Aanbesteding IT-platform Data Safe House
Conformiteitenlijst

Non-functionele Eisen, SLA en Contractuele Afspraken

27-02-2026: Update na Nota's van inlichtingen

Introductie

Dit document beschrijft de uitgangspunten en randvoorwaarden voor de ontwikkeling, implementatie, het beheer en de doorontwikkeling van het IT-platform van Stichting Data Safe House (DSH). Het doel van dit document is om marktpartijen helder inzicht te geven in de kwaliteitsverwachtingen, de wijze waarop deze worden geborgd in de uitvoering en het beoogde contractuele kader, zonder onnodig oplossingen voor te schrijven.

Het document is opgebouwd uit drie samenhangende hoofdstukken:

1. **Non-functionele eisen**
   Dit hoofdstuk beschrijft de kwaliteitskenmerken en randvoorwaarden waaraan het IT-platform dient te voldoen. De non-functionele eisen zijn gebaseerd op ISO/IEC 25010:2023 en beschrijven aspecten zoals performance, betrouwbaarheid, beveiliging, onderhoudbaarheid en overdraagbaarheid. Enkele eisen zijn oplossingsneutraal geformuleerd en laten ruimte voor marktpartijen om met passende technische en organisatorische oplossingen te komen.

2. **Service Level Agreement (SLA)**
   In dit hoofdstuk worden de non-functionele kwaliteitsdoelen vertaald naar operationele serviceafspraken over onder andere beschikbaarheid, incidentafhandeling, beveiliging, monitoring en wijzigingsbeheer. De SLA maakt onderdeel uit van de overeenkomst en borgt de kwaliteit van de dienstverlening gedurende de looptijd. De opgenomen servicelevels zijn contractueel van aard.

3. **Overige contractuele afspraken (indicatief kader)**
   Dit hoofdstuk schetst het beoogde kader voor aanvullende contractuele afspraken tussen DSH en de opdrachtnemer, waaronder intellectueel eigendom, aansprakelijkheid, compliance, exit en overdraagbaarheid. De beschrijving is richtinggevend en informatief; de definitieve uitwerking vindt plaats in de conceptovereenkomst en de uiteindelijke contractstukken na gunning.

Met deze opzet beoogt DSH duidelijkheid te bieden over verwachtingen en uitgangspunten, terwijl tegelijkertijd voldoende ruimte blijft voor marktpartijen om hun expertise en oplossingsrichtingen in te brengen binnen een transparant en proportioneel aanbestedingsproces.

Inhoudsopgave

1. Non-functionele eisen

De onderstaande non-functionele eisen beschrijven de kwaliteitskenmerken en randvoorwaarden waaraan het IT-platform dient te voldoen. Deze eisen zijn gebaseerd op ISO/IEC 25010:2023.

Waar relevant worden deze kwaliteitsdoelen nader geconcretiseerd en contractueel geborgd in de Service Level Agreement (SLA), zie hoofdstuk 2. De SLA maakt onderdeel uit van de overeenkomst, maar de daarin opgenomen servicelevels gelden niet als uitsluitingscriteria in de aanbestedingsprocedure.

1.1 Performance efficiency

1.1.1. Time behavior

Het platform dient een vlotte gebruikerservaring te bieden. Responstijden en verwerkingssnelheid moeten passend zijn bij het gebruiksdoel van het platform en het aantal gelijktijdige gebruikers.
Nadere prestatieniveaus worden vastgelegd in de SLA.

1.1.2. Resource utilization

Het platform dient efficiënt om te gaan met infrastructuur- en hostingresources. Kostenbeheersing is hierbij een belangrijk uitgangspunt.
Concrete afspraken over hostingkosten en monitoring worden vastgelegd in de SLA en het prijzenblad

1.1.3. Capacity

Het platform dient ondersteuning te bieden voor ten minste 100 gelijktijdige gebruikers. Opschaling naar een groter aantal gebruikers moet mogelijk zijn zonder ingrijpende herbouw van de oplossing.

1.1.4 Energie-efficiëntie en duurzaamheid

De missie van Stichting Data Safe House (DSH) is onlosmakelijk verbonden met de verduurzaming van de energie-infrastructuur. Van leveranciers verwacht DSH daarom dat het IT-platform wordt gehost en geëxploiteerd op een wijze die aantoonbaar energie-efficiënt en toekomstbestendig is. DSH streeft naar een proportionele benadering, waarin duurzaamheid een wezenlijk kwaliteitsaspect is, zonder dat dit onnodig belemmerend werkt voor markttoegang, innovatie of uitvoerbaarheid.
De wijze waarop energie-efficiëntie wordt gemeten, gemonitord en geborgd, wordt nader uitgewerkt en geconcretiseerd in de Service Level Agreement (SLA).

