Version dated March 11th, 2026

RAINBOW HDS PAID SERVICE IN UCaaS MODE – Health Data Hosting Special Terms of Use

These Special Terms of Use (the "Terms of Use") govern the use of the paid Rainbow HDS service (the "Rainbow HDS Service" or "Service") that you have purchased directly from ALE International or an Authorized Reseller (hereinafter the "Service Provider").

The Rainbow Service is a communication solution provided by ALE International ("ALE"), a French company headquartered at 32 avenue Kléber, 92700 Colombes, France, registered with the Nanterre Chamber of Commerce under number 602 033 185 RCS Nanterre (for more information, please click on the following link https://www.al-enterprise.com). The Rainbow HDS Service is described in more detail in Section 3.

All capitalized terms used but not defined in these Special Terms and Conditions shall have the meanings assigned to them in Appendix 1, General Terms of Use.

ARTICLE 1: PURPOSE

These Special Terms and Conditions, which supplement the General Terms and Conditions of Use for the Service, are intended to define the technical conditions under which the Provider undertakes to provide the Service to the Customer.

These Special Terms and Conditions shall prevail over the General Terms and Conditions of Use for the Rainbow Paid Service in the event of any conflict between these two documents.

ARTICLE 2: DEFINITIONS

In addition to the terms defined in the Glossary, the following terms, whether in the singular or plural, shall have the following meanings between the Parties:

HDS Certification: certification required for the processing and hosting of personal health data on digital media, as defined by Articles L 1111-14 through L 1111-24 of the Public Health Code and its implementing decree No. 2018-137 of February 26, 2018.

Special Terms: these terms and conditions.

Client: A natural or legal person who subscribes to the "Rainbow HDS Service" offering. It is the Client's responsibility to ensure compliance with the obligation to obtain HDS certification if required for their own business activities. In the context of health data hosting, the Customer is a healthcare professional or facility that submits Health Data through the Service. It is the Customer's responsibility to ensure compliance with their obligations under the PGSSI-S.

Agreement: The combination of these Special Terms and Conditions and the General Terms of Service.

Data: All data entered, transmitted, and/or processed by the Customer, its own Users, and Data Subjects when using the Service. This data may include Health Data.

Personal Health Data (or Health Data): Any data relating to the physical or mental health of a natural person who is identified or can be identified, directly or indirectly, collected or generated in the course of prevention, diagnosis, or treatment activities, as well as the provision of healthcare services, which reveals information about that person's state of health.

Health Data Host – IT Service Provider (or Host): a natural or legal person holding a certification and therefore authorized to host Health Data.

Data Subjects: natural persons to whom the Personal Data relates.

Service: communication solution, subject to the Special Terms and Conditions, through which ALE or the Service Reseller enables the Customer to communicate, share, and store Data with Users and Data Subjects.

UCaaS: Unified Communications as a Service.
Users: end users of the Service made available to them by You as a Service Customer or your own users, within the scope of the Rainbow HDS Service. These include the Customer's staff members and individuals authorized by the Customer to access the Service.

ARTICLE 3: RAINBOW HDS SERVICE

As part of the provision of the Service, ALE or an Authorized Reseller (in the context of a subscription through an Authorized Reseller) provides you with a communication service for the exchange of Data in compliance with HDS regulations.

ALE acts in connection with the Service as a Health Data Host and Manager within the meaning of Articles L1111-8 and R1111-9 of the Public Health Code and, as part of the Service, performs the following activities mentioned in points 1, 2, 3, 4, 5, and 6 of the aforementioned Article R 1111-9:

1- provision and maintenance of the physical sites used to host the hardware infrastructure of the information system used for the processing of Health Data;

2- providing and maintaining in operational condition the hardware infrastructure of the information system used for the processing of health data;

3- providing and maintaining in operational condition the application hosting platform of the information system;

4- Provision and maintenance of the virtual infrastructure of the information system used for processing Health Data;

5- administration and operation of the information system containing the Data;

6- Backing up the Data.

It is understood that activities 1, 2, 3, and partially activity 4 are subcontracted to OVH as a certified health data host (HDS LNE-35608-0)

Regarding Activity 6, Data Backup:

- The HDS Rainbow Service is not an archiving service approved by the Ministry of Culture. The Service does not include archiving and retention services for Health Data, as required under the PGSSI-S (retention of archives on Data of Data Subjects/patients).
- However, ALE provides the necessary tools and interfaces so that the Customer can perform or have these archiving services performed by a third party of their choice.
- In this regard, ALE provides a monthly, quarterly, or annual extract of the items exchanged during use of the service (messages, files) as well as the User's account identification data (last name, first name, and user profiles), either to a certified archiver (for an additional fee) or to the Customer if you perform the archiving yourself.

  ALE makes the HDS and ISO 27001 certification documents available on its website. Any changes related to the HDS activities carried out by ALE, or by extension any changes related to the associated standards (ISO 27001), will be notified to the Client within 10 business days

The Service is intended for healthcare facilities and professionals in accordance with applicable laws and regulations.

Personal Data is used solely for the purpose of the Service (communication, data sharing, and data storage). The processing of Data carried out by ALE is intended exclusively to enable the provision of the communication Service that you, as a Client, use with your Users and/or Data Subjects within the healthcare sector, and to enable the sharing and storage of Data.

The Service allows your Users to submit, share, send, and display content to and with other Users. As such, you acknowledge and agree (on behalf of yourself and your Users) that this content may only be viewed by participants in the conversation.

In connection with the use of this Service, you confirm, as a Customer, that you possess full knowledge of the Regulations and PGSSI-S guidelines to use the Service yourself and solely through personnel authorized to administer Health Data.

As a Customer and as a data controller, you are responsible for complying with the applicable PGSSI-S regulations when using this Service.

3.1: MANAGEMENT OF HEALTH DATA

The Data you store on the Service may include personal data as well as Health Data. As a Customer and data controller, you are responsible for overseeing the processing of this data. The Parties agree to process Health Data in accordance with applicable legal and regulatory provisions, particularly regarding the protection of personal data and the hosting of health data. ALE, and any person involved in the Service, shall act only on the Client's instructions.

As a data processor, ALE undertakes not to access the data processed by ALE on behalf of the Client except (i) in cases provided for by law, (ii) or in cases of corrective maintenance, all of which will be logged and associated with a support ticket.

ALE ensures that its staff is made aware of compliance with the legal and regulatory requirements applicable to the security of Health Data, in particular regarding their confidentiality and the observance of professional secrecy. To this end, ALE provides its employees involved in the Service with a specific clause in their employment contract regarding the confidentiality of the Data.

ALE certifies, through its hosting provider OVH, that the Service Data is located exclusively in France and therefore within the European Economic Area (EEA). This includes production, backup, log, and metadata environments.

ALE specifies that, within the scope of the Service, there is no transfer of personal health Data to a country outside the European Economic Area;

Within the scope of the Service, the Customer is responsible for ensuring that the processed Data complies with applicable legal and regulatory requirements, particularly regarding the protection of personal data and the hosting of health data. As such, and in its capacity as the data controller, the Client is specifically responsible for the accuracy of the Data and its updating, for determining a retention period, for deleting the Data, for providing prior notice to the data subjects, for obtaining the necessary consents from the data subjects in accordance with applicable regulations, for managing end-users' access to the Health Data, and for the security of such Data. The Parties undertake to cooperate with the competent personal data or health data protection authorities.

No access to personal health data ("DSCP") from a country outside the EEA is permitted: Any access to data by the Client outside the European Economic Area (EEA) is the sole responsibility of the Client. In this regard, ALE recommends that the Client, in its capacity as data controller, implement an appropriate security policy.

If either Party receives a request from an administrative or judicial authority, ALE shall be required to transmit said Data to the competent authorities. ALE shall notify the Client of any request from the authorities, unless prohibited by a court order.

