BrynQ
Service level agreement

Preamble

SERVICE LEVEL AGREEMENT

This Service Level Agreement (“SLA”) describes how BrynQ provides and supports its Software-as-a-Service (“SaaS”) offering. The purpose of this SLA is to clearly define:

- the level of services provided (including availability, security, and support);
- the responsibilities of both BrynQ and the Customer;
- the procedural cooperation during onboarding, implementation, and daily use.

This SLA forms an integral part of, and is supplemental to, the main agreement between BrynQ and the Customer (the “Agreement”). Together, these documents define the legal and operational framework of the collaboration.

In the event of any conflict between this SLA and the Agreement, the Agreement shall prevail. The data processing agreement and BrynQ’s general terms and conditions remain fully applicable.

This SLA applies exclusively to the BrynQ service as hosted and managed by BrynQ. Custom developments, customer-specific configurations, and third-party systems fall outside the scope of this SLA unless explicitly stated otherwise.

About BrynQ

At BrynQ, we are more than just technology enthusiasts. We are problem solvers. With a strong foundation in HR and Payroll, we specialise in creating connectors and APIs that enable HR and payroll systems to communicate more effectively than ever before. We invite you to a new era of data management that empowers your organisation through intelligent, secure, and efficient data processing.

1. Definitions

- BrynQ Service: The complete BrynQ-managed cloud environment, including the integration engine, scheduler, dashboards, interface framework, logging, management portals, and supporting processes. The service functions as an integration and data platform between HR, payroll, and related systems.
- Incident: Any unplanned interruption or degradation of the service, including functional errors, performance issues, security incidents, or complete service unavailability. Incidents are classified by priority (P1–P4) to determine urgency and response times.
- Production Environment: The BrynQ-managed live environment in which the Customer processes production data.
- Uptime: The percentage of time per calendar month during which the Customer can log in and core BrynQ functionalities (such as integration runs and dashboards) are available, excluding the exceptions defined in this SLA.
- Business Hours: Monday to Thursday from 09:00 to 17:00 and Friday from 09:00 to 16:00 (CET/CEST), excluding Dutch public holidays.
- RPO (Recovery Point Objective): The maximum acceptable amount of data loss, expressed in time.
- RTO (Recovery Time Objective): The target time within which the BrynQ service is restored after a severe outage.

2. Scope of the SLA

This SLA applies to the use of the BrynQ service hosted in professional Dutch data centres that comply with recognised standards such as ISO 27001, NEN 7510, and SOC 1.

The SLA includes:

- hosting, infrastructure, platform software, and standard BrynQ functionality;
- standard logging, monitoring, and backup services;
- support and incident handling as described herein;
- the project approach and onboarding as described in Section 8.

The following are explicitly excluded from the scope unless agreed otherwise:

- customer-specific code, scripts, or dashboards developed by the Customer or third parties;
- configurations within source or target systems (including AFAS, SAP, Workday, and other SaaS or on-premise applications);
- the Customer's own network and identity infrastructure (such as VPNs, firewalls, and SSO configurations).
- Customer-specific configurations and customisations are backed up in accordance with BrynQ's backup policy but remain the Customer's responsibility with regard to content and changes.

3. Service description and architecture

The BrynQ service is a multi-tenant SaaS platform that collects, transforms, and distributes data from various source systems to dashboards, reports, and outbound interfaces. It acts as a central integration layer between HR, payroll, and related systems.

The platform uses a container-based architecture. Each Customer is assigned a logically separated customer container, with application, database, and scheduler components segregated. Separate development, test, acceptance, and production environments are maintained.

Customer data is logically segregated, including the use of dedicated databases per Customer. This ensures that Customer data is not accessible to other customers and that incidents within one customer container do not directly affect others.

This architecture is designed to maximise security, stability, and recoverability. Containers are reproducible, allowing rapid rebuilding or redeployment in the event of incidents.

4. Product development and releases

BrynQ continuously develops and improves the BrynQ service based on customer feedback, regulatory developments, and market and vendor changes.

New releases are deployed automatically without requiring customer action. Releases are designed to be backward compatible and generally do not impact availability. In exceptional cases, a short interruption may be required and will be communicated as planned maintenance.

