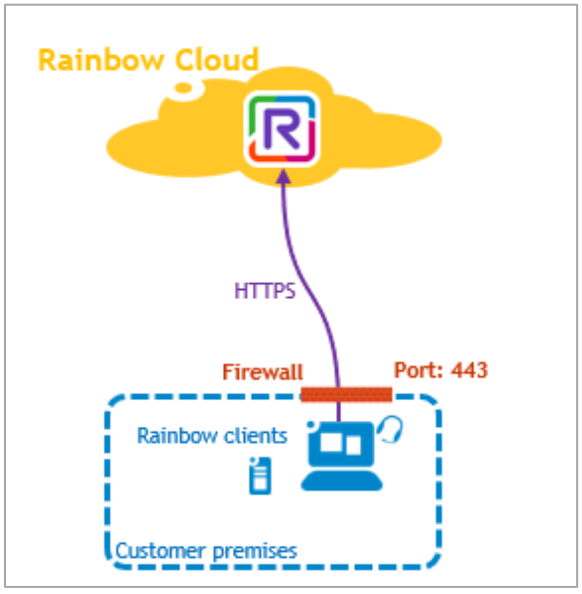
Rainbow offre différentes possibilités pour authentifier les utilisateurs

a) Authentification interne

Par défaut, les utilisateurs Rainbow sont authentifiés par le service Rainbow. Dans ce cas, Rainbow sait comment vérifier les identifiants de l'utilisateur et est responsable de cette vérification. Lorsqu'un utilisateur ouvre l'application Rainbow UCAAS, le formulaire de connexion Rainbow s'affiche et est utilisé pour l'authentification.

- Laissez Rainbow gérer entièrement les règles de sécurité relatives aux identifiants et mots de passe.
- Sous le contrôle de l'administrateur Rainbow.
- Rien à configurer, c'est la solution par défaut.

Authentification interne



L'authentification interne met en œuvre plusieurs règles de sécurité :

- Lors de l'auto-inscription, un e-mail est envoyé pour vérifier la création du compte.
- Les mots de passe des utilisateurs doivent respecter un niveau de complexité minimum
  Au moins 8 caractères (64 au maximum)
  - 1 lettre minuscule
  - 1 lettre majuscule

- 1 chiffre et
- 1 caractère spécial.

- La réinitialisation du mot de passe est sécurisée par un code PIN temporaire à 6 chiffres envoyé à l'adresse e-mail de l'utilisateur
- Il doit ensuite être saisi lors de la phase de mise à jour du mot de passe

Le contrôle d'accès aux services Rainbow repose sur le rôle attribué par l'administrateur aux utilisateurs :
- Invité
- Utilisateur
- Administrateur de l'entreprise

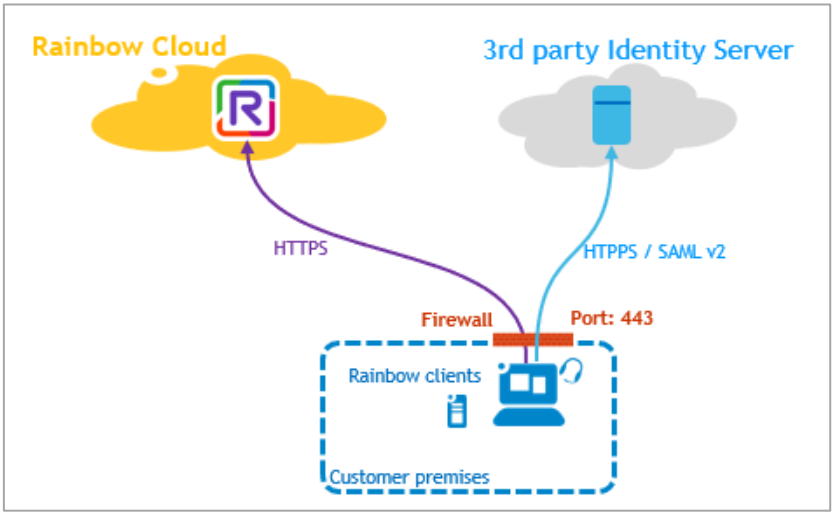
b) Authentification externe

Présentation

- Délègue les règles de sécurité relatives aux identifiants et mots de passe à un serveur d'authentification centralisé externe (par exemple, MS Azure AD).
- Permet de partager le même mot de passe avec plusieurs applications
- Prend uniquement en charge les serveurs d'authentification dans le cloud.
- Prise en charge depuis les PC et les smartphones (iOS, Android).
- Prend en charge les protocoles HTTPS/SAML v2 et OIDC (OpenID Connect).
- OIDC (OpenID Connect) est basé sur OAuth2
- SAML v2 (Security Assertion Markup Language)

Détails
La solution Rainbow permet d'utiliser un fournisseur d'identité externe basé sur SAML et OIDC. Dans ce cas d'utilisation, d'un point de vue administratif, l'administrateur du service d'authentification de l'entreprise doit déclarer un nouveau service externe dans le service d'identité externe (comme dans l'interface d'administration de Microsoft Azure) utilisé par l'entreprise afin de permettre à Rainbow d'interagir avec celui-ci lorsqu'un utilisateur doit se connecter.

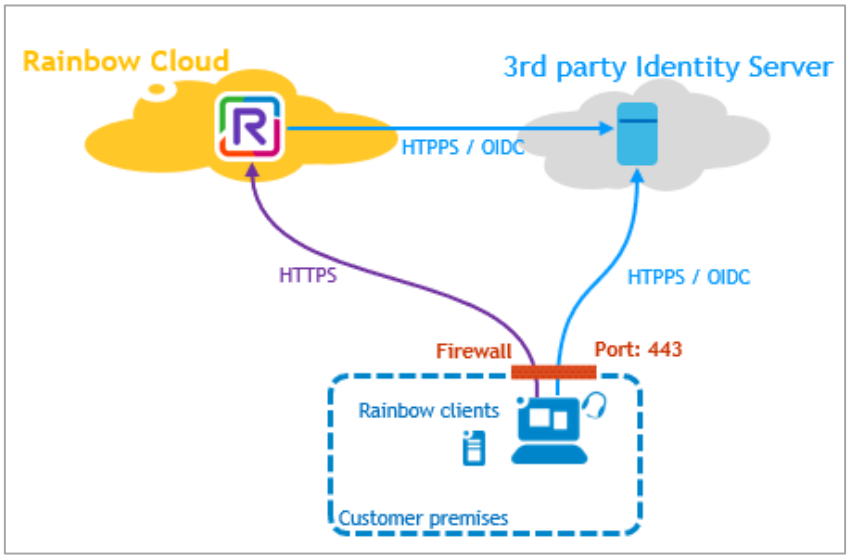
Authentification externe via SAML V2
Le Security Assertion Markup Language (SAML v2) est un protocole utilisé pour l'authentification. Ce protocole est largement utilisé, car il est déployé dans le monde de l'entreprise depuis longtemps. Cette technologie repose principalement sur des interactions avec les navigateurs Web. Ce protocole permet de donner accès à une ressource protégée, en utilisant un service d'authentification centralisé sans donner accès aux identifiants à des entités externes. Par exemple, vous pouvez vous connecter à votre compte Rainbow à l'aide de votre identifiant et de votre mot de passe d'entreprise, mais Rainbow ne doit pas avoir accès aux identifiants de l'entreprise. Comme il existe une dissociation entre la ressource protégée et l'élément qui contrôle l'identité, SAMLv2 permet à l'utilisateur d'utiliser les mêmes identifiants pour accéder à un large éventail de ressources ou de services protégés. Ce cas d'utilisation est également bien connu sous le principe de l'authentification unique (SSO).



