Service Level Agreement

(Template voor aanbesteding)

Dit template dient als bijlage bij het bestek. De specifieke details worden na gunning in overleg met de gegunde leverancier ingevuld. Van inschrijvers wordt verwacht dat zij deze onderwerpen standaard in hun SLA hebben uitgewerkt.

Documentgegevens

Veld	Waarde
Versie	*[Versienummer]*
Datum	*[Datum]*
Status	*[Concept/Definitief]*
Opdrachtgever	*[Naam organisatie]*
Leverancier	*[Naam leverancier]*

Documenthistorie

Tabel met versiegeschiedenis: datum, versie, omschrijving wijziging, auteur

1. Inleiding

1.1 Doel van de SLA

Beschrijf het doel van deze Service Level Agreement: het vastleggen van afspraken over kwaliteit, beschikbaarheid en ondersteuning van de geleverde diensten.

1.2 Partijen

Opdrachtgever	Leverancier
Rechtspersoon: *Adres:* *KvK-nummer:*	*Rechtspersoon:* *Adres:* *KvK-nummer:*

1.3 Diensten en applicaties

Opsomming van alle diensten en/of applicaties die onder deze SLA vallen, inclusief verwijzing naar de onderliggende overeenkomst(en).

1.4 Contactpersonen

Overzicht van contactpersonen aan beide zijden, inclusief: naam, functie, telefoonnummer, e-mailadres. Onderscheid maken tussen operationeel, tactisch en strategisch niveau.

1.5 Doelgroep

Voor wie is deze SLA bedoeld? Denk aan: IT-management, functioneel beheerders, applicatiebeheerders, eindgebruikers.

1.6 Geldigheidsduur

Startdatum en einddatum van de SLA. Koppeling met looptijd van de onderliggende overeenkomst. Voorwaarden voor verlenging.

1.7 Beheer van de SLA

Wie is verantwoordelijk voor het beheer? Hoe vaak wordt de SLA geëvalueerd? Procedure voor aanpassing van de SLA.

1.8 Relatie met andere documenten

Verwijzing naar gerelateerde documenten: hoofdovereenkomst, verwerkersovereenkomst, GIBIT-voorwaarden, beveiligingsbijlagen, exit-plan.

1.9 Definitielijst

Tabel met alle gebruikte begrippen en hun definities. Minimaal: SLA, Dienst, Incident, Probleem, Change, Workaround, Bug, Feature Request, SaaS, Beschikbaarheid, Servicewindow, Reactietijd, Oplostijd.

2. Scope en randvoorwaarden

2.1 Binnen scope

Expliciete opsomming van wat wel onder de SLA valt. Denk aan: toegang tot supportportaal, bug-registratie en afhandeling, technische ondersteuning, functionele ondersteuning, productupdates, security-informatie, beschikbaarheid SaaS-omgeving, koppelingen/integraties.

2.2 Buiten scope

Expliciete opsomming van wat niet onder de SLA valt. Denk aan: consultancy, procesadvies, maatwerk development, training, organisatie specifieke koppelingen, infrastructuur aan klantzijde.

2.3 Verantwoordelijkheden opdrachtgever

Welke zaken moet de opdrachtgever regelen? Denk aan: netwerkconnectiviteit, geschikte werkplekken/browsers, aanleveren correcte gegevens, tijdige melding van incidenten, beschikbaarheid van testcapaciteit.

2.4 Verantwoordelijkheden leverancier

Welke zaken moet de leverancier regelen? Denk aan: hosting, onderhoud, beveiliging, support, documentatie, updates.

3. Service Levels

3.1 Beschikbaarheid

3.1.1 Beschikbaarheidspercentage

Aspect	Afspraak
Beschikbaarheidspercentage	*[XX,X%] per [maand/kwartaal/jaar]*
Meetmethode	*[Hoe wordt gemeten?]*
Meetperiode	*[Maand/kwartaal/jaar]*

3.1.2 Service window applicatie

Tijden waarop de applicatie beschikbaar moet zijn. Onderscheid maken tussen normale beschikbaarheid en eventueel uitgebreide beschikbaarheid.

3.1.3 Onderhouds window

Tijdstippen waarop gepland onderhoud mag plaatsvinden (bijv. 's nachts). Aankondigingstermijn voor gepland onderhoud.