1.2. Compatibility

Het technisch beheer wordt uitgevoerd door de leverancier. De oplossing dient zodanig te zijn ingericht dat overdracht aan een derde partij mogelijk is zonder onredelijke belemmeringen.
Exit- en overdrachtsafspraken worden uitgewerkt in de SLA en overeenkomst.

1.2.1. Co-existence

De oplossing dient geschikt te zijn voor moderne deployment- en beheeromgevingen, zoals containerisatie en schaalbare infrastructuren (bijvoorbeeld Docker of vergelijkbaar).

1.2.2. Interoperability

Het huidige platform heeft geen API capaciteiten, echter moet het wel mogelijk zijn om in de toekomst API functionaliteiten (bijv. op basis van open standaarden zoals REST met JSON of vergelijkbaar) toe te voegen, ten behoeve van gegevensuitwisseling met externe systemen.

1.3. Reliability

1.3.1. Faultlessness

De oplossing dient betrouwbaar om te gaan met data, waarbij dataintegriteit en vertrouwelijkheid zijn geborgd. Testen, rapportage en acceptatie maken integraal onderdeel uit van de ontwikkel- en releasecyclus.
Concrete test- en acceptatieafspraken worden vastgelegd in de SLA.

1.3.2. Availability

Het platform dient een hoge mate van beschikbaarheid (uptime) te kennen, passend bij het maatschappelijke en operationele belang van de dienstverlening.
Beschikbaarheidspercentages en servicevensters worden vastgelegd in de SLA.

1.3.3. Fault tolerance

De oplossing dient zodanig te zijn ingericht dat verstoringen automatisch kunnen worden opgevangen waar redelijkerwijs mogelijk.

1.3.4. Recoverability

De oplossing dient te beschikken over passende back-up- en herstelvoorzieningen om dataverlies en hersteltijd te beperken. Elke dag backup in een DSH account voor exit plan, in de vorm van een csv export op basis van nader overeen te komen format (bijv: 'Landelijk data format' + gebruikersgegevens).
Exacte RTO- en RPO-afspraken worden vastgelegd in de SLA.

1.4. Security

1.4.1. Confidentiality & Authenticity

Het platform dient te voldoen aan actuele beveiligingsstandaarden en overheidsadviezen (zoals NCSC). Authenticatie, autorisatie en versleuteling worden toegepast conform marktstandaarden. Multi-Factor Authentication (MFA) vereist, AES-256 encryptie en TLS 1.3 (of gelijkwaardig) voor opslag en transport. Het platform wordt initieel als stand-alone applicatie ingericht. Integratie met een extern SSO of identity-provider is geen vereiste in fase 1, maar dient technisch mogelijk te zijn in een latere fase.

1.4.2. Integrity

Wijzigingen in (inkomende) data en configuratie moeten traceerbaar zijn. Directe handmatige toegang tot productiedatabases is niet toegestaan.

1.4.3. Non-repudiation & accountability

Logging van kritieke wijzigingen (wijziging van rechten) en acties (logins, data invoer, data uitvoer). Logmeldingen moeten herleidbaar zijn tot specifieke accounts. Logs bewaard voor 2 jaar.

1.4.4. Resistance

Het platform dient beschermd te zijn tegen gangbare dreigingen, zoals ongeautoriseerde toegang en DDoS-aanvallen, passend bij de gekozen infrastructuur. (bijv. basis WAF en DDoS-bescherming via cloudprovider, handmatige mitigatiestrategieën)

1.5. Maintainability

De oplossing dient zodanig te zijn opgezet en gedocumenteerd dat deze goed onderhoudbaar, overdraagbaar en doorontwikkelbaar is. De broncode is overzichtelijk gestructureerd, begrijpelijk gedocumenteerd en sluit aan bij gangbare software-engineeringprincipes. DSH hecht waarde aan het borgen van de codekwaliteit. DSH behoudt zich het recht voor om optioneel en op eigen initiatief een onafhankelijke codekwaliteitstoets of audit te laten uitvoeren, bijvoorbeeld door een externe partij. Het uitvoeren van een specifieke codekwaliteitsmeting of het hanteren van een specifieke beoordelingsmethode (zoals SIG) is niet verplicht, mits de leverancier aantoonbaar kan onderbouwen dat de codekwaliteit op professioneel niveau is geborgd.