Authentification externe via OAuth2
OAuth2 est un framework conçu pour accorder des autorisations. Plus récent que SAMLv2, il est moins lié au navigateur Web et

davantage orienté API. Il est rapidement devenu très populaire et largement utilisé. OAuth2 est conçu pour accorder des autorisations et non pour l'authentification. De nombreuses applications utilisaient OAuth2 pour effectuer également l'authentification (et c'est toujours le cas). Comme il faut identifier la personne pour demander une autorisation, cela ne pose pas de problème. Mais chaque application doit définir une méthode spécifique pour renvoyer l'identité de l'utilisateur à l'application externe. C'est ce que l'OIDC est censé faire, mais dans un format bien normalisé.

Authentification externe via OIDC
Open ID Connect (OIDC) est un protocole basé sur OAuth2 qui permet d'effectuer l'authentification (comme le fait SAML). OIDC est également utilisé pour mettre en œuvre l'authentification unique (SSO). OIDC hérite des technologies et de la popularité d'OAuth2 et finira par remplacer SAMLv2.



Chiffrement et sécurité

- Les mots de passe des utilisateurs finaux sont hachés et salés dans la base de données interne de Rainbow.
- Toutes les données (messages instantanés, fichiers) échangées entre les utilisateurs ou via les bulles sont chiffrées en transit et au repos.
- Pour le transit, HTTPS + WSS via TLS 1.2/1.3 uniquement
- Au repos, l'AES 256-GCM est utilisé
- Les communications vocales/vidéo sont chiffrées en natif à l'aide de la technologie WebRTC utilisant DTLS et SRTP.
- Tous les fichiers téléchargés par les utilisateurs sont systématiquement analysés par un antivirus (ClamAV) avant leur stockage et leur transmission.

1.3 Contrôle d'accès au traitement des données et aux données

Mesures de gestion du contrôle d'accès au traitement des données et aux données au niveau de l'infrastructure d'hébergement (OVH)

- Les autorisations d'accès sont accordées et suivies par les superviseurs selon la règle du moindre privilège et le principe de confiance progressive.
- Dans la mesure du possible, toutes les autorisations d'accès sont basées sur des rôles et non sur des droits individuels.
- La gestion des droits d'accès et des autorisations accordées à un utilisateur ou à un système s'effectue par le biais d'enregistrements, de modifications et de désenregistrements effectués par les superviseurs, le service informatique interne et les ressources humaines.
- Tout accès à distance au système d'information d'OVH s'effectue via un VPN. Cela nécessite un certificat connu uniquement de l'utilisateur et un secret partagé configuré sur le poste de travail.
- Les données sont chiffrées au repos et en transit
- Le fournisseur d'infrastructure cloud n'a pas d'accès logique aux serveurs.

Sécurité réseau OVH

OVH gère un réseau privé à fibre optique hautement performant, connecté à de nombreux opérateurs et transporteurs. OVH gère en interne sa propre dorsale. Elle distribue la connectivité aux réseaux locaux de chaque datacenter et les interconnecte.
Tous les équipements sont sécurisés par les mesures suivantes :

- Gestion de l'inventaire dans une base de données de gestion de configuration
- Mise en place d'un processus de renforcement de la sécurité, avec des instructions sur les paramètres à modifier pour garantir une configuration sécurisée
- L'accès aux fonctions d'administration des appareils est restreint via des listes de contrôle
- Tous les appareils sont gérés par un hôte bastion selon le principe du moindre privilège
- Des sauvegardes sont effectuées pour toutes les configurations des appareils réseau
- Les journaux sont collectés, centralisés et surveillés en permanence par l'équipe d'exploitation du réseau
- La mise en œuvre des configurations est automatisée et repose sur des modèles approuvés

Contrôle d'accès aux systèmes informatiques cloud d'OVH

OVHcloud applique une politique stricte pour gérer les droits d'accès logiques. Cette politique comprend les dispositions suivantes :

- Les droits d'accès sont accordés selon le principe du « privilège minimal ».
- Les droits d'accès doivent être basés sur des rôles plutôt que sur des droits spécifiques à des unités individuelles.
- L'octroi d'accès à un utilisateur ou à un système est géré selon des procédures de provisionnement initial, de modification et de suppression, avec la participation de leurs responsables, du support informatique / des services centraux et des RH.
- Tous les employés utilisent des comptes avec un identifiant utilisateur unique.
- Déconnexion automatique après une période d'inactivité.
- L'utilisation de comptes d'utilisateurs génériques et/ou anonymes est interdite.
- Une politique stricte en matière de mots de passe est appliquée.
- Les mots de passe doivent être générés de manière aléatoire.
- Les terminaux ont une longueur minimale de mot de passe de 10 caractères alphanumériques.
- Il est interdit de sauvegarder les mots de passe dans des fichiers non chiffrés, sur papier ou dans des navigateurs web.
- L'utilisation d'un logiciel de gestion des mots de passe local approuvé par le service de sécurité informatique est obligatoire.
- L'accès à distance aux systèmes informatiques cloud d'OVH doit se faire via un VPN. Un mot de passe connu de l'utilisateur et un certificat client configuré sur le poste de travail doivent être utilisés.

Mesures de gestion des accès aux ressources informatiques et de sécurité de l'ALE

Politique d'accès
Les accès sont contrôlés par l'utilisation de rôles et d'autorisations, sont enregistrés et les activités sont surveillées. Une description complète figure dans la directive de sécurité ALE (ALE_000835).
Principes du contrôle d'accès

Exigences métier en matière de contrôle d'accès :
Autorisations accordées selon le principe du « besoin d'en connaître » Chaque identifiant utilisateur ne peut accéder qu'aux données qui sont
a) non confidentielles (publiques)
b) nécessaires à l'accomplissement de tâches professionnelles individuelles
c) autorisées par un supérieur

Gestion des droits d'accès :
les responsables de niveau N+1 sont impliqués. Les identifiants sont bloqués s'ils ne sont pas utilisés.