3.1.4 Uitsluitingen beschikbaarheid

Omstandigheden die niet meetellen voor het beschikbaarheidspercentage: gepland onderhoud, overmacht, storingen bij derden, etc.

3.2 Support

3.2.1 Service window support

Openingstijden van de helpdesk. Bereikbaarheid (telefoon, e-mail, portaal). Eventueel verschillende niveaus van support buiten kantooruren.

3.2.2 Prioriteitsniveaus

Definieer de prioriteitsniveaus met criteria. Bijvoorbeeld:

Prioriteit	Omschrijving	Criteria
Kritiek	*Volledige uitval dienst*	*[Criteria voor kritiek]*
Hoog	*Ernstige beperking*	*[Criteria voor hoog]*
Normaal	*Beperkte impact*	*[Criteria voor normaal]*
Laag	*Minimale impact*	*[Criteria voor laag]*

3.2.3 Reactie- en oplostijden

Prioriteit	Reactietijd	Workaround	Definitieve oplossing
Kritiek	*[tijd]*	*[tijd]*	*[tijd]*
Hoog	*[tijd]*	*[tijd]*	*[tijd]*
Normaal	*[tijd]*	*[tijd]*	*[tijd]*
Laag	*[tijd]*	*[tijd]*	*[tijd]*

Specificeer of tijden in klokuren of werkuren zijn, en wanneer de teller start (bijv. na ontvangstbevestiging).

3.2.4 Escalatieprocedure

Beschrijf de escalatieprocedure met: escalatieniveaus, tijdslijnen voor automatische escalatie, contactpersonen per niveau, wanneer mag worden geëscaleerd.

3.3 Performance

Afspraken over responstijden van de applicatie, maximale laadtijden, aantal gelijktijdige gebruikers dat ondersteund moet worden.

4. Wijzigingenbeheer

4.1 Soorten wijzigingen

Definieer de verschillende soorten wijzigingen: standaard releases, hotfixes, security patches, major updates, emergency changes.

4.2 Release-beleid

Frequentie van releases. Aankondigingstermijn. Beschikbaarheid van release notes. Mogelijkheid tot uitstel van updates.

4.3 Testomgeving

Beschikbaarheid van acceptatieomgeving. Voorwaarden voor testen. Wie is verantwoordelijk voor testen? Doorlooptijd tussen acceptatie en productie.

4.4 Emergency changes

Procedure voor spoedwijzigingen. Communicatie. Goedkeuring achteraf.

4.5 Feature requests

Hoe kunnen wensen worden ingediend? Hoe wordt geprioriteerd? Terugkoppeling over status.

5. Incident- en probleembeheer

5.1 Incidentproces

Beschrijf het volledige incidentproces: aanmelding, registratie, diagnose, oplossing, afsluiting. Wie doet wat? Hoe wordt de melder geïnformeerd?

5.2 Probleembeheer

Hoe worden terugkerende incidenten geïdentificeerd en structureel opgelost? Root cause analysis.

5.3 Omgaan met bugs

Definitie van een bug. Afhandeling van bugs. Wanneer workaround? Wanneer definitieve fix? Welke bugs krijgen voorrang?

5.4 Calamiteitenplan

Wat gebeurt er bij een calamiteit? Wie wordt geïnformeerd? Herstelplannen. Communicatieprotocol.

6. Beveiliging en compliance

6.1 Beveiligingsmaatregelen

Overzicht van getroffen beveiligingsmaatregelen: encryptie, toegangsbeheer, netwerkbeveiliging, applicatiebeveiliging, fysieke beveiliging.

6.2 Certificeringen

Welke certificeringen heeft de leverancier? ISO 27001, NEN 7510, SOC 2, etc. Geldigheid en beschikbaarheid van certificaten.

6.3 Audits

Frequentie van audits. Beschikbaarheid van auditrapporten. Recht op eigen audit door opdrachtgever.

6.4 Penetratietesten

Frequentie van pentesten. Beschikbaarheid van resultaten. Opvolging van bevindingen.

6.5 Beveiligingsincidenten

Hoe worden beveiligingsincidenten gemeld? Aan wie? Binnen welke termijn? Wie is verantwoordelijk voor melding aan toezichthouder?

6.6 Kwetsbaarheden

Hoe worden kwetsbaarheden afgehandeld? Responsible disclosure beleid. Doorlooptijd voor patches.

7. Gegevensbeheer

7.1 Datacenter

Locatie van datacenters (binnen EU/EER). Certificeringen van datacenter. Redundantie.

