



BrynQ
**Service level
agreement**

Introductie

SERVICE LEVEL AGREEMENT

Deze Service Level Agreement (“SLA”) beschrijft de wijze waarop BrynQ de SaaS-dienst levert en ondersteunt. Het doel is om voor beide partijen helderheid te scheppen over:

- ↳ -het niveau van dienstverlening (zoals beschikbaarheid, beveiliging en support);
- ↳ -de verantwoordelijkheden van zowel BrynQ als de Klant;
- ↳ de procesmatige samenwerking tijdens onboarding, implementatie en het dagelijks gebruik.

De SLA vormt geen losstaand document, maar is een aanvulling op de Overeenkomst. Het geheel bepaalt het juridische en operationele kader van de samenwerking.

Bij strijdigheid tussen de SLA en de Overeenkomst prevaleert de Overeenkomst. De verwerkersovereenkomst en de algemene voorwaarden van BrynQ blijven onverkort van toepassing.

Deze SLA geldt uitsluitend voor de BrynQ-dienst zoals gehost en beheerd door BrynQ. Maatwerk, klantconfiguraties en systemen van derden vallen alleen onder deze SLA waar dat expliciet is bepaald.

Over BrynQ

Bij BrynQ zijn we niet alleen techfanaten. We zijn probleemoplossers. Met een sterke basis in HR & Payroll zijn we gespecialiseerd in het creëren van connectoren en API's die uw HR- en salarisadministratiesystemen laten communiceren als nooit tevoren. We nodigen u uit voor een nieuw tijdperk van gegevensbeheer dat uw bedrijf versterkt met slimme, veilige en efficiënte gegevensverwerking.

1. Definities

- BrynQ-dienst: de volledige door BrynQ beheerde cloudomgeving inclusief integratie-engine, scheduler, dashboards, interface-framework, logging, beheerportalen en ondersteunende processen. De dienst fungeert als integratie- en dataplatform tussen HR-, payroll- en aanverwante systemen.
- Incident: elke onverwachte verstoring van de dienstverlening, waaronder functionele fouten, performanceproblemen, beveiligingsincidenten en totale uitval. Incidenten worden geclassificeerd op basis van prioriteit (P1–P4) zodat duidelijk is welke urgentie en responstijd gelden.
- Productieomgeving: de door BrynQ beheerde live-omgeving waarin de Klant productiegegevens verwerkt.
- Uptime: de tijd waarin de Klant kan inloggen én de kernfunctionaliteiten van de BrynQ-dienst (zoals integratieruns en dashboards) beschikbaar zijn, uitgedrukt als percentage van een kalendermaand, exclusief de in deze SLA genoemde uitzonderingen.
- Business hours: maandag t/m donderdag 09:00–17:00 uur en vrijdag 09:00–16:00 uur (CET/CEST), exclusief Nederlandse feestdagen.
RPO (Recovery Point Objective): de maximaal acceptabele hoeveelheid dataverlies, uitgedrukt in tijd.
RTO (Recovery Time Objective): de streeftijd waarbinnen de BrynQ-dienst na ernstige uitval weer beschikbaar is.

2. Scope van de SLA

De SLA is van toepassing op het gebruik van de BrynQ-dienst, gehost in professionele Nederlandse datacenters die voldoen aan relevante normen zoals ISO 27001, NEN 7510 en SOC 1.

De SLA omvat in ieder geval:

- ↳ de hosting, infrastructuur, platformsoftware en standaardfunctionaliteit van BrynQ;
- ↳ standaard logging, monitoring en back-up;
- ↳ support- en incidentafhandeling zoals beschreven in dit document;
- ↳ de projectaanpak en onboarding zoals beschreven in artikel 8.
- ↳ Buiten scope vallen, tenzij expliciet anders overeengekomen:
- ↳ klant-specifieke code, scripts en dashboards die door de Klant of derde partijen zijn ontwikkeld;
- ↳ configuraties in bronsystemen of doelsystemen (waaronder AFAS, SAP, Workday en overige SaaS- of on-premises applicaties);
- ↳ netwerk- en identity-infrastructuur van de Klant (zoals VPN, firewalls, SSO-configuraties).
- ↳ Klant-specifieke configuraties en maatwerk worden wel geback-upt volgens het back-upbeleid, maar vallen primair onder verantwoordelijkheid van de Klant voor wat betreft inhoud en wijzigingen.