Contrôle d'accès au système et aux applications :

- Contrôle des sessions :
  Il existe de nombreuses ressources informatiques auxquelles il est possible d'accéder (connexion réseau, poste de travail, appareil mobile, routeur) et chacune est soumise à des règles spécifiques de verrouillage après un certain nombre de tentatives infructueuses.
- Accès aux fonctions avancées :
  Celles-ci sont soumises au consentement des utilisateurs (ex. : enregistrement)
- Contrôle d'accès au réseau :
  Liste blanche pour l'accès filaire ; chiffrement pour l'accès sans fil.
- Accès aux services réseau externes :
  Tous les services réseau externes sont filtrés par les dispositifs de sécurité de l'entreprise, qui n'autorisent que les protocoles, les ports, les adresses IP source et destination, les applications et les délais d'expiration de session spécifiés. Liste blanche des services en place.
- Accès sortant des utilisateurs :
  Utilisation d'un proxy et surveillance du trafic. L'accès à distance nécessite une authentification forte.
- Ports de gestion et de diagnostic à distance :
  La gestion des ports (désactivation) permet de gérer cette sécurité.
- Segmentation du réseau :
  Les réseaux non gérés par le service informatique sont segmentés (même en l'absence de connectivité externe). Des routeurs ou des pare-feu sont utilisés pour n'autoriser que le trafic nécessaire, le cas échéant, à passer dans le réseau de l'entreprise.
- Ordinateurs à double connexion :
  Il est interdit de se connecter à un réseau externe à l'entreprise à l'aide des ressources de l'entreprise.
- Routage réseau :
  L'infrastructure de routage et de commutation du réseau ALE est surveillée afin de détecter les attaques par déni de service. L'accès externe aux informations réseau relatives au réseau interne de l'entreprise est restreint
- Le service de noms de domaine (DNS) est protégé contre les réseaux non fiables :
  Gestion des informations accessibles depuis l'extérieur, aucune redirection des requêtes DNS internes.

Mesures de gestion du contrôle d'accès au traitement des données et aux données chez Rainbow

Définition des rôles

Les utilisateurs Rainbow au sein d'une entreprise cliente finale peuvent avoir l'un des deux rôles suivants :

- Administrateur de l'entreprise
  - En plus des droits de l'utilisateur simple, il peut administrer son entreprise.

- En tant qu'utilisateur simple
  - L'accès aux fonctionnalités de Rainbow dépendra de son abonnement Rainbow.

Restriction de l'accès à la fonctionnalité de partage de fichiers
Afin de contrôler les échanges de fichiers entre les utilisateurs, il est possible de restreindre l'accès à la fonctionnalité « Partage de fichiers » (téléchargement et transfert). La configuration est effectuée par l'administrateur de l'entreprise pour l'ensemble de l'entreprise ou pour chaque utilisateur individuellement.
Restriction de la modification du nom d'utilisateur
Afin de se prémunir contre l'usurpation d'identité, il est possible d'interdire à l'utilisateur de modifier son titre, son prénom et son nom.

Cryptage et sécurité

Stockage crypté de la base de données des mots de passe
Les mots de passe des utilisateurs finaux sont hachés et salés dans la base de données interne de Rainbow.

Chiffrement en transit et au repos

- Toutes les données (messages instantanés, fichiers) échangées entre les utilisateurs ou via des bulles sont chiffrées en transit et au repos.
- Pour le transit, HTTPS + WSS via TLS 1.2/1.3 uniquement.
- Au repos, l'algorithme AES 256-GCM est utilisé.
- Les communications vocales/vidéo sont chiffrées en natif à l'aide de la technologie WebRTC utilisant DTLS et SRTP.

Analyse antivirus des fichiers

Tous les fichiers téléchargés par les utilisateurs sont systématiquement analysés par un antivirus (ClamAV) avant leur stockage et leur transmission.

1.4 Contrôles de séparation des clients

Capacité multi-clients
- Rainbow est entièrement compatible avec la gestion multi-clients
- Séparation logique des comptes clients

Fonctionnalités dédiées aux clients :
Offre Rainbow Edge : https://support.openrainbow.com/hc/fr/articles/360012465520

Séparation des systèmes de test et de production
- Environnement de test pour les nouvelles applications logicielles ou les mises à jour critiques.
- Le déploiement n'a lieu qu'après un test réussi.

1.5 Pseudonymisation

Pseudonymisation des journaux de requêtes

Toutes les requêtes adressées à l'application Rainbow sont enregistrées
Les journaux sont :

- entièrement anonymisés.
- envoyés vers un cluster de serveurs où ils sont stockés de manière redondante.
- conservés pendant la durée minimale imposée par la loi.

2. Intégrité

2.1 Contrôles des transferts

Communications chiffrées dans Rainbow

Toute connexion en clair depuis Internet est systématiquement refusée

Seule la connectivité HTTPS est utilisée (port 443)

- Les WebSockets sont alors sécurisés
- Aucun autre service n'est ouvert sur l'Internet public
- L'accès au port 80 est systématiquement redirigé vers le port 443

OpenSSL, utilisé pour le chiffrement, est toujours maintenu à jour.

SSLv2, SSLv3, TLS 1.0 et TLS 1.1 sont désactivés au profit de TLS 1.2 et TLS 1.3

- Nous n'offrons pas de prise en charge SSL obsolète et peu sécurisée.
- Toutes les négociations HTTPS s'effectuent exclusivement via TLS

Certificats SSL/TLS Wildcard standard de Gandi / Comodo CA

- Avec une clé ECDDSA de 256 bits (courbe elliptique) et signée avec RSA-SHA256.
- Aucun certificat auto-signé n'est utilisé.

2.2 Contrôles des entrées

Contrôles des entrées chez ALE

Il est possible de vérifier et de déterminer a posteriori si des données ont été saisies, modifiées ou supprimées dans les systèmes informatiques, et par qui :
- des profils d'utilisateurs
- l'identification des utilisateurs
- des concepts d'autorisation

Les fonctions de journalisation de tous les systèmes de production fonctionnent en permanence et sont conservées pendant une durée suffisante.

Contrôle des entrées dans Rainbow (analyse des journaux)

Résumé de la sécurité de Rainbow : https://support.openrainbow.com/hc/en-us/articles/115001019330

L'équipe opérationnelle ALE Rainbow est en mesure d'analyser avec précision les journaux d'activité stockés en cas de :

- attaque,
- d'activité suspecte,
- ou sur demande judiciaire.

Les clients finaux et les partenaires commerciaux n'ont pas accès aux journaux.
En cas de nécessité, l'équipe opérationnelle d'ALE peut extraire ponctuellement certaines informations à leur intention.