Releases follow a defined secure software development lifecycle (SDLC), including:

- the use of standards such as OWASP and NIST;
- code reviews and automated testing;
- security and performance testing;
- controlled deployment to production.

Information about new functionality and significant changes is provided through release notes, the customer portal, and documentation platforms such as help.brynq.com or kb.brynq.com.

5. Availability, maintenance, and continuity

5.1 Uptime target

BrynQ targets a minimum monthly uptime of 99.9% for the Production Environment, corresponding to a maximum of approximately 43 minutes of downtime per calendar month.

Uptime is measured monthly using internal monitoring and an external monitoring page (e.g. uptime.brynq.com), focusing on actual availability of core functionality rather than server status alone.

The following are excluded from downtime calculations:

- announced planned maintenance within defined windows;
- outages caused by the Customer's systems or third parties;
- force majeure events as defined in the Agreement;
- major outages of external SaaS or cloud providers beyond BrynQ's control.

5.2 Planned maintenance

Maintenance is required to ensure security and stability. BrynQ aims to schedule maintenance in a way that minimises impact on availability.

If maintenance is expected to affect availability, BrynQ will normally notify Customers at least five (5) days in advance via the support or status page and/or email. Planned maintenance typically takes place outside business hours or during weekends, unless urgent circumstances require otherwise.

5.3 Monitoring and status communication

BrynQ continuously monitors availability and performance using APM tools and health checks.

In case of incidents, BrynQ communicates via:

- a public status page (e.g. status.brynq.com);
- support.brynq.com for incident registration and customer-specific

communication;
- optional email or portal notifications for subscribed customers.

5.4 Backup and recovery

BrynQ performs backups of customer data and relevant platform components in accordance with its internal backup policy, including:

- database backups at least every 15 minutes, retained for 91 days;
- monitoring of backup execution;
- periodic restore tests to verify data integrity and recovery times.

Container-based application components are not individually backed up but can be rapidly redeployed from the container infrastructure.

Upon request, BrynQ can perform point-in-time restores of customer databases within the retention period. Such restores are treated as additional services and may be charged separately.

5.5 Continuity (RPO and RTO)

BrynQ maintains a Business Continuity and Disaster Recovery plan for handling major incidents.

Target objectives:

- RPO: maximum 15 minutes;
- RTO: restoration of the production environment within one business day after a complete outage.

In the event of a major incident, BrynQ activates its recovery plan. Roles, escalation paths, and communication channels (including the status page and support portal) are defined as part of this plan.

5.6 Remedies in case of structural SLA breach

If BrynQ fails to meet the uptime target for three consecutive months or more than twice within a calendar year (excluding the exceptions defined in this SLA), the Parties shall enter into consultation to discuss:

- a remediation plan including concrete corrective measures;
- potential compensation, for example in the form of additional support services or agreed service credits.

Any compensation shall be provided only if explicitly agreed in the Agreement or in a separate written addendum.

6. Security and compliance

BrynQ delivers its services in an environment that meets high security and compliance standards, appropriate for processing HR and payroll data.

BrynQ and/or Salure are certified under ISO 27001 and maintain an ISAE 3402 Type II assurance report for relevant processes. Customers may request the latest certificates and reports.

Security measures include:

- Data centres and infrastructure:
  - ✓ hosting in Dutch data centres compliant with, among others, ISO 27001, NEN 7510 and SOC 1;
  - ✓ network protection through firewalls, IDS/IPS, DDoS protection and SSL/TLS encryption.
- Application and software security:
  - ✓ application of secure SDLC principles based on, among others, OWASP and NIST guidelines;
  - ✓ code reviews, automated testing and periodic penetration tests;
  - ✓ controlled release and patch management processes.
- Access security:
  - ✓ strong password policy and modern authentication methods;
  - ✓ role-based access control (RBAC) with segregated roles (for example admin, user, read-only);
  - ✓ logging of logins and relevant administrative actions;
  - ✓ strict management of accounts and access rights.
- Encryption and key management:
  - ✓ encrypted storage of sensitive data and access keys where appropriate;
  - ✓ management of encryption keys in accordance with internal policy guidelines;
  - ✓ restricted access to servers via secure management environments and password/key managers.
- Incident response:
  - ✓ a central process for security incidents, including classification, assessment and response actions;
  - ✓ notification and escalation procedures, taking into account applicable privacy and security legislation;

- ✓ communication with Customers regarding incidents that (may) impact their data or services.