3.2: RIGHTS OF DATA SUBJECTS

3.2.1: INFORMATION AND CONSENT

As a Customer, you must ensure that Data Subjects are informed in advance regarding the use of the Service, in accordance with applicable laws and regulations. This information must include the mandatory disclosures regarding the protection of personal data, as well as disclosures regarding the hosting of health data and the procedures for accessing and transmitting such data. Providing prior information to Data Subjects regarding the hosting of Health Data is in no way the responsibility of ALE. Where applicable, it is the Client's responsibility to ensure that prior information is provided to the Data Subjects. The Client must communicate the terms of use of the Service to its own Users.

3.2.2: EXERCISE OF DATA SUBJECTS' RIGHTS

In accordance with applicable laws and regulations, particularly regarding the management of rights over personal data and the hosting of Health Data, any User of the Service or Data Subject has rights over their Data provided that such rights are not restricted by other prevailing legal provisions (for example, a Data Subject's request to delete their Health Data may not be granted because the Public Health Code stipulates a regulated retention period for such data (for example, for 20 years from the date of the patient's last stay or last consultation, reduced to 10 years from the date of the patient's death in public or private facilities; 10 years from the stabilization of the Patient's health for private practitioners).

These include the right to transparency regarding the purposes of data processing, the rights of access, rectification, or deletion of data, the right to object to all or part of the purposes of data processing, the right to be notified of events occurring to or affecting the data, the right to restrict processing, and the right to data portability.

The Service User acting as the data controller remains solely responsible for processing these requests in accordance with applicable regulations, in particular Articles L1110-4 and L1111-7 of the Public Health Code and Chapter III of Regulation 2016/679 of the European Parliament and of the Council dated April 27, 2016.

To this end, it is the Client's responsibility to process or arrange for the processing of requests to exercise rights submitted to it by Data Subjects, in accordance with applicable legal and regulatory provisions. Upon receipt of a Request to Exercise Rights from a Data Subject, the Client undertakes to i) authenticate the requester, ii) validate the admissibility of the request and, in particular, verify that the request does not conflict with other prevailing legal provisions, iii) respond to the request to the extent of its capabilities and the means made available to it by ALE within the scope of the Service (Service administration tools).

ALE forwards to the Client all requests from Data Subjects who wish to exercise their rights.

ALE provides the Data Controller with assistance and cooperation in processing such requests as follows.

If the Customer demonstrates that it has been unable to respond to the Data Subject's request given its resources, then it may forward the request to its Authorized Reseller (in the event that ALE is not the Provider) or to ALE after the Authorized Reseller has forwarded the Customer's request to ALE (if ALE is not the Provider), or upon receipt of the Customer's request by ALE, ALE undertakes to respond to this request in accordance with applicable laws and regulations, with the Customer's prior consent and within the statutory time limits, provided that the request was received by ALE within two days of the initial request.

To this end:

• The Customer must identify the contact person(s) and their duly authorized representatives to request that the Authorized Reseller (if ALE is not the Supplier) take or arrange for the actions necessary to respond to requests to exercise the Data Subject's rights.
• The Customer must identify and attach to the request a means of communication allowing for a direct response to the Data Subject: for example, an email from the requesting Data Subject.
Since ALE cannot identify a Data Subject's Health Data (e.g., text or file exchanges between two doctors regarding a patient), it is therefore the responsibility of the Client and its data controller to provide this information to the Data Subject in accordance with applicable regulations.

Upon request, the Customer may, either through its Authorized Reseller (if ALE is not the Provider) or directly to ALE, request access to the DSCP access logs generated by personnel under its control.

3.2.4: SECURITY

In connection with the provision of the Service, ALE undertakes to take all necessary precautions, given the nature of the Data and the risks posed by its processing, to preserve the security of the Data.

In particular, ALE undertakes to implement protective measures as well as the technical and organizational measures set forth in Appendix 1 to ensure the confidentiality, integrity, and availability of the Service and the Health Data in accordance with the security policies and guidelines of the Rainbow HDS service related to the Statement of Applicability resulting from ISO 27001 and HDS certifications.

The Statement of Applicability (SoA) relating to ALE's HDS certification is available upon request and in French from Rainbow Support via email at support@openrainbow.com.

The Parties undertake, in particular, to respect the founding principles of the PGSSI-S (General Policy on Health Information System Security) and to comply with the associated technical standards and guidelines.

It is ALE's responsibility to:

- Provide the Customer, throughout the duration of the Service and via an interface, with individual and secure access, based on strong authentication methods, to the Data hosted by ALE as part of the Service.
- Formalize a security policy whose scope covers the Service and the Data;
- Ensure the security of the network architecture and services related to the Service. In particular, ALE undertakes to ensure that under no circumstances will Data be transmitted in plain text over a public network.
- Maintain compliance with HDS and ISO 27001:2022
- Raise awareness among its staff regarding confidentiality and professional secrecy, particularly concerning personal health data submitted as part of the Service in accordance with the confidentiality clause as set forth in their employment contracts.
- Ensure the contractual implementation of non-disclosure agreements with its subcontractors who may have access to personal data. It is specified that said subcontractors may only access personal identification data within the scope of support but under no circumstances the content of communications, provided that the Client has taken care not to include Health Data in its support tickets.
- Ensure the traceability of access and operations performed on the Service and the Data, both by its staff and by Users, in accordance with the LCEN law;
- Retain connection logs for a period of twelve (12) months and implement the technical means necessary to extract data for the archiving of the Data
- Manage security incidents and notify the Authorized Reseller, who will inform the Customer in the event of a breach of data security in accordance with current regulations
- Implement a business continuity and disaster recovery plan.

The Customer is hereby informed that all Data and files exchanged within the scope of the ALE Service are retained for the duration of the Contract.

However, the Customer expressly acknowledges that ALE transfers the responsibility for certain legal and regulatory obligations to the Customer. To this end, the following obligations within the scope of the Service are exclusively your responsibility as the Customer:

- Ensure that its own Users involved in the Service manage Health Data in compliance with the PGSSI-S;

• Formalize a security policy whose scope covers Health Data;

• Ensure the security of workstations and equipment from which its Users, and any person authorized by the Customer, access the applications and Health Data;

• Carefully manage the authorizations, identification, authentication, and access control of its staff and users to the applications and Health Data;

• Ensure that no Health Data is included in tickets submitted to the Reseller's support team.

• Monitor the use of strong authentication methods by individuals authorized to access Health Data;

• Raise awareness and train your staff on information system security;
- Raise staff awareness regarding confidentiality and professional secrecy, particularly concerning personal Health Data submitted as part of the service, and identify the Users authorized to access Health Data;
- Archive and retain Health Data in accordance with PGSSI-S regulations
- Transmit and update the List of Contact Points as set forth in Appendix 2.

3.2.5: MANAGEMENT OF ACCESS TO HEALTH DATA

In accordance with applicable laws and regulations, access to
is restricted to healthcare personnel and individuals under the Client's authority.

The Client is responsible for managing the authorizations of the Service's end users, of any person whom it has individually authorized to access Health Data, and, where applicable, of Patients. The Client is also responsible for implementing the corresponding access rights and for monitoring the use of access methods, in compliance with applicable legal and regulatory provisions.

With regard to technical staff, the Client undertakes to grant access rights to Health Data only to individually identified persons who have a strict need to know and who are contractually bound to the Client. The Client is reminded that, in accordance with the applicable legal and regulatory provisions , these persons are subject to professional confidentiality.

It is the Client's responsibility to ensure that technical staff accessing the Health Data:

• are qualified to perform operations on the Health Data and to ensure the
security of such data;
• are trained in the management of Health Data and in respecting the privacy of
Data Subjects;
• are aware of the need to maintain professional confidentiality;
• have a confidentiality clause in their employment contract;
• are proficient in the enhanced security measures specific to health data;
• use individual access accounts;
• are equipped with state-of-the-art authentication methods, namely a username/password compliant with CNIL recommendations and strong authentication methods, such as the use of healthcare professional cards (CPS) as a second authentication factor.

