Service Level Agreement

Reference	SLA-001
Version	2.1
Date	June 2026
Scope	Rhaegal Production Environment

1. General presentation

This Service Level Agreement describes the Service Level commitments that Rhaegal makes to Paying Users of the Services. It may be revised from time to time.

2. System availability

Rhaegal will take appropriate redundancy, monitoring, and management measures for the Services to ensure optimal availability of the Services outside of scheduled maintenance windows.
The Services are considered unavailable when authentication is not possible via SSO or at least one key feature of the Services is not accessible
Key features are defined as follows: site structure (1 career site, up to 8 content pages, unlimited blocks per page, customizable menu and footer), branding and identity (favicon, font choice, custom URL, logos), content blocks (standard blocks, Code block, Container block), multilingual and multi-brand capabilities-(unlimited languages, multi-brand configuration-), ATS integrations (ATS Connect with SmartRecruiters, automatic import of ads, Job Ads, Job Alerts), conversion features (customization of job descriptions and calls-to-action), candidate experience (filters, advanced search, geolocation of offers) as well as the environments made available (production and sandbox).
Annual availability of the Services:

- 365 days a year,
- 24 hours a day,
- 99% system availability.

3. Service levels

3.1 Technical Support

This document defines the help desk workflow (ITSM) and service level agreement (SLA) metrics. The triggering of the contractual deadlines takes effect from the opening of an incident ticket (TI) by the Client on the Jira Service Management portal.

Technical support is operational on working days, Monday to Friday from 09:00 to 18:00 (CET).
On-call duty outside working hours
Outside the working hours applicable in France, Rhaegal's support team is on call at all times. This on-call duty covers all non-working days, weekends and public holidays in the geographical area concerned. In the event of an SEV 1 incident (total unavailability of the service or critical malfunction blocking the Client's activity), a notification is sent to the designated on-call person by email: support+astreinte@rhaegal.com . Upon receipt of the notification, the on-call person undertakes to acknowledge receipt and initiate coverage within the GTI period applicable to this level of severity. This organization guarantees continuity of coverage without interruption, regardless of the Customer's time zone.
The support portal is the only valid escalation channel for opening a trouble ticket (TI).

Notice: Off-portal solicitations (direct emails, instant messaging) are not tracked by the ticketing tool and do not trigger SLA counters.

3.2. Processing Workflow and Technical Qualification

Input: The customer declares the incident on the Jira Portal and assigns an initial severity when the ticket is opened. This severity immediately triggers contractual deadlines (GTI and TTRes).
Qualification (Triage): The Rhaegal support team performs a technical analysis to confirm the reproducibility and impact on critical components. The final classification of the ticket is determined exclusively by our engineers in order to align the technical priority with the contractual matrix In case of disagreement, the customer will be able to request an escalation of the ticket which will then be monitored by the support manager, who will make the final decision after communicating with the customer.
Output: The deployment of a patch (hotfix) or, temporarily, a workaround to restore the nominal service. Implementing a workaround does not change the severity classification of the incident. The resolution timer (TTRes) remains active until the final fix is deployed.

3.3. Escalation Matrix and Metrics (SLA)

In accordance with ITIL practices, two separate metrics apply from the time the ticket is created on the Support Portal:
First response time (GTI, Intervention Time Guarantee): the time elapsed between the creation of the ticket by the Customer and the first response from support. This stopwatch cannot be suspended or interrupted.
Resolution time (GTR, Resolution Time Guarantee): the time elapsed between the creation of the ticket and the restoration of the service. This timer can only be suspended during waiting periods attributable to the Customer (status 'Customer Waiting' in the Support Portal), with timestamp. It resumes upon receipt of the requested item.
The commitments by level of severity are as follows:

Incident Level (SEV)	Impact Criteria (Technical Definition)	TTR (Answer)	TTRes (Resolution)
SEV 1 - Major functionalities	Critical Failure: Crash of the Services, total inaccessibility of the tenant (total downtime).	< 1 hour	< 8 hours
SEV 2 - Minor functionalities	Service Degradation: Application up, but failure to execute on major/critical application features.	< 3 hours	< 3 working days
SEV 3 - Key features	Minor Bug: Nominal application, isolated failure on minor features that do not impact the main workflow.	< 6 hours	< 3 working weeks

Note: a break in the API connection with SmartRecruiters is classified as SEV 2 (the solution remains accessible, only the SR data flow is interrupted).