3. Dienstbeschrijving en architectuur

De BrynQ-dienst is een multi-tenant SaaS-platform dat gegevens uit verschillende bronsystemen verzamelt, transformeert en ontsluit naar dashboards, rapportages en interfaces. De dienst vervult een centrale rol tussen HR-, payroll- en aanverwante systemen.

De platformarchitectuur is container-gebaseerd. Per Klant wordt in beginsel een eigen set containers gebruikt (customer-container), waarbij applicatie, database en scheduler logisch gescheiden zijn. Daarnaast bestaan er gescheiden ontwikkel-, test-, acceptatie- en productieomgevingen.

Klantdata wordt logisch gescheiden, onder andere via dedicated databases per Klant en container-isolatie. Dit betekent dat data van verschillende Klanten niet toegankelijk is voor andere Klanten en dat incidenten binnen één klantcontainer niet rechtstreeks de omgevingen van andere Klanten raken.

Deze architectuur is gekozen om veiligheid, stabiliteit en herstelbaarheid te verhogen. Containers zijn reproduceerbaar, waardoor BrynQ bij incidenten een omgeving snel kan herbouwen of opnieuw kan uitrollen.

4. Productontwikkeling en releases

BrynQ ontwikkelt de BrynQ-dienst continu door op basis van klantwensen, wettelijke/regulatorische ontwikkelingen en markt- en leveranciersontwikkelingen.

Nieuwe releases worden standaard uitgerold zonder dat de Klant actie hoeft te ondernemen. Releases zijn erop gericht om backwards compatible te zijn en hebben in beginsel geen impact op de beschikbaarheid. In uitzonderlijke gevallen kan een korte onderbreking nodig zijn, die dan wordt aangekondigd als gepland onderhoud.

Releases volgen een vastgelegd ontwikkel- en releaseproces (secure SDLC), met onder andere:

- ↳ gebruik van richtlijnen zoals OWASP en NIST;
- ↳ code reviews en automatische tests;
- ↳ beveiligings- en performancetests;
- ↳ gecontroleerde uitrol naar productie.

Informatie over nieuwe functionaliteit en belangrijke wijzigingen wordt via releasenotes, de customer portal en/of documentatieportalen (zoals help.brynq.com of kb.brynq.com) beschikbaar gesteld.

5. Beschikbaarheid, onderhoud en continuïteit

5.1 Uptime-doelstelling

BrynQ streeft naar een minimale maandelijkse uptime van 99,9% voor de Productieomgeving. Dit betekent dat de dienst per kalendermaand gemiddeld maximaal circa 43 minuten niet beschikbaar mag zijn.

Uptime wordt gemeten per kalendermaand op basis van interne monitoring en een externe monitoringpagina (zoals uptime.brynq.com). Hiermee wordt niet alleen gekeken naar serverstatus, maar naar daadwerkelijke beschikbaarheid van de kernfunctionaliteit.

De volgende situaties tellen niet mee als downtime:

- ↳ aangekondigd gepland onderhoud binnen de in deze SLA vastgelegde vensters;
- ↳ storingen die aantoonbaar zijn veroorzaakt door of in systemen/netwerken van de Klant of derden;
- ↳ omstandigheden die onder de in de Overeenkomst omschreven overmacht (force majeure) vallen;
- ↳ ernstige storingen in externe SaaS- of cloudproviders die buiten de invloedssfeer van BrynQ vallen.

5.2 Gepland onderhoud

Onderhoud is noodzakelijk om beveiliging en stabiliteit te waarborgen. BrynQ plant onderhoud bij voorkeur zo dat de beschikbaarheid niet wordt beïnvloed.

Wanneer onderhoud naar verwachting invloed heeft op de beschikbaarheid, communiceert BrynQ dit in beginsel minimaal 5 dagen vooraf via de support- of statuspagina en/of per e-mail. Klanten hebben zo de mogelijkheid om interne stakeholders te informeren.

Gepland onderhoud vindt normaliter plaats buiten kantooruren (tussen 17:00 en 08:00 uur CET/CEST) of in het weekend, tenzij dringende redenen anders vereisen.

5.3 Monitoring en statuscommunicatie

BrynQ monitort de beschikbaarheid en performance van de BrynQ-dienst continu via APM-tools en health-checks.