With regard to Users, the Customer is solely responsible for ensuring that they:
• are legally authorized to access Health Data and to process Health Data;
• are bound by professional confidentiality, including medical confidentiality;
• access Health Data in compliance with applicable laws and regulations.

The Client is responsible for managing the access granted to Data Subjects. In particular, the Client ensures that the identity of Data Subjects is verified and that state-of-the-art strong authentication methods are used.

Once the Customer uses the Service, it is the Customer's responsibility, in accordance with applicable laws and regulations, to verify the Data Subject's direct access to the Service.

ALE and/or the Authorized Reseller shall in no event be held liable for any consequences of improper use by the Client's Users or by any person to whom the Client has provided access.

3.2.6: MAJOR CHANGES TO THE SERVICE

Any major changes to the Service, initiated by ALE, shall not result in any regression or non-compliance with the requirements regarding the protection of Health Data and the protection of Personal Data. ALE undertakes to ensure service continuity during major changes. ALE undertakes to inform the Customer of any major changes, in accordance with the legal and regulatory requirements in force regarding the hosting of health data.

3.2.7: FRENCH LANGUAGE SUPPORT

The application is available in its entirety in French. First-level support is also available in French.

3.2.8: INCIDENT MANAGEMENT

The Parties agree to cooperate in managing any Incident (excluding all incidents related to misuse of the Service, failure to comply with state-of-the-art security standards for the assets within the scope of the Depositor or the Service Provider, etc.). ALE undertakes to notify the Authorized Reseller as soon as possible—with a target of 48 hours—of any incident of which it becomes aware and which is likely to affect Health Data; the Authorized Reseller will then inform the Customer.

Communication is provided via the Rainbow Customer Service web . A crisis response team is organized to identify the causes and the corrective actions to be implemented. During this crisis management period , the Service may switch to degraded mode (for example, by isolating the affected system, filtering, or active monitoring, etc.). The Service may be restored online in particular through the Business Continuity Plan. If necessary, the Customer shall ensure that the relevant competent authorities, Users, and affected individuals are notified within the regulatory timeframes. In the event that ALE detects that the Service is compromised or experiencing a malfunction, ALE reserves the right to limit the Service until the problem is resolved, provided that ALE deems such resolution possible.

Excluded from this process are all Incidents related to misuse of the Service by the Customer or the Customer's failure to comply with state-of-the-art security standards for assets within their scope.

3.2.9: POINT OF CONTACT

The Parties (ALE, the Authorized Reseller of the Service, and the Customer) agree to each designate a primary contact and a secondary contact responsible for the proper performance of the Service, including security issues. This contact must be able to designate a healthcare professional to ALE when necessary (e.g., access to health data, management of patient relations).

The Customer shall ensure the designation of at least one primary and one secondary contact person responsible for issues related to the processing of Health Data on the Service. The Customer shall provide the Authorized Reseller with its contact points and ensure that the Authorized Reseller is aware of these contacts (in the event that ALE is not the reseller of the Service). In this regard, the Customer agrees to complete the Contact Information Form in Appendix 2 and ensure it is regularly updated; this form must be submitted to ALE via its Authorized Reseller. To this end, the Authorized Reseller submits an eService Request (eSR) with this Contact Information Form attached, indicating the following keywords in the eSR: "HDS" and "Contact."

All of these contacts must facilitate communication between the Parties.

ARTICLE 4: SUBCONTRACTING

The Customer is informed that ALE uses subcontractors in connection with the performance of the Service, a list of which is provided in Appendix 3.

1. The Service is hosted by an HDS-certified hosting provider.

It is understood that if ALE offers multiple hosting providers and/or data center locations in the list of its subcontractors in Appendix 3, the Client will have the choice of where to locate its Data.

ALE may modify the list of its subcontractors at any time as set forth in Appendix 3, provided that it informs the Customer in advance.
ALE undertakes to include, in the agreements it enters into with the sub-processor, the obligations incumbent upon it under the applicable legal and regulatory provisions; in this regard, ALE has entered into a data processing agreement in accordance with the GDPR.

ARTICLE 5: LIABILITY

ALL PROVISIONS OF ARTICLE 9 OF THE GENERAL TERMS OF USE FOR THE RAINBOW PAID SERVICE SHALL APPLY IN THEIR ENTIRETY.

FURTHERMORE, ANY LIABILITY OF THE SERVICE PROVIDER, ITS AFFILIATES, ANY THIRD-PARTY PROVIDER INVOLVED IN THE PROVISION OF THE HDS SERVICE (INCLUDING, WITHOUT LIMITATION, IN CASES WHERE YOU PURCHASED THE SERVICE FROM AN AUTHORIZED RESELLER), THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS COLLECTIVELY, SHALL NOT BE HELD LIABLE (i) IN THE EVENT OF THE CUSTOMER'S FAILURE TO COMPLY WITH ITS OWN LEGAL OBLIGATIONS (ii) FOR THE DISCLOSURE OR UNLAWFUL USE OF THE PASSWORD CONFIDENTIALLY PROVIDED TO THE CUSTOMER (iii) FOR THE PARTIAL OR TOTAL DESTRUCTION OF INFORMATION TRANSMITTED OR STORED AS A RESULT OF ERRORS DIRECTLY OR INDIRECTLY ATTRIBUTABLE TO THE CUSTOMER (IV) IN THE EVENT OF LOSS OR DAMAGE TO DATA ENTRUSTED TO ALE IN CONNECTION WITH THE SERVICE.

IT IS RECALLED THAT ALE PERFORMS DATA BACKUPS AS PART OF THE SERVICE, BUT THIS DOES NOT EXEMPT THE CLIENT FROM PERFORMING A COMPLETE BACKUP OF THEIR DATA FOR ARCHIVING PURPOSES. IN THIS REGARD, IT IS RECALLED THAT IT IS THE CLIENT'S RESPONSIBILITY TO REGULARLY ENSURE THE ARCHIVING OF HEALTH DATA AND ITS STORAGE ON A TAMPER-PROOF MEDIUM IN ACCORDANCE WITH APPLICABLE REGULATIONS.

ARTICLE 6: DISASTER RECOVERY PLAN AND BUSINESS CONTINUITY PLAN

Mechanisms and features are in place to ensure the availability and continuity of the Service. ALE notes that the Service has established and maintains a business continuity plan (BCP) as well as a disaster recovery plan (DRP).
These documents describe the nature of the systems, the system testing activities performed by ALE, and the conditions for triggering the BCP and BRP.
The RTO (Recovery Time Objective) and RPO (Recovery Point Objective) values are set at 48 hours and 24 hours, respectively.

ARTICLE 7: Quality and Performance Indicators

ALE provides a continuous service that allows users to view the status of the service and ongoing operations via the website https://status.openrainbow.health/. These metrics are monitored continuously.

The service availability rate is 99.5%.

ALE does not impose penalties for failure to meet availability targets.

ARTICLE 8: AUDIT – HDS CERTIFICATION

8.1 As part of the Service's organizational structure, ALE has implemented an HDS-certified information security management system. ALE undertakes to maintain this certification (or any equivalent certification) for the duration of the Contract, and in this context, annually commissions an accredited body to conduct a follow-up audit and, every three years, to issue the HDS certification. This accredited body appoints a recognized auditor in this field to audit the Service in accordance with the provisions of the HDS standard.

8.2 Under the HDS framework, the Customer may, subject to the conditions set forth in the Service audit procedure, conduct or have conducted at its own expense an audit regarding compliance with the HDS framework.
8.3 In the event of loss of its Certification, ALE shall immediately notify the Authorized Reseller, who shall in turn notify the Customer. In such a circumstance, the Customer may terminate the Contract as of right and without compensation. Since the Service is contingent upon ALE's HDS certification, the Customer acknowledges that any loss of certification by ALE entails the Customer's obligation to recover the Health Data that it may have exchanged within the scope of the Service.

In this event, ALE undertakes to assist the Customer in the full recovery of the Health Data, under the conditions set forth in Article 8. Reversibility.