7.2 Back-up en restore

Aspect	Afspraak
Back-up frequentie	*[dagelijks/uurlijks/etc.]*
Retentieperiode	*[X dagen/maanden]*
Recovery Point Objective (RPO)	*[maximaal dataverlies]*
Recovery Time Objective (RTO)	*[maximale hersteltijd]*
Restore-procedure	*[wie, hoe, doorlooptijd]*
Back-up testen	*[frequentie tests]*

7.3 Bewaartermijnen

Bewaartermijn van gegevens tijdens contract. Bewaartermijn na beëindiging. Onderscheid tussen operationele data en logging/audit trails.

7.4 Data-export

Mogelijkheden voor export van data. Beschikbare formaten. API-toegang. Frequentie waarmee export mogelijk is.

7.5 Dataverwijdering

Procedure voor verwijdering van data na beëindiging. Certificering van verwijdering. Termijnen.

8. Governance en overleg

8.1 Overlegstructuur

Type overleg	Frequentie	Deelnemers	Onderwerpen
Operationeel	*[frequentie]*	*[rollen]*	*[agendapunten]*
Tactisch	*[frequentie]*	*[rollen]*	*[agendapunten]*
Strategisch	*[frequentie]*	*[rollen]*	*[agendapunten]*

8.2 Escalatiestructuur

Beschrijf de escalatieladder met contactpersonen aan beide zijden, van operationeel tot directieniveau. Wanneer wordt geëscaleerd? Door wie?

8.3 Rapportages

Rapportage	Frequentie	Inhoud	Levering
SLA-rapportage	*[frequentie]*	*[KPI's, prestaties]*	*[format, wijze]*
Incidentrapportage	*[frequentie]*	*[statistieken]*	*[format, wijze]*
Security-rapportage	*[frequentie]*	*[bevindingen]*	*[format, wijze]*

9. Financiële bepalingen

9.1 Bonus-malusregeling

Beschrijf de gevolgen van het niet halen van de afgesproken service levels:

KPI	Grenswaarde	Consequentie
Beschikbaarheid	*[percentage]*	*[korting/boete]*
Reactietijd kritiek	*[tijd]*	*[korting/boete]*
Oplostijd kritiek	*[tijd]*	*[korting/boete]*

Specificeer ook: maximale malus per periode, cumulatie van malus, eventuele bonus bij overtreffen targets.

9.2 Meerwerk

Welke werkzaamheden vallen buiten de standaard SLA en worden apart gefactureerd? Tarieven. Goedkeuringsprocedure.

10. Beëindiging en transitie

10.1 Exit-strategie

Hoofdlijnen van de exit-strategie. Verwijzing naar apart exit-plan (conform GIBIT).

10.2 Data-overdracht

In welke formaten wordt data aangeleverd? Op welke gegevensdragers? Binnen welke termijn? Kosten?

10.3 Ondersteuning bij transitie

Welke ondersteuning biedt de leverancier bij overgang naar een andere partij? Duur van ondersteuning. Tarieven.

10.4 Kennisoverdracht

Hoe wordt kennis overgedragen? Documentatie. Training. Beschikbaarheid van experts.

10.5 Continuïteit na beëindiging

Hoe lang blijft de dienst beschikbaar na opzegging? Hoe lang blijven gegevens beschikbaar? Procedure voor verlenging van deze periode indien nodig.

11. Ondertekening

Aldus overeengekomen en in tweevoud opgemaakt te [plaats], op [datum].

Opdrachtgever	Leverancier
_____ *Naam:* *Functie:* *Datum:*	_____ *Naam:* *Functie:* *Datum:*

Bijlagen

Bijlage A: Dienstencatalogus

Gedetailleerde beschrijving van alle diensten die onder de SLA vallen.

Bijlage B: Technische specificaties

Technische eisen aan infrastructuur, browsers, bandbreedte, etc.

Bijlage C: Contactpersonenlijst

Volledige lijst van contactpersonen met bereikbaarheidsgegevens.

Bijlage D: Escalatiematrix

Gedetailleerde escalatiestructuur met contactgegevens per niveau.

Bijlage E: Exit-plan

Uitgewerkt exit-plan conform GIBIT-voorwaarden.

Bijlage F: Verwerkersovereenkomst

Indien van toepassing: verwerkersovereenkomst conform AVG.