Bij storingen communiceert BrynQ via:

- ↪ een statuspagina (bijvoorbeeld status.brynq.com) voor actuele meldingen;
- ↪ support.brynq.com voor incidentregistratie en individuele communicatie;
- ↪ optioneel e-mail- of portaal meldingen voor Klanten die zich daarop hebben geabonneerd.

5.4 Back-up en herstel

BrynQ maakt back-ups van klantdata en relevante platformcomponenten volgens het interne back-upbeleid. Kernpunten:

- ↪ databaseback-ups worden minimaal elke 15 minuten gemaakt en gedurende 91 dagen bewaard;
- ↪ er vindt monitoring plaats op de succesvolle uitvoering van back-up taken;
- ↪ periodiek worden hersteltests uitgevoerd om te controleren of data tijdig en correct kan worden teruggezet.

Container-gebaseerde applicatiecomponenten worden in principe niet individueel geback-upt, maar kunnen snel opnieuw worden uitgerold vanuit de containerinfrastructuur.

Op verzoek van de Klant kan BrynQ een point-in-time herstel uitvoeren van de Klantdatabase naar een eerdere back-up binnen de retentieperiode. Dergelijk herstel wordt als maatwerk uitgevoerd en kan afzonderlijk in rekening worden gebracht.

Back-ups worden opgeslagen in beveiligde omgevingen die voldoen aan dezelfde beveiligingsstandaarden als de Productieomgeving.

5.5 Continuïteit (RPO en RTO)

BrynQ onderhoudt een Business Continuity en Disaster Recovery-plan dat beschrijft hoe wordt gehandeld bij ernstige verstoringen.

BrynQ hanteert als doelstellingen:

- ↳ RPO: maximaal 15 minuten, aansluitend bij het back-upinterval;
- ↳ RTO: bij volledige uitval van de Productieomgeving is de doelstelling om de dienst binnen 1 werkdag weer beschikbaar te hebben.

Bij een groot incident activeert BrynQ het recovery-plan. Rollen, escalatielijnen en communicatiekanalen (waaronder statuspagina en supportportaal) zijn daarin vastgelegd.

5.6 Remedies bij structurele SLA-schending

Indien BrynQ de uptime-doelstelling gedurende drie opeenvolgende maanden of meer dan twee keer per jaar niet haalt (buiten de genoemde uitzonderingen), treden Partijen in overleg over:

- ↳ een verbeterplan met concrete maatregelen;
- ↳ eventuele compensatie, bijvoorbeeld in de vorm van extra ondersteuning of overeengekomen service-credits.

Compensatie worden uitsluitend verstrekt indien dit expliciet in de Overeenkomst of een afzonderlijke bijlage is vastgelegd.

6. Beveiliging en compliance

BrynQ levert de BrynQ-dienst in een omgeving die aantoonbaar voldoet aan hoge beveiligings- en compliance-eisen. Dit is essentieel omdat de dienst veelal persoonsgegevens en HR-/payrolldata verwerkt.

BrynQ en/of Salure zijn gecertificeerd conform ISO 27001 en beschikken over een ISAE 3402 Type II-verklaring voor relevante processen. Klanten kunnen op verzoek de meest recente certificaten en rapportages inzien.

↳ Datacenters en infrastructuur:

- ✓ hosting in Nederlandse datacenters met onder meer ISO 27001, NEN 7510 en SOC 1;
- ✓ netwerkbescherming door firewalls, IDS/IPS, DDOS-bescherming en SSL/TLS-versleuteling.

↳ Applicatie- en softwarebeveiliging:

- ✓ toepassing van secure SDLC-principes op basis van o.a. OWASP- en NIST-richtlijnen;
- ✓ code reviews, geautomatiseerde tests en periodieke pentests;
- ✓ gecontroleerde release- en patchprocessen.

↳ Toegangsbeveiliging:

- ✓ sterke wachtwoordpolicy en moderne authenticatiemethoden;
- ✓ role-based access control (RBAC) met gescheiden rollen (bijvoorbeeld admin, user, read-only);
- ✓ logging van logins en relevante beheeracties;
- ✓ strikt beheer van accounts en rechten.

↳ Versleuteling en sleutelbeheer:

- ✓ versleutelde opslag van gevoelige gegevens en toegangssleutels waar passend;
- ✓ beheer van encryptiesleutels volgens interne beleidsrichtlijnen;
- ✓ beperkte toegang tot servers via beveiligde beheeromgevingen en password-/keymanagers.