8.4 ALE undertakes to provide, upon request, the latest HDS certification audit report via email to support@openrainbow.com

8.5 The Client may request that ALE provide a management summary of a technical audit report covering the shared resources within the scope of the Service. The audit report must not be more than 3 years old.

ARTICLE 9: REVERSIBILITY

ALE will ensure the return of the Data to the Customer within thirty (30) days of receiving a ticket requesting the return of the data, following the termination of the Service, i.e., the end of your Subscription Agreement, regardless of the cause.
To request data return, the Authorized Reseller agrees to open a ticket with ALE on the Business Portal to request the return of the data. The subject of this ticket will be "Reversibility HDS." ALE will return the data to the Customer within thirty (30) days.
From the date of the request to terminate the Service for the Customer in question, the Authorized Reseller agrees not to modify any of this Customer's data or configurations and not to delete the Rainbow company created in the HDS environment.
The Client will retrieve their Data in a digital file format defined by ALE that is readable by the Client. DSCPs and metadata will be provided in open formats. Attached documents will retain their original format.
To this end, the Customer shall provide ALE with a secure data storage space and shall define, together with ALE and the Authorized Reseller, the secure communication channels to be used (email, text message, etc.) for exchanging integrity control and access rights information.
The Customer is informed that ALE will delete all Data that the Customer has uploaded to the Service sixty (60) days following the end of the Service.
At the end of this sixty (60)-day period, the data will be deleted, and neither ALE nor the Authorized Reseller may be held liable for any failure to reconcile the Data that was not duly detected by the Customer during the reversibility process. Verification of the complete restoration of the Data is the sole responsibility of the Customer.
Subject to the data that ALE is required to retain in accordance with applicable regulations and the data necessary to defend its rights, ALE undertakes, upon completion of the reversibility operations, not to retain any copy of the relevant data.
ALE does not charge any fees for the reversibility process provided that the data extraction and transfer do not take more than three (3) business days. If the duration is extended due to data volumes or delays caused by the Client, ALE may request payment for time spent beyond the 3-day period. This rule shall not apply in the event that ALE is responsible for the loss of its HDS certification.

List of Appendices:
APPENDIX 1 – TECHNICAL AND ORGANIZATIONAL MEASURES
APPENDIX 2 – RAINBOW HDS SERVICE CONTACT INFORMATION – CLIENT
APPENDIX 3 – LIST OF SUBCONTRACTORS
APPENDIX 4 – HDS CERTIFICATES

Appendix 1
Technical and Organizational Measures
ALE Rainbow

Contents

Foreword
The purpose of this document is to list the technical and organizational measures implemented at ALE, which contribute to adequately protecting not only data in general, but also and above all personal data.
These measures aim to meet standard control objectives regarding confidentiality, integrity, and availability, which constitute a standard methodology for demonstrating that an adequate level of data protection exists and is effective.
Identification of Responsibilities:
Within the scope of the Rainbow service, ALE is the data controller and data processor in all situations, except when the service is provided from a private cloud operated by an entity other than ALE. Thus, except in the latter case, ALE is the data processor and outsources the hosting and connectivity of the data center as well as its security.
Certified Security
Rainbow is certified according to the DIN ISO 27001:2013, ISO 27017, and ISO 27018 standards, which can be viewed at any time at https://support.openrainbow.com/hc/fr/articles/360003802400-ISO-Certification-EN-

Hosting with OVH

OVH is committed to ensuring the optimal security of its infrastructure, in particular through the implementation of an information security policy. Furthermore, OVH's infrastructure complies with numerous international standards and is certified according to PCI DSS, ISO/IEC 27001, SOC 1 TYPE II, and SOC 2 TYPE II, among others.
For more information on data protection and security at OVH, visit https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml#accordion_1872-1.

1. Confidentiality

1.1 Physical Access Control and Security

Physical access protection; data center (OVH

The data center is operated by the provider OVH. You can find more details on security measures at https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml.

General security measures for physical sites
Physical access is based on restrictive contextual security, which applies starting at the entrance area. Each site is divided as follows:

- Private circulation areas
- Offices accessible to all employees and registered visitors
- Private offices accessible only to authorized personnel
- Areas housing data center equipment
- Private data center areas
- Data center areas housing critical services
- General security measures for physical sites

The following security measures are implemented to control access to OVH's physical sites:

- An access authorization policy
- Partitions (or similar installations) between each zone
- Cameras at the entrances and exits of the premises and in the server rooms
- Secure access, controlled by badge readers
- Laser barriers in the parking lots
- Motion detection system
- Burglary prevention mechanisms at the entrances and exits of data centers
- Mechanisms for detecting unauthorized intrusions (24-hour security service and video surveillance)
- Permanent monitoring center that monitors the opening of entrance and exit doors

Physical access control is managed via a badge system. Each badge is linked to an OVH account, which is in turn linked to a specific individual. Thanks to this system, every person on the premises can be identified and access controls verified:

- Anyone entering OVH sites must have a personal badge linked to their identity.
- Each identity must be verified before a badge is issued.
- The badge must always be worn visibly on the premises.
- Badges must not display the owner's name or the company name.
- It must be possible to immediately identify the category of people present using the badge (employees, third parties, temporary access, visitors).
- The badge will be deactivated as soon as its holder is no longer authorized to access the premises.
- OVH employee badges are activated for the duration of the employment contract; for other categories,
- the badge is automatically deactivated after a specified period. Badges that are not used for three weeks are automatically deactivated.

Door access via badge. This is the standard access control system at OVH's premises:

- The door is connected to the central access authorization management system.
- The person must present their badge in front of the special reader to unlock the door.
- Each access attempt is verified during reading to ensure that the person has the appropriate authorization.
- In the event of a failure in the central access authorization management system, the authorizations configured at the time of the failure remain valid for the duration of the incident.
- The door locks are protected against power outages and remain locked in such situations.

Key-controlled access to doors. Certain areas or pieces of equipment are equipped with locks that can be secured with keys:

- The keys for each site are stored in a centralized, restricted-access location and listed in an inventory.
- Each key is labeled with an identification tag.
- A key inventory is kept up to date. Each use of the keys can be tracked using a management system or a paper log.
- The key inventory list is checked daily against the inventory.

Access to data centers via single-person airlocks. Access to our data centers is exclusively via single-person airlocks:

- Each airlock consists of two doors and a closed area between them to ensure that only one person passes through at a time.
- One door can only be opened when the other is closed (airlock).
- The airlocks use the same badge system as the other doors, and the same rules apply.
- Detection mechanisms verify that only one person is in the airlock (anti-piggybacking).
- The system configuration prevents the badge from being used more than once in the same direction (anti-passback).
- Thanks to a camera installed in the airlock area, access can be monitored.

Access to goods airlocks. Goods are received at data centers exclusively through specially designed entry points:

- The delivery area is configured in the same way as a single-person airlock, but with more space, no volume or weight checks, and badge readers located only outside the airlock.
- Only the delivered item passes through the delivery area; people must enter via the single-person airlocks.
- A camera with no blind spots is installed in the delivery zone.

Protection of access to ALE facilities

At ALE sites, teams have remote access to the Rainbow instance.

Physical access protection measures

Locking systems

ALE generally uses electronic access control systems. The corresponding access authorizations are assigned organizationally and technically by authorized personnel. There are rules regarding the use of electronic locking systems, such as how employees should act if a transponder is lost.
Manual locking systems are still sometimes used at smaller ALE sites.

ALE ID Cards / Badges

ALE badges are mandatory and indicate status (employee, visitor, guest, or non-employee). They remain the property of the company and must be worn visibly.

Visitor Policy

Visitors are registered and must always be accompanied by an ALE employee.

Sensitive Areas

Access to sensitive areas (e.g., the data center) is authorized and logged on a need-to-know basis. Sensitive areas are also monitored outside of regular business hours.

Delivery and Loading Areas

Delivery and loading areas used for the receipt or distribution of ALE goods are equipped with an exterior door and an interior door that do not open simultaneously.