L'analyse des journaux permet de déterminer :

- L'adresse IP source,
- L'identité de l'utilisateur,
- La date et l'heure des requêtes,
- Le type des requêtes.

L'analyse des journaux ne permet en aucun cas de récupérer :

- Conversations / Discussions
- Mots de passe

3. Disponibilité et résilience

3.1 Contrôle de la disponibilité

Continuité opérationnelle (serveur)

La continuité opérationnelle des infrastructures (disponibilité des appareils, des applications et des processus d'exploitation) est assurée par diverses mesures :

- Refroidissement continu par liquide et par air
- Alimentation électrique continue et redondante
- Gestion de la capacité des équipements sous la responsabilité des fournisseurs de cloud
- Assistance technique du service
- Redondance des appareils et des serveurs utilisés pour l'administration du système
- De plus, d'autres mécanismes, tels que la sauvegarde des configurations des équipements réseau, garantissent la reprise du système en cas de défaillance

Prévention des risques naturels et environnementaux

- Installation de paratonnerres pour réduire les ondes électromagnétiques associées
- Implantation des locaux des fournisseurs de services cloud dans des zones non exposées aux risques d'inondation ou de tremblement de terre
- Une alimentation sans coupure (UPS) d'une capacité suffisante et des transformateurs auxiliaires avec commutation automatique de charge
- Commutation automatique vers des générateurs électriques d'une autonomie minimale de 24 heures
- Installation d'un système de refroidissement par liquide pour les serveurs (98 % des salles de serveurs ne sont pas climatisées)
- Utilisation d'unités de chauffage, de ventilation et de climatisation (CVC) qui maintiennent la température et l'humidité à un niveau constant
- Gestion d'un système d'alarme incendie (des exercices d'évacuation incendie sont organisés dans les centres de données tous les 6 mois)

Mesures techniques pour la disponibilité

Afin de garantir la haute disponibilité des données, différents mécanismes sont en place :

- Au niveau matériel avec des disques HA
- Les bases de données sont mises en cluster et répliquées
- Les fichiers des utilisateurs et les données statiques sont stockés en triple exemplaire sur des serveurs de stockage objet OpenStack Swift répliqués

Sauvegarde de toutes les bases de données

- Fréquence : instantanés horaires du système de fichiers de la base de données
- Sauvegarde quotidienne des bases de données sur deux sites distants et auprès de deux fournisseurs

Haute disponibilité

- HA sur les serveurs, les baies de stockage et les disques sous la responsabilité d'ALE
- Haute disponibilité électrique et réseau sous la responsabilité de l'hébergeur (OVH).

Surveillance

Une infrastructure de surveillance est en place pour tous les services OVH. Elle a plusieurs objectifs :

- Détection des incidents de production et de sécurité
- Surveiller les fonctions critiques et déclencher des alarmes vers le système de surveillance
- Notification des personnes responsables et lancement des procédures correspondantes
- Garantie de la continuité du service lors de l'exécution de tâches automatisées
- Vérification de l'intégrité des ressources surveillées

Plan de continuité des activités (ALE)

ALE a mis en place un plan de continuité des activités basé sur la norme ISO 27001 et précisé par les exigences de la norme ISO 27018 (extension de la norme ISO 27001).

3.2 Résilience/capacité de charge

Protection contre les attaques DDoS et pare-feu

Vous trouverez des informations détaillées ici : https://www.ovh.de/anti-ddos/.

Rainbow est protégé contre les attaques DDoS (déni de service distribué) grâce à la solution créée par OVH appelée VAC (vacuum).

- Entièrement configurée et gérée par OVH.

VAC est une combinaison de technologies développées par OVH pour :

- analyser rapidement les paquets de données en temps réel
- détourner le trafic entrant vers votre serveur
- séparer les requêtes non légitimes des autres et laisser passer le trafic légitime

Il s'agit d'une boîte noire dont les filtres ne sont pas divulgués pour des raisons de sécurité.

- Il s'agit d'un équipement matériel de filtrage de paquets basé sur la technologie ASIC.

Le traitement VAC se déroule en quatre étapes

1. pré-pare-feu
   Il est entièrement géré par OVH et applique des règles qui définissent des filtres dirigeant les paquets de données vers le réseau pare-feu

2. Réseau pare-feu
   Le réseau pare-feu est une solution qui limite l'exposition aux attaques provenant du réseau public. Il s'active automatiquement dès qu'une attaque DDoS commence.

3. Shield
   Le Shield intervient si une attaque utilise une technique d'amplification (DNS amp, NTP amp). Armor est le filtre le plus avancé de notre VAC et atténue les attaques les plus puissantes.

4. Armor
   Armor est le filtre le plus avancé du VAC et intervient pour atténuer les attaques les plus puissantes.

4. Procédures de réexamen, d'évaluation et d'analyse réguliers (art. 32, al. 1, let. d RGPD ; art. 25, al. 1 RGPD)

A. Protection des données - Gestion

Les politiques, procédures ou directives suivantes concernant la sécurité des données sont documentées dans le système SMSI d'ALE :

- Obligation de confidentialité pour tous les employés (confidentialité des données)
- Mesures de sensibilisation des employés.
- Charte de sécurité d'ALE
- Directives de sécurité ALE
- Politique de sécurité d'ALE
- Politique de protection des données et de confidentialité d'ALE
- Politique ALE relative au RGPD
- Directives relatives à la gestion de crise : politique et procédure
- Directives relatives aux informations confidentielles
- Système de gestion de l'information
- Audits réalisés par le délégué à la protection des données
- Audits par des auditeurs externes
- Activités de traitement documentées.
- Révision régulière des mesures techniques et organisationnelles.
- Sélection rigoureuse des prestataires de services (voir également la rubrique « Gestion des contrats »).
- Certification ISO 27001, y compris ISO 27017 et ISO 27018

B. Délégué à la protection des données

Louis-Philippe Ollier

E-mail : dataprivacy@al-enterprise.com
Téléphone : +331 5566 3147
Les coordonnées du DPD sont également disponibles sur https://www.al-enterprise.com/en/legal/privacy

C. Gestion des incidents

OVH
Un processus de gestion des incidents est en place. Il permet la prévention, la détection et la résolution de ces événements au sein des infrastructures de gestion des services et du service lui-même. Ce processus comprend :

- Un guide de classification des événements de sécurité
- La gestion des événements de sécurité
- Des exercices de simulation pour l'équipe de crise
- Des tests du plan d'intervention en cas de perturbations
- La communication avec les clients dans le cadre d'une équipe de gestion de crise

Ces procédures font l'objet d'un processus d'amélioration continue pour le suivi et l'évaluation des incidents, la gestion globale des incidents et les mesures correctives associées.
ALE
Directives de gestion de crise
Processus établis et documentés pour la gestion des incidents

- Responsabilités définies
- Canaux de signalement définis
- Procédure en cas de violation de données

D. Protection de la vie privée dès la conception

Par principe, dans le service Rainbow, seules les données appropriées et nécessaires à des fins commerciales sont collectées et traitées. Les procédures de collecte et de traitement automatisés des données sont conçues de manière à ce que seules les données nécessaires soient collectées.
Il n'y a pas de gestion des données comportementales dans Rainbow. Aucune donnée collectée pour, générée dans ou résultant des activités de Rainbow ou de l'analyse de ces activités n'est communiquée ni vendue à des tiers.
Rainbow peut être utilisé avec un minimum d'informations, à savoir une adresse e-mail et un mot de passe.