3.4. Prerequisites for Technical Investigation

To avoid a "Waiting for Customer" ticket status (pausing the SLA timer), the request payload must include the following artifacts:

- STR (Steps to Reproduce): The exact path to reproduce the anomaly.
- Environment & Context: Tenant ID, browser, OS version.
- Technical artifacts: Captures of failed network requests (. HAR), console stack traces (HTTP 4xx/5xx errors), or relevant log extracts.

3.5.Downtime Plan

If the application is unavailable with data loss, the data will be restored from a backup. Data is backed up on an hourly, daily, weekly, and monthly basis. The server, application, and data recovery time is less than 8 hours.

3.6 Database Backup Policy Frequency and Retention

Frequency	All	Retention period	Snapshot time
Schedule	6 hours	7 days	08:50 UTC
Daily	N/A	7 days	08:50 UTC
Weekly	Saturday	4 weeks	08:50 UTC
Monthly	Last day of the month	12 months	08:50 UTC

Rhaegal performs a minimum of one full database restore test per year, to validate backup integrity and compliance with restore time commitments.

4.Updates

Rhaegal updates its platform frequently to deliver new features and resolve issues quickly. Release notes and resources for new features are posted on our doc.rhaegal.com Documentation.
Common deployments, defined as patches and minor evolutions, are carried out in hot deployment mode and do not require any service interruption. Major updates, understood as evolutions introducing structural changes impacting the operation of the Services or infrastructure migrations, are made available in advance in a test environment for validation by the Customer before their deployment in production (available at From the fourth quarter of 2026) When a major update requires a service interruption, the service -will be subject to a maintenance window in accordance with the following provisions-.
Scheduled maintenance windows are open on weekends or outside of weekday business hours. They are always notified to the Client at least 24 hours in advance.
Rhaegal can also open a Maintenance Window within short periods of time in the event of a security breach being detected or a Bug Sev1 requiring a service interruption.

5. Vulnerability Management

Rhaegal undertakes to correct the vulnerabilities identified on the Services within the following timeframes, from the detection or publication of the publisher patch:

Level (CVSS)	Correction time
Review (≥ 9.0)	Mitigation within 72 hours, final fix within 15 calendar days
High (7.0 to 8.9)	30 calendar days
Average (4.0 to 6.9)	90 calendar days

Bass (< 4.0)	180 calendar days

Any patch is validated in a pre-production environment before being deployed to production.
In the event of a critical vulnerability affecting the Client's environment, the Client will be notified by email within 24 hours. Lower-level fixes can be found on the public changelog Rhaegal: https://feedback.rhaegal.com/changelog

6. Security Incident Management

In the event of a security incident affecting the Customer's environment

Personal data breach: notification to the Client within 48 hours (in accordance with the General Data Protection Regulation).
Major security incident (confirmed intrusion, data compromise): notification to the Client within 24 hours.
Minor incident (attempt blocked, alert with no impact observed): information in the periodic monitoring report.
During an ongoing major incident, Rhaegal provides updates to the Customer every 4 hours until resolved.
For any major security incident, Rhaegal provides a post-mortem report within 10 working days including: chronology of the incident, root cause identified, corrective measures applied, preventive actions taken.
These obligations cover the Arago Easy Attract infrastructure and application (AWS hosting, database, application layer, SOC monitoring). Third-party services used (Brevo, CM.com) are covered to the extent that Rhaegal is aware of them.