Video surveillance

Video surveillance / closed-circuit television (CCTV) covers the main entry points, the main lobby, the loading dock, and the parking lots at large sites.

Clean Desk Policy

Each desk must be tidied up at the end of the workday, and computers must be turned off.

Security windows

Window restrictors are installed on the ground-floor windows.

1.2 Access Control to IT Resources

Access control for infrastructure resources (OVH hosting provider)

- All employees use personal user accounts.

- Login sessions automatically expire after a duration appropriate for each application.
- Before any changes are made to authentication methods, user identities are verified.
- The use of standard, generic, and anonymous accounts is prohibited.
- All access to resources is managed via authentication using individual SSH keys. The validity of individual SSH keys must be renewed every 3 days.
- All access is logged, stored, and reviewed regularly

Access control to infrastructure resources on ALE premises

Identity and access management
Identity and access management is based on the role or task to be performed and reflects the principles of separation of duties and the principle of least privilege.

Unique user ID and access
Each person is assigned a unique **user ID** to access ALE information resources.
Account names must distinguish between user, administrator (privileged), and service accounts.

User ID / Service Account Authentication and Password Management

Authentication mechanisms may include:
i) password/PIN, or
ii) two-factor (such as a password or PIN combined with a hardware device, software token, or digital certificate).

Password Policy
Passwords must be at least eight (8) characters long for user accounts and twenty (20) characters long for service accounts. Passwords must contain at least three of the following four categories: uppercase letters, lowercase letters, numbers, and special characters.

Monitoring of ALE Information System Usage
- Ensure compliance with applicable laws and regulations;
- Detect any violations of applicable laws and regulations;
- Ensure the effective use of information systems and their normal operation;
- Ensure the effective confidentiality and integrity of ALE data, as well as employees' compliance with their security obligations;
- Ensure the effective security of ALE's information systems by implementing features to detect security threats—including viruses, Trojan horses, worms, malware, and spam (unsolicited messages)—as well as protection against them and forensic investigations.
- Ensure cost control.

(not limited to the above)

Organizational Measures
- Authentication Guidelines
- Information Security Policy
- Guidelines on the use of the intranet and the Internet
- Guidelines on email communication

Other Technical Measures
- Use of Professional Firewalls
- Use of antivirus software
- Use of intrusion detection systems

- Internet proxy management
- SSO/SAML
- Restricting access to servers

User access control in Rainbow

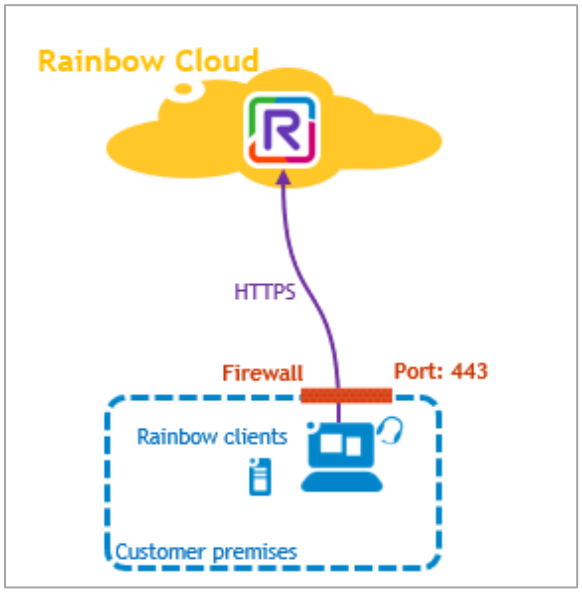
Rainbow offers various options for authenticating users

a) Internal Authentication

By default, Rainbow users are authenticated by the Rainbow service. In this case, Rainbow knows how to verify the user's credentials and is responsible for this verification. When a user opens the Rainbow UCAAS application, the Rainbow login form appears and is used for authentication.

- Let Rainbow fully manage the security rules regarding credentials and passwords.
- Under the control of the Rainbow administrator.
- No configuration required—this is the default solution.

Internal Authentication



Internal authentication implements several security rules:

- During self-registration, an email is sent to verify the account creation.
- User passwords must meet a minimum complexity requirement
  At least 8 characters (maximum 64)
  - 1 lowercase letter
  - 1 uppercase letter
  - 1 digit and
  - 1 special character.
- Password reset is secured by a temporary 6-digit PIN sent to the user's email address
- It must then be entered during the password update process

Access control to Rainbow services is based on the role assigned to users by the administrator:

- Guest
- User
- Company Administrator

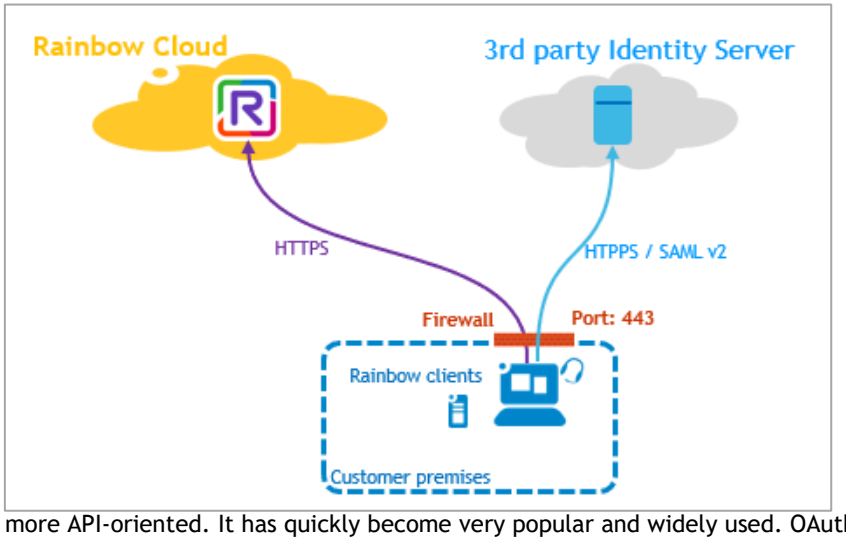
b) External authentication

Overview

- Delegates security rules related to usernames and passwords to an external centralized authentication server (e.g., MS Azure AD).
- Allows the same password to be used across multiple applications
- Supports only cloud-based authentication servers.
- Supported on PCs and smartphones (iOS, Android).
- Supports HTTPS/SAML v2 and OIDC (OpenID Connect) protocols.
- OIDC (OpenID Connect) is based on OAuth2
- SAML v2 (Security Assertion Markup Language)

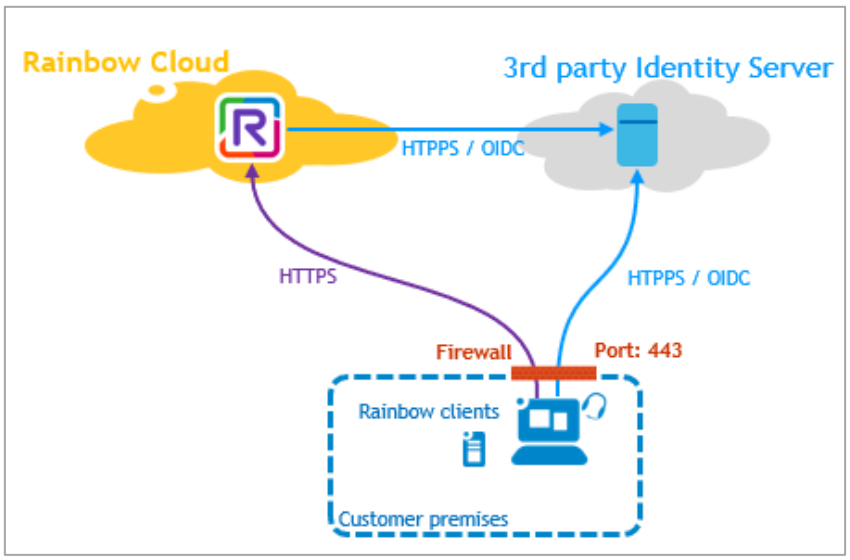
Details
The Rainbow solution allows you to use an external identity provider based on SAML and OIDC. In this use case, from an administrative standpoint, the administrator of the company's authentication service must declare a new external service in the external identity service (such as in the Microsoft Azure administration interface) used by the company to allow Rainbow to interact with it when a user needs to log in.