E. Gestion des contrats

Si des sous-traitants sont utilisés pour le traitement des données, certaines exigences s'appliquent. Il s'agit notamment de s'assurer que les mesures techniques et organisationnelles des sous-traitants sont conformes à l'article 28 du RGPD, en liaison avec l'article 32, paragraphe 1, du RGPD.
Les exigences suivantes s'appliquent à une relation de sous-traitance :

- Informations détaillées sur la finalité, la nature et l'étendue du traitement et de l'utilisation des données à caractère personnel du client, conformément à l'article 28, paragraphe 3, du RGPD. Les détails correspondants sont fixés par contrat.
- Les prestataires de services allemands / de l'UE ont désigné un délégué à la protection des données au sein de l'entreprise si la loi l'exige et veillent, par le biais de l'organisation de protection des données, à ce qu'il soit intégré de manière appropriée et efficace dans les processus opérationnels concernés.
- Les commandes verbales doivent être confirmées et documentées par écrit.
- Les contrats individuels ne sont attribués que par l'intermédiaire de contacts désignés.
- Seules des autorisations d'accès restrictives sont accordées pour les environnements techniques concernés. En cas d'accès externe au système, l'accès sera désactivé ou bloqué après la fin de la coopération.
- Pour la transmission de données à caractère personnel à des prestataires de services externes, un modèle de contrat de sous-traitance est disponible, qui contient des dispositions de contrôle appropriées.
- ALE a conclu des accords de protection des données avec toutes ses parties liées, le cas échéant, conformément aux dispositions de l'article 28 du RGPD.

ANNEXE 2 – FICHE POINT DE CONTACTS SERVICE RAINBOW HDS – CLIENT

Le Client transmet au Revendeur Agréé ses points de contact et s'assure de la connaissance des interlocuteurs par le Revendeur Agréé (au cas où ALE ne soit pas le revendeur du Service). Le Revendeur Agréé s'engage à renseigner les points de contact du Client et les siens sur le portail Rainbow. Le Client et le Revendeur Agréé s'assurent de la régulière mise à jour de ces points de contact, cette fiche devant être transmise à ALE via son Revendeur Agréé pour s'assurer :

- De désigner à ALE un professionnel de santé lorsque cela est nécessaire (exemple : Accès aux Données de santé, gestion des relations avec le patient).
- Du traitement des incidents ayant un impact sur les Données de santé hébergées dans le cadre du Service Rainbow.

Organisme
Entité Client du Service Rainbow HDS :
Raison Sociale :
Adresse :

Contact principal
Prénom Nom :
Fonction :
Mail :
Téléphone :

Contact secondaire (si indisponibilité du contact principal)
Prénom Nom :
Fonction :
Mail :
Téléphone :
Délégué à la Protection des Données (ou personne en charge de la conformité du traitement des données personnelles) à contacter pour le traitement des incidents ayant un impact sur les Données de santé hébergées dans le cadre des Services.
Prénom Nom :
Fonction :
Mail :
Téléphone :

ANNEXE 3 – Liste des Sous-traitants

1. Hébergeur :

- **OVH Healthcare en France, hébergeur certifié HDS.**
  - Adresse : OVH, siège social 2 RUE KELLERMANN 59100 ROUBAIX, France
  - Data center OVH Strasbourg (SBG3)
    9, rue du bassin de l'industrie
    67 000 Strasbourg
  - Data Center OVH Roubaix (RBX2a et RBX8)
    2, rue Kellermann
    59 100 Roubaix

2 Back up :

- **IBM , hébergeur certifié HDS**

- Data center IBM (PAR1)
  9, rue du Petit Clichy
  92110 CLICHY

3 La gestion du routage des tickets d'incidents s'appuie sur le support technique de la Société SalesForce

Adresse : salesforce.com EMEA Limited, Floor 26 Salesforce Tower, 110 Bishopsgate London EC2N 4AY, UK

3. Le service de maintenance corrective s'appuie sur le support technique :

1. de la Société X-ACT.
   Adresse : X-act Luis Morote 6, 6e Planta, 35007 Las Palmas de Gran Canaria, Spain

ALE USA Inc. | 26801 West Agoura Rd. | Calabasas, CA 91301, USA
T: +1 818 880 3500 | F: +1 818 880 3505

www.al-enterprise.com

ANNEXE 4 – CERTIFICATION HDS ALE INTERNATIONAL, OVH et IBM

ALE USA Inc. | 26801 West Agoura Rd. | Calabasas, CA 91301, USA
T: +1 818 880 3500 | F: +1 818 880 3505

Certificat

Certificate

N° 2019/84634.5 **Page 1 / 2**

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

ALE INTERNATIONAL
exerçant sous la marque / operating under the brand
ALCATEL-LUCENT ENTERPRISE

pour les activités suivantes :
for the following activities:

RAINBOW SERVICE HDS
HÉBERGEUR INFOGÉREUR :

4. LA MISE A DISPOSITION ET LE MAINTIEN EN CONDITION OPÉRATIONNELLE DE L'INFRASTRUCTURE VIRTUELLE DU SYSTÈME D'INFORMATION UTILISE POUR LE TRAITEMENT DES DONNÉES DE SANTE

5. L'ADMINISTRATION ET L'EXPLOITATION DU SYSTÈME D'INFORMATION CONTENANT LES DONNÉES DE SANTE

6. LA SAUVEGARDE DE DONNÉES DE SANTE

DECLARATION D'APPLICABILITE _v3.2 DU 09/01/2024
ALE INTERNATIONAL est certifié selon: NF EN ISO/IEC 27001:2023 / ISO/IEC 27001:2022

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of:

REFERENTIEL DE CERTIFICATION HDS 1.1 - Mai 2018

et est déployé sur les sites suivants :
and is developed on the following locations:

260 rue Léon Foucault FR-67400 Illkirch-Graffenstaden

2000 CORPORATE CENTER DRIVE THOUSAND OAKS - 91320 OAKS USA

32 AVENUE KLEBER -92700 COLOMBES

115-225 RUE A DE ST EXUPERY ZAC Prat Pip FR-29806 BREST CEDEX 9

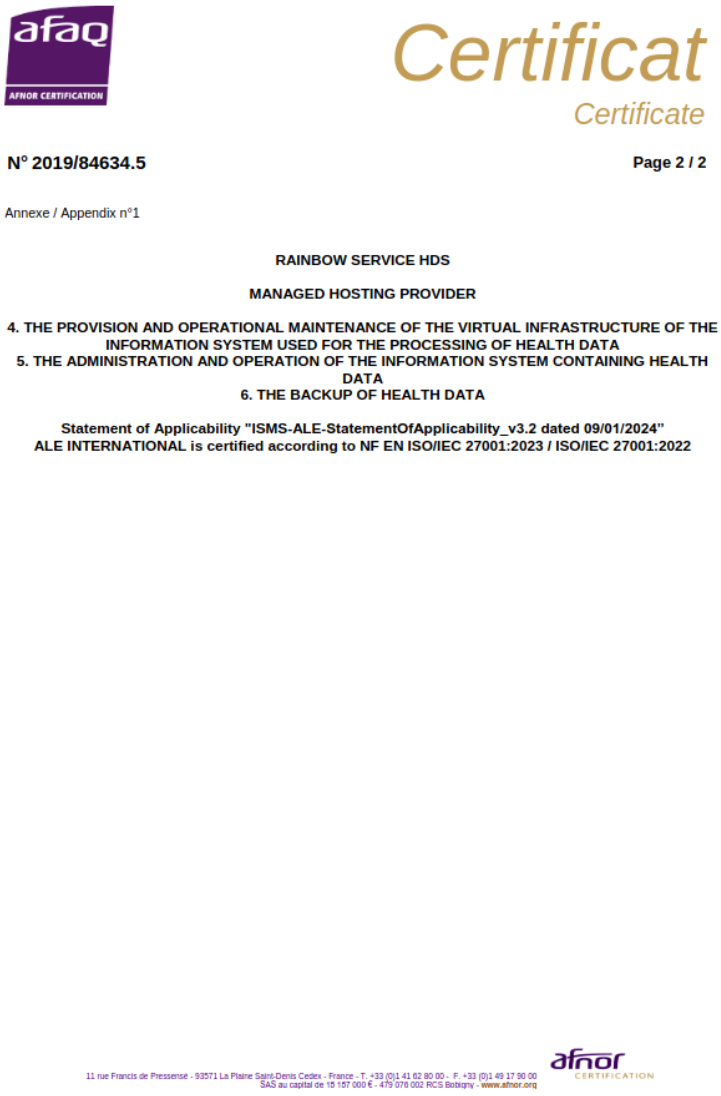
Ce certificat est valable à compter du (année/mois/jour) *This certificate is valid from (year/month/day)* **2024-05-14** Jusqu'au *Until* **2027-05-13**

Julien NIZRI
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Flashez ce QR Code pour vérifier la validité du certificat

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex - France - T. +33 (0)1 41 62 80 00 - F. +33 (0)1 49 17 90 00

ALE USA Inc. | 26801 West Agoura Rd. | Calabasas, CA 91301, USA
T: +1 818 880 3500 | F: +1 818 880 3505



Certificat

Certificate

N° 2019/84634.5

Page 2 / 2

Annexe / Appendix n°1

RAINBOW SERVICE HDS

MANAGED HOSTING PROVIDER

4. THE PROVISION AND OPERATIONAL MAINTENANCE OF THE VIRTUAL INFRASTRUCTURE OF THE INFORMATION SYSTEM USED FOR THE PROCESSING OF HEALTH DATA
5. THE ADMINISTRATION AND OPERATION OF THE INFORMATION SYSTEM CONTAINING HEALTH DATA
6. THE BACKUP OF HEALTH DATA

Statement of Applicability "ISMS-ALE-StatementOfApplicability_v3.2 dated 09/01/2024"
ALE INTERNATIONAL is certified according to NF EN ISO/IEC 27001:2023 / ISO/IEC 27001:2022

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex - France - T. +33 (0)1 41 62 80 00 - F. +33 (0)1 49 17 90 00
SAS au capital de 15 157 000 € - 479 076 002 RCS Bobigny - www.afnor.org

Certificat OVH HDS v2

ALE USA Inc. | 26801 West Agoura Rd. | Calabasas, CA 91301, USA
T: +1 818 880 3500 | F: +1 818 880 3505

BYCYB

Certificat
Certificate

Numéro de certificat
Certificate number

37387-7

OVH GROUPE

2 RUE KELLERMANN 59100 - ROUBAIX - FRANCE

met en œuvre et entretient un système de management conforme au référentiel de certification,
operates a management system which complies with the requirements of,

Hébergeur de Données de Santé version 2.0

Pour les activités suivantes / for the following activities
Offres OVH Healthcare,

OVH Healthcare Services,

Hébergeurs de données de santé	Health Data Host
1. La mise à disposition et le maintien en condition opérationnelle de sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé	1. The provision and maintenance in operational condition of physical sites for hosting the hardware infrastructure of the information system used to process the health data
2. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé	2. The provision and maintenance in operational condition of the hardware infrastructure of the information system used to process the health data
3. La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé	3. The provision and maintenance in operational condition of the virtual infrastructure of the information system used to process the health data
4. La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information	4. The provision and maintenance in operational condition of the platform for hosting information system applications
5. L'administration et l'exploitation du système d'information contenant les données de santé	5. The management and operation of the information system containing the health data
6. La sauvegarde des données de santé	6. Backing up of health data

Déclaration d'applicabilité / Statement of applicability
OVHCloud Statement of applicability.xlsx - V9 du 10/10/2025

Ce certificat est valide sous réserve de la validité à isopérimètre du certificat ISO/IEC 27001 ou NF ISO/IEC 27001 référencé :
This certificate is valid subject to the validity at the isoperimeter of the ISO/CEI 27001 or NF ISO/CEI 27001 referenced certificate:
LNE-37383

Site(s) concerné(s) / Concerned location(s)
voir annexe / see annex

Date début de validité 12 mars 2026
Effective date March 12th, 2026
Valable jusqu'au 03 février 2027
Expiry date February 3rd, 2027
Annule et remplace / Cancels and replaces le certificat 37387-6

Antoine SIMON
Signature numérique de Antoine SIMON
Date : 2026.03.11 09:49:13 +01'00'
Responsable Département Certification
Head of Certification Department

cofrac
CERTIFICATION DE SYSTÈMES DE MANAGEMENT
Accréditation n°4-0508
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

BYCYB
build your cyber

Annexe au certificat n° 37387 rév. 7
Certificate Annex n° 37387 rev. 7

Hébergeur de Données de Santé version 2.0
Health Data Host version 2.0

Activités couvertes par la certification / Activities covered by certification :