↳ Incidentrespons:

- ✓ centraal proces voor beveiligingsincidenten, inclusief classificatie, beoordeling en acties;
- ✓ meld- en escalatieprocedures, rekening houdend met toepasselijke privacy- en beveiligingswetgeving;
- ✓ communicatie met Klanten over incidenten die (mogelijk) impact hebben op hun data of dienstverlening.

7. Support en incidentafhandeling

7.1 Supportkanalen

Incidenten, serviceverzoeken en wijzigingsverzoeken worden geregistreerd via support.brynq.com.

De Knowledge Base op kb.brynq.com bevat documentatie en antwoorden op veelgestelde vragen. Klanten worden aangemoedigd deze informatie te raadplegen bij gebruikersvragen, zodat support zich kan richten op incidenten en complexere vraagstukken.

Tijdens business hours is BrynQ telefonisch bereikbaar via het algemene supportnummer zoals vermeld op de supportsite.

7.2 Openingstijden en bereikbaarheid

Support is bereikbaar:

- maandag t/m donderdag: 09:00–17:00 (CET/CEST);
- vrijdag: 09:00–16:00 (CET/CEST);

tenzij anders vermeld op de supportsite (bijvoorbeeld rond feestdagen). Registratie van incidenten via het supportportaal is 24/7 mogelijk.

7.3 Prioriteiten en responstijden

Bij registratie van een incident wordt in overleg tussen Klant en BrynQ een prioriteit toegekend. BrynQ beslist welke prioriteit uiteindelijk wordt toegekend. We gebruiken dit kader:

Prioriteit	Reactietijd	Doel hersteltijd
P1 - Kritiek	1 uur	1 werkdag workaround
P2 - Hoog	4 business hours	10 werkdagen
P3 - Normaal	1 werkdag	3 werkdagen
P4 - Wens	Bevestiging	n.v.t.

Wat verstaan we onder reactietijd en hersteltijd?

Reactietijd betekent de periode tot de eerste inhoudelijke reactie door BrynQ en hersteltijd betreft de periode tot een werkbare oplossing of workaroud.

Voorbeelden van prioriteiten:

- ↳ P1 - Voorbeeld: alle gebruikers kunnen niet inloggen; interfaces draaien niet en er is geen workaroud.
- ↳ P2 - Voorbeeld: een cruciale interface faalt deels, maar een tijdelijke workaroud is mogelijk.
- ↳ P3 - Voorbeeld: foutmeldingen met beperkte impact, gebruikersvragen, rapportage-issues.
- ↳ P4 - Voorbeeld: feature requests, optimalisaties en niet-kritieke veranderingen.

7.4 Extra support buiten kantooruren

Op verzoek kan BrynQ (betaalde) ondersteuning leveren buiten business hours, bijvoorbeeld bij begeleide go-lives of kritieke payrollmomenten.

De Klant dient dit bij voorkeur minimaal 10 werkdagen vooraf aan te vragen. BrynQ bevestigt schriftelijk de beschikbaarheid, scope en kosten.

8. Projectaanpak en onboarding

8.1 Roadmap en fasering

Implementaties en grote wijzigingen worden uitgevoerd volgens de BrynQ projects & onboarding roadmap, zoals gepubliceerd via onboarding.brynq.com en/of de CustomerHub.

De roadmap kent vijf hoofd-fasen:

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

Binnen deze fasen zijn concrete stappen gedefinieerd, zoals Selectie, Onboarding, Intake, Monday board setup, Scenario template, Technical testing, Acceptance testing, Approve setup, Go-live en Handover to support.

Bij iedere stap is vastgelegd:

- ✓ welke activiteiten BrynQ uitvoert;
- ✓ welke klanttaken en -beslissingen noodzakelijk zijn;
- ✓ welke kennis aan klantzijde vereist is;
- ✓ welke gevolgen er zijn als klanttaken niet of niet tijdig worden uitgevoerd.

Deze gestructureerde aanpak maakt de voortgang voorspelbaar en voorkomt dat projecten onnodig uitlopen door onduidelijke scope of ontbrekende informatie.