External Authentication via SAML v2
Security Assertion Markup Language (SAML v2) is a protocol used for authentication. This protocol is widely used because it has been deployed in the enterprise world for a long time. This technology relies primarily on interactions with web browsers. This protocol allows access to a protected resource using a centralized authentication service without granting access to credentials to external entities. For example, you can log in to your Rainbow account using your corporate username and password, but Rainbow does not need access to the corporate credentials. Since there is a decoupling between the protected resource and the entity that controls identity, SAMLv2 allows the user to use the same credentials to access a wide range of protected resources or services. This use case is also well known as the principle of single sign-on (SSO).



External authentication via OAuth2
OAuth2 is a framework designed to grant authorizations. More recent than SAMLv2, it is less tied to the web browser and more API-oriented. It has quickly become very popular and widely used. OAuth2 is designed to grant authorizations, not for authentication. Many applications used OAuth2 to perform authentication as well (and still do). Since the user must be identified to request authorization, this is not a problem. However, each application must define a specific method to return the user's identity to the external application. This is what OIDC is intended to do, but in a well-standardized format.

External Authentication via OIDC
Open ID Connect (OIDC) is a protocol based on OAuth2 that enables authentication (just like SAML does). OIDC is also used to implement single sign-on (SSO). OIDC builds on the technologies and popularity of OAuth2 and will eventually replace SAMLv2.



Encryption and security

- End-user passwords are hashed and salted in Rainbow's internal database.
- All data (instant messages, files) exchanged between users or via bubbles is encrypted in transit and at rest.
- For transit, HTTPS + WSS via TLS 1.2/1.3 only
- At rest, AES 256-GCM is used
- Voice/video communications are natively encrypted using WebRTC technology with DTLS and SRTP.
- All files uploaded by users are systematically scanned by antivirus software (ClamAV) before being stored and transmitted.

1.3 Access control for data processing and data

Measures for managing access control to data processing and data at the hosting infrastructure level (OVH)

- Access permissions are granted and monitored by supervisors in accordance with the principle of least privilege and the principle of progressive trust.
- To the extent possible, all access authorizations are based on roles rather than individual rights.
- The management of access rights and authorizations granted to a user or system is carried out through registrations, modifications, and deregistrations performed by supervisors, the internal IT department, and human resources.
- All remote access to OVH's information system is conducted via a VPN. This requires a certificate known only to the user and a shared secret configured on the workstation.
- Data is encrypted at rest and in transit
- The cloud infrastructure provider has no logical access to the servers.

OVH Network Security

OVH manages a high-performance private fiber-optic network connected to numerous operators and carriers. OVH manages its own backbone internally. It distributes connectivity to the local networks of each data center and interconnects them.
All equipment is secured by the following measures:

- Inventory management in a configuration management database
- Implementation of a security hardening process, with instructions on which settings to modify to ensure a secure configuration
- Access to device administration functions is restricted via access control lists
- All devices are managed by a bastion host following the principle of least privilege
- Backups are performed for all network device configurations
- Logs are collected, centralized, and continuously monitored by the network operations team
- Configuration deployment is automated and based on approved templates

Access control to OVH's cloud IT systems

OVHcloud enforces a strict policy for managing logical access rights. This policy includes the following provisions:

- Access rights are granted according to the “least privilege” principle.
- Access rights must be based on roles rather than on rights specific to individual units.
- Granting access to a user or system is managed through procedures for initial provisioning, modification, and deletion, involving their managers, IT support/central services, and HR.
- All employees use accounts with a unique user ID.
- Automatic logout after a period of inactivity.
- The use of generic and/or anonymous user accounts is prohibited.
- A strict password policy is enforced.
- Passwords must be randomly generated.
- Terminals have a minimum password length of 10 alphanumeric characters.
- It is prohibited to save passwords in unencrypted files, on paper, or in web browsers.
- The use of local password management software approved by the IT security department is mandatory.
- Remote access to OVH cloud computing systems must be via a VPN. A password known to the user and a client certificate configured on the workstation must be used.

ALE IT Resource Access and Security Management Measures

Access Policy

Access is controlled through the use of roles and permissions, is logged, and activities are monitored. A complete description is provided in the ALE security directive (ALE_000835).

Access Control Principles

Business requirements for access control:

Authorizations granted according to the "need-to-know" principle Each user ID can only access data that is
(a) non-confidential (public)
b) necessary for the performance of individual professional duties
c) authorized by a supervisor

Access rights management:

N+1 level managers are involved. Logins are blocked if they are not used.

System and application access control:

- Session control:
  There are many IT resources that can be accessed (network connection, workstation, mobile device, router), and each is subject to specific lockout rules after a certain number of failed attempts.
- Access to advanced features:
  These require user consent (e.g., registration)
- Network access control:
  Whitelist for wired access; encryption for wireless access.
- Access to external network services:
  All external network services are filtered by the company’s security devices, which allow only specified protocols, ports, source and destination IP addresses, applications, and session timeouts. Whitelist of services in place.
- Outbound user access:
  Use of a proxy and traffic monitoring. Remote access requires strong authentication.
- Remote management and diagnostic ports:
  Port management (deactivation) is used to manage this security.
- Network segmentation:
  Networks not managed by the IT department are segmented (even in the absence of external connectivity). Routers or firewalls are used to allow only necessary traffic, if any, to pass through the corporate network.
- Dual-connected computers:
  It is prohibited to connect to a network outside the company using company resources.
- Network routing:
  The ALE network’s routing and switching infrastructure is monitored to detect denial-of-service attacks. External access to network information regarding the company’s internal network is restricted
- The Domain Name System (DNS) is protected against untrusted networks:
  Management of externally accessible information; no redirection of internal DNS queries.

Measures for managing access control to data processing and data at Rainbow

Role definitions

Rainbow users within an end-customer company can have one of the following two roles:

- Company Administrator
  - In addition to the rights of a standard user, they can administer their company.

- As a standard user
  - Access to Rainbow features will depend on their Rainbow subscription.

Restricting access to the file sharing feature
To control file exchanges between users, access to the "File Sharing" feature (uploading and transferring) can be restricted. The configuration is performed by the company administrator for the entire company or for each user individually.
Restricting username changes
To prevent identity theft, you can prevent users from changing their title, first name, and last name.

Encryption and security

Encrypted storage of the password database
End-user passwords are hashed and salted in Rainbow's internal database.

Encryption in transit and at rest

- All data (instant messages, files) exchanged between users or via bubbles is encrypted in transit and at rest.
- For transmission, HTTPS + WSS via TLS 1.2/1.3 only.
- At rest, the AES 256-GCM algorithm is used.
- Voice/video communications are natively encrypted using WebRTC technology with DTLS and SRTP.

Antivirus scanning of files
All files uploaded by users are systematically scanned by antivirus software (ClamAV) before being stored and transmitted.

1.4 Client isolation controls

Multi-client capability
- Rainbow is fully compatible with multi-client management
- Logical separation of client accounts

Client-specific features:
Rainbow Edge offering: https://support.openrainbow.com/hc/fr/articles/360012465520

Separation of test and production systems
- Test environment for new software applications or critical updates.
- Deployment only takes place after a successful test.

1.5 Pseudonymization

Pseudonymization of request logs

All requests sent to the Rainbow app are logged
The logs are:

- fully anonymized.
- sent to a server cluster where they are stored redundantly.
- retained for the minimum period required by law.

2. Integrity

2.1 Transfer Controls

Encrypted communications in Rainbow

Any unencrypted connection from the Internet is systematically rejected

Only HTTPS connectivity is used (port 443)

- WebSockets are therefore secured
- No other services are open to the public Internet
- Access to port 80 is automatically redirected to port 443

OpenSSL, used for encryption, is always kept up to date.