Les produits intégrer dans le domaine d'application du système de management conforme au référentiel de certification HDS sont spécifiées sur la page suivante :

https://help.ovhcloud.com/csm/fr-hds-certification?id=kb_article_view&sysparm_article=KB0061195

The products included in the scope of the management system compliant with the HDS certification standard are specified on the following page:

https://help.ovhcloud.com/csm/fr-hds-certification?id=kb_article_view&sysparm_article=KB0061195

Nom du site	Pays	Adresse	Type de site
Bordeaux	FR	Batiment G4 - 56 quai Lawton 33300 BORDEAUX	Bureau (Activités 3, 4, 5 et 6)
Brest	FR	50 avenue Gaston Esnault HALL A 2ème étage 29200 BREST	Bureau (Activités 3, 4, 5 et 6)
Limburg	DE	Limburger Straße 45, 65555 Limburg-Offheim Germany	OVH DC (Activités 1 et 2)
Croix	FR	155 avenue Georges Hannart 59170 CROIX	Bureau (Activités 3, 4, 5 et 6)
Paris / Clichy	FR	7-9 Rue Petit 92582, Clichy	Datacenter colocation (Globalswitch) (Activités 1 et 2)
Eybens	FR	5 Rue Raymond Chanas, 38320 Eybens	Datacenter (DC tape) Shell & Core (DXC) (Activités 1 et 2)
Frankfurt	DE	REGUS / SPACES : Friedrich Ebert Anlage 49 – 23 floor 60308 FRANKFURT DEUTCHSLAND	Bureau (Activités 3, 4, 5 et 6)
Gravelines	FR	ZI des Huttes - Route de la ferme Masson 59820 GRAVELINES	OVH DC (Activités 1 et 2)
Groupe Datacenters Roubaix	FR	RBX1/2/4 : 2 rue Kellermann 59100 ROUBAIX RBX3/5/6/8/10 : Quai du Sartel 59100 ROUBAIX RBX7 : Boulevard Beaurepaire 59100 ROUBAIX	OVH DC (Activités 1 et 2)
HDF (Avelin)	FR	11 rue des Marlières 59710 AVELIN	OVH DC

ALE USA Inc. | 26801 West Agoura Rd. | Calabasas, CA 91301, USA
T: +1 818 880 3500 | F: +1 818 880 3505

www.al-enterprise.com

			(Activités 1 et 2)
Paris / Ferrières-en-Brie	FR	16 Av. Joseph Froelicher, 77600 Ferrières-en-Brie	Datacenter colocation (Interxion/DLR) (Activités 1 et 2)
Köln	DE	OVH Gmbh – Oskar Jäger StraBe 173/K6 - 50825 Köl	Bureau (Activités 3, 4, 5 et 6)
Paris / Marcoussis	FR	15 rue Marin Angiboust, 91460 Marcoussis	Datacenter colocation (Data4) (Activités 1 et 2)
Lisboa	PT	Avenida 5 de Outubro n°146-6° andar 1050-061 LISBOA	Bureau (Activités 3, 4, 5 et 6)
Lyon	FR	90 avenue Félix FAURE 69003 LYON	Bureau (Activités 3, 4, 5 et 6)
Madrid	ES	Calle de Luchana 23, planta 1, 23810 MADRID	Bureau (Activités 3, 4, 5 et 6)
Saint-Pierre-des-Corps	FR	213 Av. Stalingrad, 37700 Saint-Pierre-des-corps	Datacenter (DC tape) Shell & Core (Terralpha) (Activités 1 et 2)
Milan	IT	Via Carlo Imbonati, 18- MAC7, 20159 MILANO	Bureau (Activités 3, 4, 5 et 6)
Strasbourg	FR	9 rue du Bassin de l'Industrie 67000 STRASBOURG	OVH DC (Activités 1 et 2)
Villenave d'Ornon	FR	84 Av. Mirieu de Labarre, 33140 Villenave-D'Ornon	Datacenter (DC tape) Shell & Core (EXA / GTT) (Activités 1 et 2)
Nantes	FR	7 mail Pablo Picasso - 1er étage 44000 NANTES	Bureau (Activités 3, 4, 5 et 6)
Paris17	FR	42 avenue de la Porte de Clichy 75017 PARIS	Bureau (Activités 3, 4, 5 et 6)
Rennes	FR	3bis avenue de Belle Fontaine - 4ème étage 35510 CESSON SEVIGNE	Bureau (Activités 3, 4, 5 et 6)
Roubaix	FR	2 rue Kellermann 59100 ROUBAIX	Bureau et siège social (Activités 3, 4, 5 et 6)
Saarbrucken	DE	HOUSE OF INTELLIGENCE, Am Schanzenberg, 66117 Saarbrücken 5ème étage	Bureau (Activités 3, 4, 5 et 6)

ALE USA Inc. | 26801 West Agoura Rd. | Calabasas, CA 91301, USA
T: +1 818 880 3500 | F: +1 818 880 3505

BUREAU VERITAS

Bureau Veritas Certification

IBM CLOUD INFRASTRUCTURE AS A SERVICE (IAAS)

This is a multi-site certificate, additional site details are listed in the appendix to this certificate

14001 DALLAS PARKWAY
75240 SUITE M100 DALLAS
USA

Bureau Veritas Certification France certify that the Management System of the above organization has been audited and found to be in accordance with the requirements of the management system standard detailed below:

HDS CERTIFICATION REFERENTIAL V2

Scope of certification

PROVISION AND MAINTENANCE IN OPERATIONAL CONDITION OF PHYSICAL SITES FOR HOSTING THE HARDWARE INFRASTRUCTURE OF THE INFORMATION SYSTEM USED TO PROCESS THE HEALTH DATA.
PROVISION AND MAINTENANCE IN OPERATIONAL CONDITION OF THE HARDWARE INFRASTRUCTURE OF THE INFORMATION SYSTEM USED TO PROCESS THE HEALTH DATA.
PROVISION AND MAINTENANCE IN OPERATIONAL CONDITION OF THE PLATFORM FOR HOSTING INFORMATION SYSTEM APPLICATIONS.
PROVISION AND MAINTENANCE IN OPERATIONAL CONDITION OF THE VIRTUAL INFRASTRUCTURE OF THE INFORMATION SYSTEM USED TO PROCESS THE HEALTH DATA.
MANAGEMENT AND OPERATION OF THE INFORMATION SYSTEM CONTAINING THE HEALTH DATA.

THE ABOVE ORGANIZATION IS ALSO CERTIFIED ACCORDING TO THE STANDARDS
ISO 27001 V2022
STATEMENT OF APPLICABILITY :
This certificate is valid subject to obtaining a valid ISO 27001 certification for the same scope.