7.Security audits

Rhaegal carries out at least one penetration test (pentest) per year on the Arago Easy Attract infrastructure and application, conducted by a qualified third-party service provider. The summary report shall be communicated to the Client within 30 days of its receipt by Rhaegal.

8.Security infrastructure

Rhaegal undertakes, in its capacity as a Data Processor, to maintain the following security measures to protect the Client's data from unauthorized use or access:
Our Security Infrastructure includes intrusion detection services, security monitoring, Restricted Physical Access, Restricted Network Access, Encrypted Data Access, Redundant Firewalls, Isolated Public/Private LANs, Isolated NAS and SAN Access, and real-time antivirus.
Security monitoring is provided continuously (24/7) by an outsourced SOC (Security Operations Center), including monitoring of network flows, application logs and security alerts (intrusion detection, traffic anomalies, unauthorized access attempts).
In addition, only authorized individuals and workstations can update critical system elements such as firewall rules, settings, recovery procedures, and backup procedures.
The system monitors and logs all major components, including application services, system settings, load balancers, firewalls, and LAN traffic.
Any security enquiries can be directed to security@rhaegal.com.

9. Disaster Recovery Plan

Only the DB cluster is in a fault-tolerant configuration.
In the event of a total failure of the primary DB instance, operations are transferred to a secondary node where the full service can be restored.

9.1. Recovery period:

Failure of a single basic service: Instant
Breakdown of several basic services: 2 hours
Total failure of the main hosting site: 12 hours

10.Penalties

If Rhaegal fails to achieve the level of availability of the Services described in this document and upon written request of the Customer, it shall pay the Customer a penalty of 10% of the Subscription fees paid during the last twelve (12) months (calendar year) for each 1% below the availability of the Services committed.

Service penalties are deducted from the overall liability cap of 100% of the annual subscription fee. This ceiling constitutes the maximum cumulative amount of financial compensation due by Rhaegal under the Subscription Agreement. The extensions of service defined in section 11, applicable only in the event that the resolution deadlines are exceeded, constitute a separate mechanism and do not count against this ceiling.

11.Extension of service in case of resolution deadlines

11.1. Principle In addition to the availability commitments defined in Article 1, Rhaegal undertakes to comply with the resolution deadlines (TTRes) defined in Article 3 for each level of severity. If these deadlines are exceeded, the Client may benefit from a free extension of their subscription period in accordance with the terms and conditions defined in this article.

11.2. Extension grid: Extension rights are calculated per closed incident, based on the exceedance observed between the deadlines provided for in the resolution SLAs (TTRes) and the date of deployment of the final patch (excluding workaround):

Niveau	TTRes engagé	Dépassement constaté	Prorogation accordée
SEV 1	< 8 heures	0 à 4h	+ 5 jours calendaires
		4h à 12h	+ 10 jours calendaires
		> 12h	+ 15 jours calendaires
SEV 2	< 3 jours ouvrés	0 à 1 jour ouvré	+ 3 jours calendaires
		1 à 3 jours ouvrés	+ 7 jours calendaires
		> 3 jours ouvrés	+ 10 jours calendaires
SEV 3	< 3 semaines ouvrées	Tout dépassement	+ 2 jours calendaires

11.3. Ceiling Extensions granted under this Article shall be capped at 30 calendar days cumulated over any rolling 12-month period, regardless of severity.

11.4. Triggering conditions: The extension is granted subject to the following cumulative conditions:
The Client submitted the incident via the Jira Portal in accordance with Article 2 (Processing Workflow); 3.3 and 3.4 The incident is not attributable to a third party (excluding Rhaegal's authorized subcontractor) or to a planned maintenance window notified in accordance with the Updates article.

11.4. Application procedure: The extension is granted automatically. Rhaegal will examine the request and notify the Client of its decision within 10 working days of the closure of the ticket. The extension is applied to the next renewal date of the subscription, postponing it by the same amount.