SSLv2, SSLv3, TLS 1.0, and TLS 1.1 are disabled in favor of TLS 1.2 and TLS 1.3

- We do not support obsolete and insecure SSL.
- All HTTPS negotiations are conducted exclusively via TLS

Standard Gandi / Comodo CA Wildcard SSL/TLS certificates

- With a 256-bit ECDSA key (elliptic curve) and signed with RSA-SHA256.
- No self-signed certificates are used.

2.2 Entry Checks

Input controls at ALE

It is possible to verify and determine retrospectively whether data has been entered, modified, or deleted in the IT systems, and by whom:
- user profiles
- user identification
- authorization concepts

The logging functions of all production systems operate continuously and are retained for a sufficient period of time.

Rainbow Access Control (Log Analysis)

Rainbow Security Summary: https://support.openrainbow.com/hc/en-us/articles/115001019330

The ALE Rainbow operations team is able to accurately analyze stored activity logs in the event of:

- attacks,
- suspicious activity,
- or upon legal request.

End customers and business partners do not have access to the logs.
If necessary, the ALE operations team can extract specific information for them on an ad hoc basis.

Log analysis allows us to determine:

- The source IP address,
- The user's identity,
- The date and time of the requests,
- The type of requests.

Log analysis does not under any circumstances allow for the retrieval of:

- Conversations / Discussions
- Passwords

3. Availability and Resilience

3.1 Availability monitoring

Operational continuity (server)

Operational continuity of the infrastructure (availability of devices, applications, and operational processes) is ensured by various measures:

- Continuous liquid and air cooling
- Uninterrupted and redundant power supply
- Equipment capacity management under the responsibility of cloud providers
- Technical support for the service
- Redundancy of devices and servers used for system administration
- In addition, other mechanisms, such as backing up network equipment configurations, ensure system recovery in the event of a failure

Prevention of natural and environmental risks

- Installation of lightning rods to reduce associated electromagnetic waves
- Locating cloud service providers' facilities in areas not exposed to flood or earthquake risks
- An uninterruptible power supply (UPS) with sufficient capacity and auxiliary transformers with automatic load switching
- Automatic switching to electric generators with a minimum runtime of 24 hours
- Installation of a liquid cooling system for servers (98% of server rooms are not air-conditioned)
- Use of heating, ventilation, and air conditioning (HVAC) units that maintain constant temperature and humidity
- Management of a fire alarm system (fire evacuation drills are conducted in data centers every 6 months)

Technical measures for availability

To ensure high data availability, various mechanisms are in place:

- At the hardware level with HA disks
- Databases are clustered and replicated
- User files and static data are stored in triplicate on replicated OpenStack Swift object storage servers

Backup of all databases

- Frequency: hourly snapshots of the database file system
- Daily backup of databases to two remote sites and with two providers

High availability

- HA on servers, storage arrays, and disks under ALE's responsibility
- High availability for power and network under the responsibility of the hosting provider (OVH).

Monitoring

A monitoring infrastructure is in place for all OVH services. It has several objectives:

- Detection of production and security incidents
- Monitoring critical functions and triggering alerts to the monitoring system
- Notifying responsible personnel and initiating corresponding procedures
- Ensuring service continuity during the execution of automated tasks
- Verifying the integrity of monitored resources

Business Continuity Plan (ALE)

ALE has implemented a business continuity plan based on the ISO 27001 standard and specified by the requirements of the ISO 27018 standard (an extension of the ISO 27001 standard).

3.2 Resilience/Load Capacity

Protection against DDoS attacks and firewalls

You can find detailed information here: https://www.ovh.de/anti-ddos/.

Rainbow is protected against DDoS (distributed denial-of-service) attacks thanks to the solution created by OVH called VAC (vacuum).
- Fully configured and managed by OVH.

VAC is a combination of technologies developed by OVH to:
- quickly analyze data packets in real time
- redirect incoming traffic to your server
- separate illegitimate requests from others and allow legitimate traffic through

This is a black box whose filters are not disclosed for security reasons.
- It is a packet-filtering hardware device based on ASIC technology.

VAC processing occurs in four stages

1. pre-firewall
   It is fully managed by OVH and applies rules that define filters directing data packets to the firewall network

2. Firewall network
   The firewall network is a solution that limits exposure to attacks originating from the public network. It activates automatically as soon as a DDoS attack begins.

3. Shield
   Shield intervenes if an attack uses an amplification technique (DNS amp, NTP amp). Armor is the most advanced filter in our VAC and mitigates the most powerful attacks.

4. Armor
   Armor is the most advanced filter in the VAC and intervenes to mitigate the most powerful attacks.

4. Procedures for regular review, evaluation, and analysis (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

A. Data Protection - Management

The following policies, procedures, or guidelines regarding data security are documented in ALE's ISMS:
- Confidentiality obligation for all employees (data confidentiality)
- Employee awareness measures.
- ALE Safety Charter
- ALE Security Guidelines
- ALE Security Policy
- ALE Data Protection and Privacy Policy
- ALE GDPR Policy
- Crisis Management Guidelines: Policy and Procedure
- Guidelines on Confidential Information
- Information Management System
- Audits Conducted by the Data Protection Officer
- Audits by external auditors
- Documented processing activities.
- Regular review of technical and organizational measures.
- Rigorous selection of service providers (see also the "Contract Management" section).
- ISO 27001 certification, including ISO 27017 and ISO 27018

B. Data Protection Officer

Louis-Philippe Ollier
Email: dataprivacy@al-enterprise.com
Phone: +331 5566 3147
The DPO's contact information is also available at https://www.al-enterprise.com/en/legal/privacy

C. Incident Management

OVH

An incident management process is in place. It enables the prevention, detection, and resolution of such events within the service management infrastructure and the service itself. This process includes:

- A security incident classification guide
- Security incident management
- Simulation exercises for the crisis response team
- Tests of the disruption response plan
- Communication with customers as part of a crisis management team

These procedures are subject to a continuous improvement process for incident monitoring and assessment, overall incident management, and associated corrective actions.

ALE

Crisis management guidelines

Established and documented processes for incident management

- Defined responsibilities
- Defined reporting channels
- Procedure in the event of a data breach

D. Privacy by Design

As a matter of principle, the Rainbow service collects and processes only data that is appropriate and necessary for business purposes. Automated data collection and processing procedures are designed to ensure that only necessary data is collected.

There is no behavioral data management in Rainbow. No data collected for, generated in, or resulting from Rainbow's activities or the analysis of those activities is shared with or sold to third parties.

Rainbow can be used with a minimum of information, namely an email address and a password.

E. Contract Management

If processors are used for data processing, certain requirements apply. These include ensuring that the processors' technical and organizational measures comply with Article 28 of the GDPR, in conjunction with Article 32(1) of the GDPR.

The following requirements apply to a subcontracting relationship:

- Detailed information on the purpose, nature, and scope of the processing and use of the customer's personal data, in accordance with Article 28(3) of the GDPR. The corresponding details are set forth in the contract.
- German/EU service providers have appointed a company-designated data protection officer where required by law and ensure, through their data protection organization, that the data protection officer is appropriately and effectively integrated into the relevant operational processes.
- Verbal orders must be confirmed and documented in writing.
- Individual contracts are awarded only through designated contacts.
- Only restrictive access permissions are granted for the relevant technical environments. In the case of external access to the system, access will be deactivated or blocked after the end of the cooperation.
- For the transfer of personal data to external service providers, a standard data processing agreement is available that includes appropriate safeguards.
- ALE has entered into data protection agreements with all its affiliated parties, where applicable, in accordance with the provisions of Article 28 of the GDPR.