7. Support and incident handling

7.1 Support channels

Incidents, service requests, and change requests must be submitted via support.brynq.com.

The knowledge base at kb.brynq.com provides documentation and FAQs. During business hours, BrynQ is also reachable by phone.

7.2 Support hours

Support is available:

- Monday–Thursday: 09:00–17:00 CET/CEST
- Friday: 09:00–16:00 CET/CEST

unless otherwise stated on the support website (for example during public holidays). Incident registration is available 24/7 via the support portal.

7.3 Priorities and response times

Incidents are classified in consultation with the Customer; BrynQ determines the final priority:

Priority	Response Time	Target Resolution Time
P1 - Critical	1 hour	1 business day workaround
P2 - High	4 business hours	10 business days
P3 - Normal	1 business day	3 business days
P4 - Request	Acknowledgement	n/a

What do we mean by reaction time and recovery time?

Response time means time to first substantive response; resolution time means time to a workable solution or workaround.

Examples of priorities:

- P1 - Example: all users cannot log in; interfaces don't run and there is no workaround.
- P2 – Example: a crucial interface partially fails, but a temporary workaround is possible.
- P3 – Example: Low-impact error messages, user queries, reporting issues.
- P4 – Example: feature requests, optimizations and non-critical changes.

7.4 Additional out-of-hours support

Paid out-of-hours support (e.g. for go-lives or critical payroll runs) can be provided upon request, subject to availability and prior written confirmation of scope and costs.

The Customer should preferably request this at least 10 working days in advance.

8. Project approach and onboarding

8.1 Roadmap and phases

Implementations and major changes follow the BrynQ projects & onboarding roadmap (onboarding.brynq.com) en/of de CustomerHub, consisting of five phases:

- Preparation
- Setup
- Implementation
- Testing & Go-Live
- Support & Handover

Within these phases, specific steps are defined, including but not limited to Selection, Onboarding, Intake, Monday board setup, Scenario template, Technical testing, Acceptance testing, Approve setup, Go-live, and Handover to support.

- ✓ For each step, the following is defined:
- ✓ the activities performed by BrynQ;
- ✓ the tasks and decision points required from the Customer;
- ✓ the knowledge required on the Customer's side;
- ✓ the consequences if Customer tasks are not performed or not performed in a timely manner.

This structured approach ensures predictability of progress and prevents unnecessary delays caused by unclear scope or missing information.

8.2 Project management and tools

BrynQ uses a project board (for example in Monday.com) as the central tool for:

- planning and progress tracking (including timeline views);
- assignment of tasks and responsibilities;
- documentation of decisions and agreements.

For projects up to a value of EUR 7,500, no project management is provided. In such cases, the Customer manages the project independently via the Monday project board and coordinates directly with BrynQ consultants. One or more intake sessions may be scheduled where necessary to ensure a proper start.

Projects with a value exceeding EUR 7,500 are actively managed by BrynQ. A standard 15% project management fee applies to ensure proper planning, risk management, dependency management, and communication. Project management fees are always charged.

Premium Support may be requested for any project, regardless of size.

E-mail will be replaced by communication via the project board, so that information remains central, up-to-date and transferable.

8.3 Definition of Done and handover to support

A project is considered completed when:

- the agreed interfaces and/or integrations have been deployed to production (Go-live);
- the Customer has formally approved the configuration (Approve setup);
- a formal handover to support has taken place (Handover to support).

From that moment onwards, the provisions of this SLA relating to support, incident handling, and changes apply in full. This clear Definition of Done prevents projects from continuing unnecessarily and protects both BrynQ and the Customer against scope creep.

9. Customer responsibilities

9.1 General cooperation

The Customer shall provide all reasonable cooperation necessary for the timely and proper execution of projects and support services, including but not limited to:

- the availability of authorised and knowledgeable staff (HR, payroll, IT, process owners);
- timely decision-making and formal approvals;
- the provision of accurate, complete, and timely information and test data.