8.2 Projectmanagement en tools

BrynQ gebruikt een projectboard (bijvoorbeeld in Monday.com) als centrale plek voor:

- ↳ planning en voortgang (inclusief timeline-weergaven);

- ↳ toewijzing van taken en verantwoordelijkheden;
- ↳ documentatie van beslissingen en afspraken.

Voor kleinere projecten (tot €7.500) wordt geen projectleiding ingezet. De klant beheert in dat geval zelf de voortgang via het toegewezen Monday-projectboard en stemt rechtstreeks af met de BrynQ-consultants. Eén of meerdere intake-sessies kunnen worden ingepland indien dat nodig is voor een correcte start.

Projecten met een waarde boven €7.500 worden actief gemanaged door BrynQ. Voor deze projecten wordt standaard 15% projectmanagement toegepast om planning, risico's, afhankelijkheden en communicatie te bewaken. Deze projectmanagementkosten worden altijd in rekening gebracht.

Indien gewenst kan voor elk project, ongeacht omvang, Premium Support worden afgenomen, voor aanvullende begeleiding, intensieve betrokkenheid of buiten-kantooruren ondersteuning.

E-mail wordt zoveel mogelijk vervangen door communicatie via het projectboard, zodat informatie centraal, actueel en overdraagbaar blijft.

8.3 Definition of Done en overdracht naar support

Een project wordt als afgerond beschouwd wanneer:

- ↳ de afgesproken interfaces/integraties in productie zijn gebracht (Go-live);
- ↳ de Klant de configuratie formeel heeft goedgekeurd (Approve setup);
- ↳ een overdracht aan support heeft plaatsgevonden (Handover to support).

Vanaf dat moment zijn de bepalingen over support, incidentafhandeling en wijzigingen in deze SLA volledig van toepassing. Deze duidelijke "Definition of Done" voorkomt dat projecten onnodig doorlopen en beschermt zowel BrynQ als de Klant tegen scope creep.

9. Verplichtingen van de Klant

9.1 Algemene medewerking

De Klant verleent alle redelijke medewerking die noodzakelijk is voor een tijdige en correcte uitvoering van projecten en support, waaronder:

- ↳ het beschikbaar stellen van bevoegde en inhoudelijk deskundige medewerkers (HR, payroll, IT, proces-eigenaren);
- ↳ tijdige besluitvorming en het geven van goedkeuringen;
- ↳ aanlevering van juiste en volledige informatie en testdata.

9.2 Specifieke klanttaken in de roadmap

De Klant is onder meer verantwoordelijk voor:

- ↳ Voorbereiding en onboarding
 - ✓ delen van contact- en systeeminformatie;
 - ✓ aanleveren van globale scope en integratiewensen;
 - ✓ uitnodigen van relevante collega's voor het projectboard en portalen.
- ↳ Systemen en data
 - ✓ inrichten en autoriseren van bron- en doelsystemen (API's, SFTP, serviceaccounts);
 - ✓ beschikbaar stellen van test- en acceptatieomgevingen;
 - ✓ aanleveren van representatieve en volledige testdata;
 - ✓ delen van proces- en payrolldocumentatie die nodig is voor correcte configuratie.
- ↳ Scope, scenario's en testen
 - ✓ invullen van scenario-templates (datastromen, businessregels, uitzonderingen);
 - ✓ beoordelen en goedkeuren van voorgestelde scenario's (Scenario approval);
 - ✓ uitvoeren van acceptatietesten en formeel akkoord geven op de opzet (Acceptance testing & Approve setup).

9.3 Gevolgen van niet-naleving klanttaken

Indien de Klant bovengenoemde taken niet of niet tijdig uitvoert, kan dit leiden tot:

- ↳ vertraging in project- of oplevertermijnen;
- ↳ extra werkzaamheden en herplanning bij BrynQ;
- ↳ beperkingen in de mogelijkheid om incidenten op te lossen.
- ↳ In die gevallen is BrynQ gerechtigd:
 - ↳ oplever- en doorlooptijden aan te passen;
 - ↳ meerwerk in rekening te brengen tegen de dan geldende uurtarieven;
 - ↳ een project tijdelijk te pauzeren totdat de benodigde input is geleverd.

Vertragingen als gevolg van het niet naleven van klantverplichtingen kwalificeren niet als tekortkoming van BrynQ.