APPENDIX 2 – RAINBOW HDS SERVICE CONTACT INFORMATION – CUSTOMER

The Customer shall provide the Authorized Reseller with its contact details and ensure that the Authorized Reseller is aware of the relevant contacts (in the event that ALE is not the reseller of the Service). The Authorized Reseller agrees to enter the Client's and its own contact details on the Rainbow portal. The Client and the Authorized Reseller shall ensure that these contact details are regularly updated, as this form must be submitted to ALE via its Authorized Reseller to ensure:

- To designate a healthcare professional to ALE when necessary (e.g., access to Health Data, management of patient relationships).
- To handle incidents that impact the Health Data hosted as part of the Rainbow Service.

Organization
Rainbow HDS Service Client Entity:
Company Name:
Address:

Primary Contact
First Name Last Name:
Job Title:
Email:
Phone:

Secondary contact (if the primary contact is unavailable)
First Name Last Name:
Position:
Email:
Phone:
Data Protection Officer (or person responsible for compliance with personal data processing) to be contacted regarding the handling of incidents affecting Health Data hosted as part of the Services.
First Name Last Name:
Position:
Email:
Phone:

APPENDIX 3 – List of Processors

1. **Hosting Provider:**

- **OVH Healthcare in France, HDS-certified hosting provider.**
  - Address: OVH, Head Office, 2 Rue Kellerman, 59100 Roubaix, France
  - OVH Strasbourg Data Center (SBG3)
    9, rue du bassin de l'industrie
    67 000 Strasbourg
  - OVH Roubaix Data Center (RBX2a and RBX8)
    2 Kellermann Street
    59 100 Roubaix

2 **Backup:**

- **IBM, HDS-certified hosting provider**
  - IBM Data Center (PAR1)

9 Petit Clichy Street
92110 CLICHY

3 Incident ticket routing is managed by SalesForce's technical support team

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

3. The corrective maintenance service relies on technical support from:

1. from X-ACT.
   Address: X-act Luis Morote 6, 6th Floor, 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

APPENDIX 4 – HDS ALE INTERNATIONAL, OVH, and IBM CERTIFICATION

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

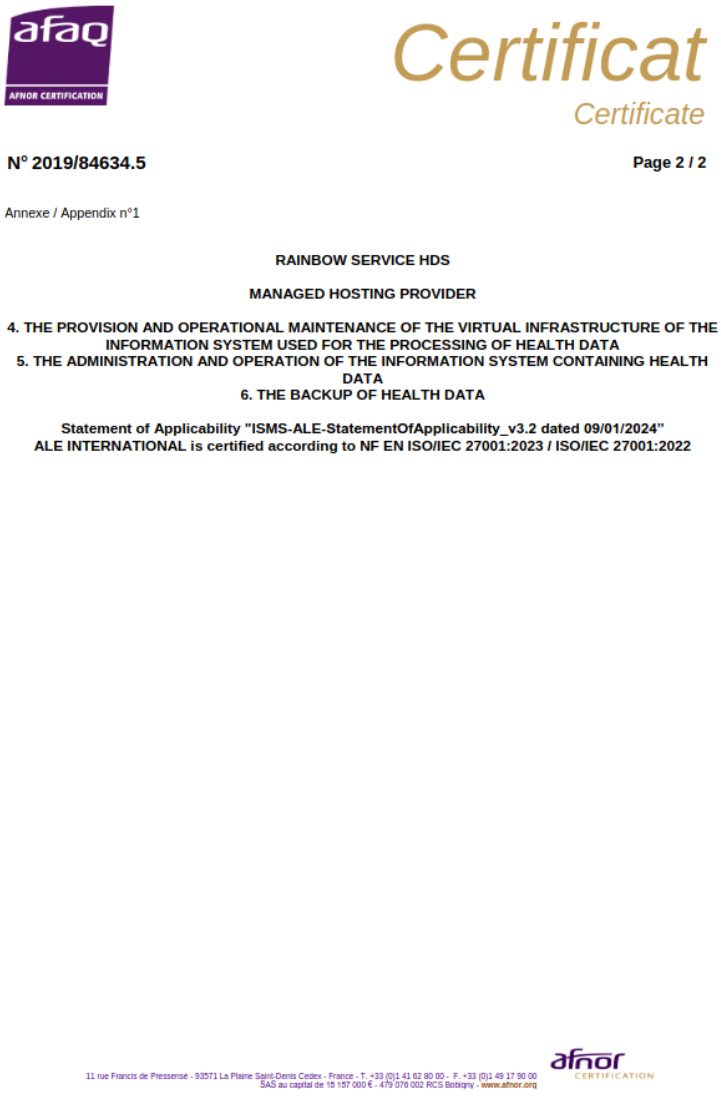
Ce certificat est valable à compter du (année/mois/jour) *This certificate is valid from (year/month/day)* **2024-05-14** Jusqu'au *Until* **2027-05-13**

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

OVH HDS v2 Certificate

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

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

Ozarow	
Toulouse	

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

BYCYB
build your cyber

			(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

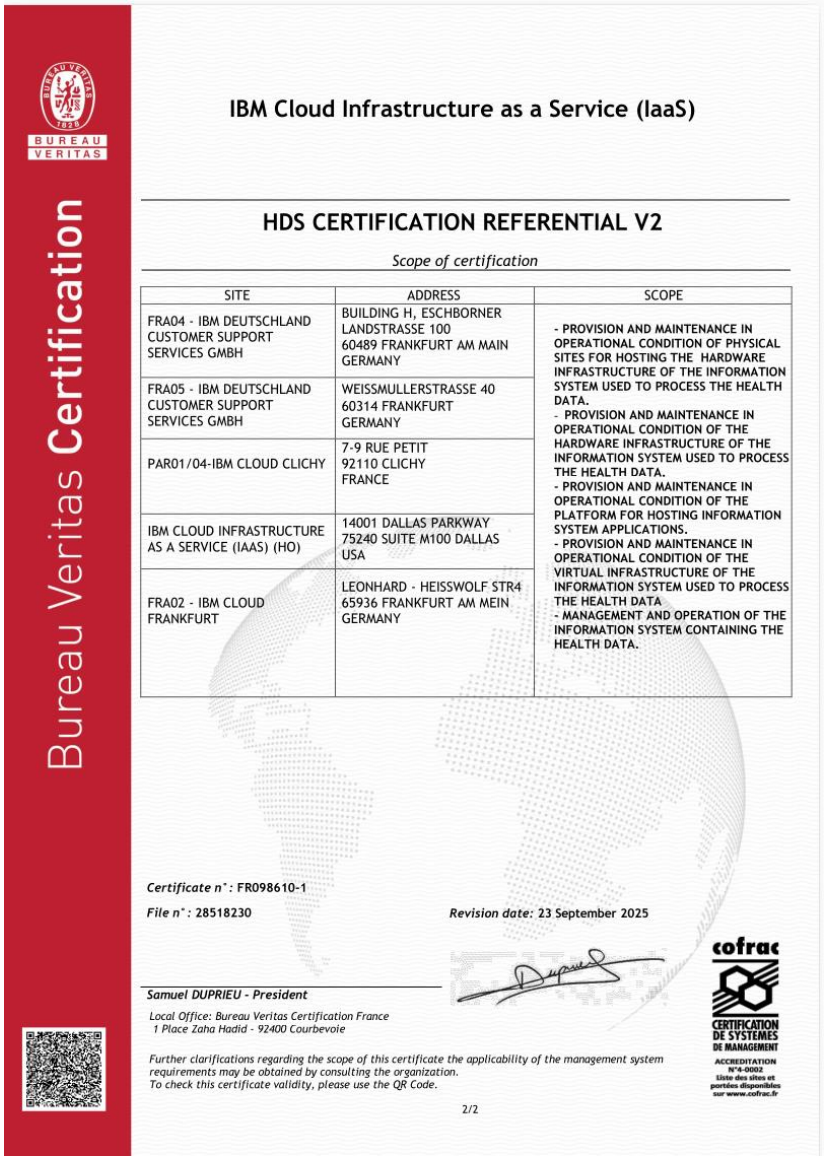
Local Office: Bureau Veritas Certification France
1 Place Zaha Hadid - 92400 Courbevoie

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