9.2 Specific customer responsibilities within the roadmap

The Customer is, among other things, responsible for:

- Preparation and onboarding
  - ✓ providing contact details and system information;
  - ✓ supplying a high-level scope and integration requirements;
  - ✓ inviting relevant colleagues to the project board and portals.

- Systems and data
  - ✓ configuring and authorising source and target systems (APIs, SFTP, service accounts);
  - ✓ providing test and acceptance environments;
  - ✓ supplying representative and complete test data;
  - ✓ providing process and payroll documentation required for correct configuration.

- Scope, scenarios, and testing
  - ✓ completing scenario templates (data flows, business rules, exceptions);
  - ✓ reviewing and approving proposed scenarios (Scenario approval);
  - ✓ performing acceptance testing and formally approving the setup (Acceptance testing & Approve setup).

9.3 Non-compliance with customer responsibilities

If the Customer fails to perform the above responsibilities, or does not perform them in a timely manner, this may result in:

- delays to project or delivery timelines;
- additional work and rescheduling by BrynQ;
- limitations in BrynQ's ability to resolve incidents effectively.

In such cases, BrynQ is entitled to:

- adjust delivery and completion timelines;
- charge additional costs at the agreed hourly rates;
- temporarily suspend a project until the required input has been provided.

Delays resulting from failure to meet customer responsibilities shall not be considered a breach of BrynQ's obligations.

9.4 Required customer environments and test data

In order to proceed from the design phase to the development phase, BrynQ requires the timely availability of the following customer environments, including representative test data:

1. Test environment – source system (HCM)
   A non-production environment of the Customer's HCM system, configured in line with the intended production setup and containing representative test data.
2. Test environment – target system (local payroll)
   A non-production environment of the Customer's local payroll system, suitable for receiving, processing, and validating test integrations and payroll-related data.
3. Production environment – source system (HCM)
   Access to the production HCM environment, or confirmation that such access will be available prior to go-live, including the required authorisations, API endpoints, and technical details.
4. Production environment – target system (local payroll)
   Access to the production payroll environment, or confirmation that

such access will be available prior to go-live, including all necessary technical and functional permissions.

The Customer is responsible for ensuring that these environments:

- are available in a timely manner;
- are sufficiently stable for development and testing purposes;
- contain complete and representative test data that accurately reflects real-life HR and payroll processes.

If one or more of the required environments or datasets are not available, not available on time, or not fit for purpose, BrynQ shall be entitled to:

- suspend or postpone the development phase;
- adjust planning and delivery timelines accordingly;
- charge additional costs for rescheduling, waiting time, or required rework, where applicable.

Delays resulting from the absence or inadequacy of the required customer environments or test data shall not be considered a breach of BrynQ's obligations.

10. Changes to the service

BrynQ may make technical and functional changes to the BrynQ service in order to:

1. improve the service;
2. safeguard security and continuity;
3. comply with applicable laws and regulations.

Changes that are reasonably expected to have a material impact on functionality or integrations will, where practicable, be communicated at least five (5) days in advance via the customer portal and/or release notes.

If a change is reasonably expected to negatively impact critical Customer processes, the Parties shall enter into timely consultation regarding mitigating measures.

11. Reporting, audits, and information provision

BrynQ makes relevant assurance documentation available upon request, such as:

- ✓ the most recent ISO 27001 certificate (including scope);
- ✓ the current ISAE 3402 Type II report;
- ✓ summaries of penetration testing and security assessments in the form of a Third Party Memorandum.

Upon request, BrynQ will also provide additional information regarding:

- ✓ security measures;
- ✓ incidents affecting the Customer;
- ✓ the status of backups and recovery tests.

Any audits conducted by or on behalf of the Customer shall be performed in accordance with the terms set out in the Agreement, including notice periods, confidentiality requirements, and cost allocation.

12. Term, evaluation, and amendments to the SLA

This SLA enters into force on the effective date of the Agreement and shall terminate automatically upon termination of the Agreement.

BrynQ may amend this SLA if:

- ✓ required due to changes in laws or regulations;
- ✓ necessary to improve security or continuity;
- ✓ BrynQ modifies its services portfolio.

Any amendments will be communicated in a timely manner. BrynQ shall not materially reduce the service levels without prior consultation with the Customer.

The Parties shall periodically evaluate this SLA (for example on an annual basis) and amend it where necessary by mutual agreement.