Certification/Recertification Cycle Start Date: **23 September 2025**

Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on: **12 August 2028**

Expiry date of previous cycle: **12 August 2025**

Certification/Recertification Audit date: **03 July 2025**

Original Cycle Start Date: **13 August 2019**

Certificate n°: **FR098610-1**

File n°: **28518230**

Revision date: **23 September 2025**

Samuel DUPRIEU - President

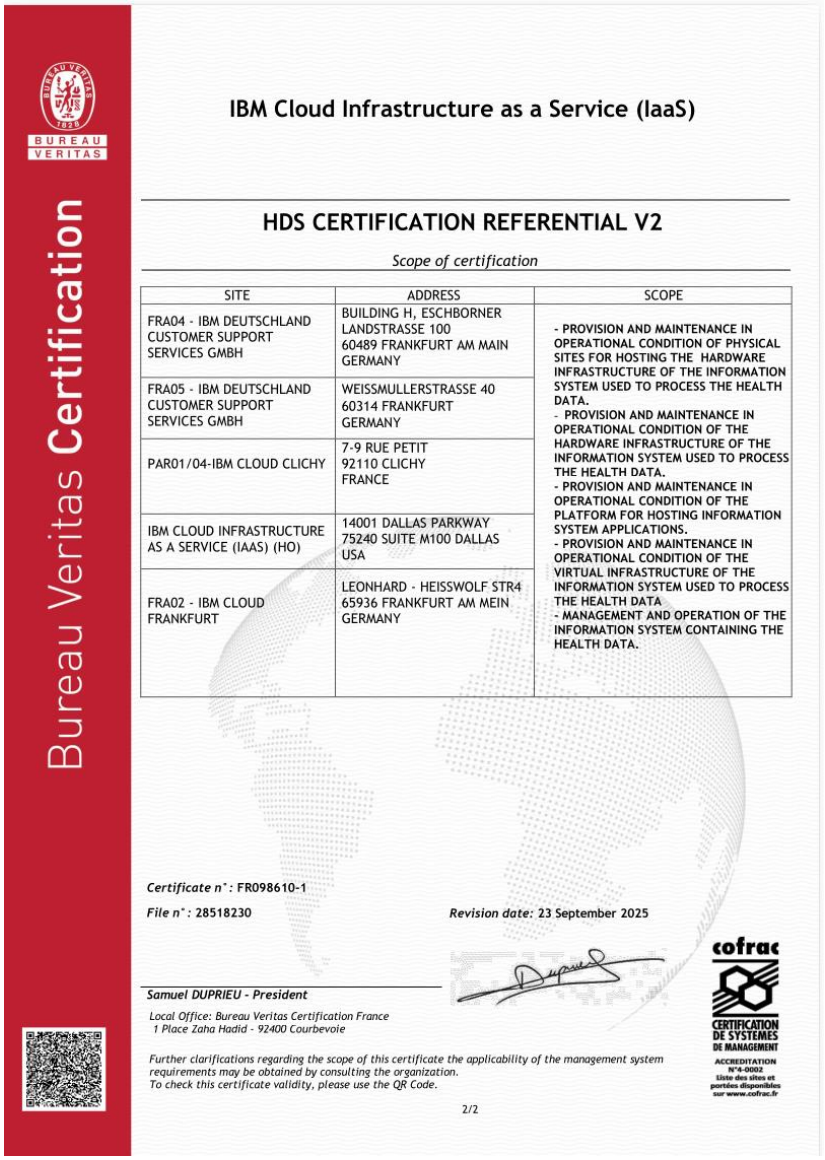
Local Office: Bureau Veritas Certification France
1 Place Zaha Hadid - 92400 Courbevoie

Further clarifications regarding the scope of this certificate the applicability of the management system requirements may be obtained by consulting the organization.
To check this certificate validity, please use the QR Code.

cofrac
CERTIFICATION DE SYSTEMES DE MANAGEMENT
ACCREDITATION N°4-0002
Liste des sites et portées disponibles sur www.cofrac.fr

1/2

ALE USA Inc. | 26801 West Agoura Rd. | Calabasas, CA 91301, USA
T: +1 818 880 3500 | F: +1 818 880 3505



Bureau Veritas Certification

IBM Cloud Infrastructure as a Service (IaaS)

HDS CERTIFICATION REFERENTIAL V2

Scope of certification

SITE	ADDRESS	SCOPE
FRA04 - IBM DEUTSCHLAND CUSTOMER SUPPORT SERVICES GMBH	BUILDING H, ESCHBORNER LANDSTRASSE 100 60489 FRANKFURT AM MAIN GERMANY	- PROVISION AND MAINTENANCE IN OPERATIONAL CONDITION OF PHYSICAL SITES FOR HOSTING THE HARDWARE INFRASTRUCTURE OF THE INFORMATION SYSTEM USED TO PROCESS THE HEALTH DATA. - PROVISION AND MAINTENANCE IN OPERATIONAL CONDITION OF THE HARDWARE INFRASTRUCTURE OF THE INFORMATION SYSTEM USED TO PROCESS THE HEALTH DATA. - PROVISION AND MAINTENANCE IN OPERATIONAL CONDITION OF THE PLATFORM FOR HOSTING INFORMATION SYSTEM APPLICATIONS. - PROVISION AND MAINTENANCE IN OPERATIONAL CONDITION OF THE VIRTUAL INFRASTRUCTURE OF THE INFORMATION SYSTEM USED TO PROCESS THE HEALTH DATA - MANAGEMENT AND OPERATION OF THE INFORMATION SYSTEM CONTAINING THE HEALTH DATA.
FRA05 - IBM DEUTSCHLAND CUSTOMER SUPPORT SERVICES GMBH	WEISSMULLERSTRASSE 40 60314 FRANKFURT GERMANY	
PAR01/04-IBM CLOUD CLICHY	7-9 RUE PETIT 92110 CLICHY FRANCE	
IBM CLOUD INFRASTRUCTURE AS A SERVICE (IAAS) (HO)	14001 DALLAS PARKWAY 75240 SUITE M100 DALLAS USA	
FRA02 - IBM CLOUD FRANKFURT	LEONHARD - HEISSWOLF STR4 65936 FRANKFURT AM MEIN GERMANY	

Certificate n°: FR098610-1

File n°: 28518230

Revision date: 23 September 2025

Samuel DUPRIEU - President

Local Office: Bureau Veritas Certification France
1 Place Zaha Hadid - 92400 Courbevoie

Further clarifications regarding the scope of this certificate the applicability of the management system requirements may be obtained by consulting the organization.
To check this certificate validity, please use the QR Code.

2/2

cofrac
CERTIFICATION DE SYSTEMES DE MANAGEMENT
ACCREDITATION N°4-0002
Liste des sites et portées disponibles sur www.cofrac.fr

ALE USA Inc. | 26801 West Agoura Rd. | Calabasas, CA 91301, USA
T: +1 818 880 3500 | F: +1 818 880 3505

www.al-enterprise.com