9.4 Vereiste klantomgevingen en testdata

Om van de ontwerpfase (design) naar de ontwikkelfase (development) te kunnen overgaan, is BrynQ afhankelijk van de tijdige beschikbaarheid van de volgende klantomgevingen, inclusief representatieve testdata:

1. Testomgeving – bronsysteem (HCM)

Een niet-productieomgeving van het HCM-systeem van de Klant, ingericht conform de beoogde productie-inrichting en voorzien van representatieve testdata.

2. Testomgeving – doelsysteem (lokale payroll)

Een niet-productieomgeving van het lokale payrollstelsel van de Klant, geschikt voor het ontvangen, verwerken en valideren van testintegraties en payrollgegevens.

3. Productieomgeving – bronsysteem (HCM)

Toegang tot de productieomgeving van het HCM-systeem, dan wel een bevestiging dat deze toegang uiterlijk voorafgaand aan de go-live beschikbaar zal zijn, inclusief de benodigde autorisaties, API-endpoints en

technische gegevens.

4. Productieomgeving – doelsysteem (lokale payroll)

Toegang tot de productieomgeving van het lokale payrollstelsel, dan wel een bevestiging dat deze toegang uiterlijk voorafgaand aan de go-live beschikbaar zal zijn, inclusief alle noodzakelijke technische en functionele rechten.

De Klant is verantwoordelijk voor het waarborgen dat deze omgevingen:

- tijdig beschikbaar zijn;
- voldoende stabiel zijn voor ontwikkel- en testdoeleinden;
- beschikken over volledige en representatieve testdata die een realistische afspiegeling vormt van de daadwerkelijke HR- en payrollprocessen.

Indien één of meerdere van de vereiste omgevingen of datasets niet, niet tijdig of niet in voldoende mate beschikbaar zijn, is BrynQ gerechtigd om de ontwikkelfase op te schorten of uit te stellen; de planning en oplevertermijnen aan te passen; aanvullende kosten in rekening te brengen voor herplanning, wachttijd of noodzakelijk meerwerk. Vertragingen die voortvloeien uit het ontbreken of onvoldoende functioneren van deze klantomgevingen of testdata worden niet aangemerkt als een tekortkoming aan de zijde van BrynQ.

10. Wijzigingen in de dienst

BrynQ mag de BrynQ-dienst technisch en functioneel wijzigen om:

- ✓ de dienstverlening te verbeteren;
- ✓ beveiliging en continuïteit te waarborgen;
- ✓ te voldoen aan wet- en regelgeving.

Wijzigingen met significante impact op functionaliteit of integraties worden, waar redelijkerwijs mogelijk, minimaal 5 dagen vooraf aangekondigd via de customer portal en/of releasenotes.

Indien een wijziging naar redelijke verwachting negatieve impact heeft op

kritieke processen van de Klant, treden Partijen tijdig in overleg over mitigerende maatregelen.

11. Rapportage, audits en informatieverstrekking

BrynQ stelt op verzoek relevante assurance-documentatie beschikbaar, zoals:

- ✓ het laatste ISO 27001-certificaat (inclusief scope);
- ✓ het actuele ISAE 3402 Type II-rapport;
- ✓ samenvattingen van penetratietesten en beveiligingsbeoordelingen in de vorm van een Third Party Memorandum.

Op verzoek verstrekt BrynQ aanvullende informatie over beveiligingsmaatregelen, incidenten die de Klant raken en de status van back-up en hersteltests.

Eventuele audits door of namens de Klant worden uitgevoerd conform de afspraken in de Overeenkomst (zoals aankondigingstermijn, vertrouwelijkheid en kostenverdeling).

12. Duur, evaluatie en wijziging van de SLA

Deze SLA treedt in werking op de ingangsdatum van de Overeenkomst en eindigt uiterlijk tegelijk met de Overeenkomst.

BrynQ kan de SLA wijzigen indien:

- ✓ dit noodzakelijk is vanwege wet- of regelgeving;
- ✓ dit noodzakelijk is om beveiliging of continuïteit te verbeteren;
- ✓ BrynQ haar dienstenportfolio aanpast.

Wijzigingen worden tijdig gecommuniceerd. BrynQ zal het serviceniveau niet wezenlijk verlagen zonder voorafgaand overleg met de Klant. Partijen evalueren deze SLA periodiek (bijvoorbeeld jaarlijks) en passen deze waar nodig in onderling overleg aan.