1.6. Flexibility

1.6.1. Adaptability

Configuratie van de oplossing dient zoveel mogelijk via instellingen plaats te vinden, zonder structurele code-aanpassingen. Fundamentelere wijzigingen vinden plaats via code-aanpassingen en handmatige implementaties.

1.6.2. Scalability

Opschaling van capaciteit (rekenkracht, data handling, opslagruimte, etc.) dient mogelijk te zijn zonder fundamentele herbouw van het platform.

1.6.3. Installability

Installatie en deployment van de oplossing dienen geautomatiseerd plaats te vinden, bijvoorbeeld via setup-scripts en/of CI/CD-ondersteuning. De oplossing dient rollback naar een stabiele versie te ondersteunen.

1.6.4 Replaceability (overdraagbaarheid, cloud-portability en technische soevereiniteit)

De oplossing dient zodanig te zijn ontworpen dat overdracht aan een andere leverancier en/of migratie naar een andere infrastructuuromgeving mogelijk is zonder onredelijke belemmeringen. In samenspraak met DSH wordt een evenwicht nagestreefd tussen overdraagbaarheid, kosten, doorlooptijd en complexiteit.
De oplossing is geschikt voor plaatsing bij een Europese cloud service provider (EU CSP) en is ontworpen om vendor lock-in te beperken. Architectuurkeuzes mogen het gebruik van gangbare cloudvoorzieningen niet onnodig beperken, mits kernfunctionaliteit, data en configuratie overdraagbaar blijven.

Eisen

- De oplossing ondersteunt het exporteren van data in open, gedocumenteerde formaten
- Relevante configuratie- en omgevingsinformatie (bijv. infrastructure-as-code/configuratie-definities) is beschikbaar ten behoeve van overdracht en continuïteit.
- De kern van de oplossing is gebaseerd op non-proprietary technologieën; waar open-source componenten worden gebruikt, beperken licentievoorwaarden de overdraagbaarheid niet.

Uitgangspunten

- De oplossing is op architectuurniveau cloud-portable: een overstap naar een andere EU CSP is mogelijk zonder fundamentele herbouw van de applicatie.
- Gebruik van cloud-specifieke diensten is toegestaan, mits deze vervangbaar zijn door functioneel gelijkwaardige alternatieven en geen onomkeerbare afhankelijkheden introduceren.
- De exacte mate van cloud-portability (en de bijbehorende ontwerpkeuzes) wordt in overleg tussen DSH en opdrachtnemer vastgesteld, met expliciete afweging tussen:
    - technische soevereiniteit en overdraagbaarheid;
    - planning en time-to-market;
    - kosten en beheersbaarheid.

2. Service Level Agreement (SLA) - Beheer en Onderhoud

Deze Service Level Agreement (SLA) beschrijft de afspraken tussen Stichting Data Safe House (DSH) en de opdrachtnemer over het beheer, onderhoud, beveiliging, continuïteit en doorontwikkeling van het IT-platform.

De SLA:

- concretiseert de kwaliteitsdoelen zoals beschreven in de non-functionele eisen;
- maakt onderdeel uit van de overeenkomst;
- is contractueel van aard en kan gedurende de looptijd, in onderling overleg, worden aangepast binnen de kaders van de aanbesteding.

2.1. Beschikbaarheid en performance

2.1.1. Beschikbaarheid

De opdrachtnemer draagt zorg voor een hoge beschikbaarheid van het platform, passend bij het doel en het gebruik van de dienstverlening.

- Beschikbaarheidseis: Minimaal 99% van het totaal aantal beschikbare uren per maand.
- Servicevenster: kantooruren (ma-vr, 09:00–17:00), tenzij anders overeengekomen.
- Gepland onderhoud wordt tijdig aangekondigd en afgestemd met DSH.

2.1.2. Performance

Het platform biedt een stabiele en voorspelbare gebruikerservaring bij normaal gebruik. Responstijden moeten passend zijn bij het gebruiksdoel van het platform en het aantal gelijktijdige gebruikers.

- **Kritieke gebruikersacties**: acties waarbij directe gebruikersfeedback vereist is (o.a. opslaan, bevestigen, navigatie). De applicatie verwerkt kritieke gebruikersacties in ten minste 95% van de gevallen binnen 1 seconde, gemeten end-to-end vanaf gebruikersactie tot zichtbare feedback in de gebruikersinterface. Aanvullende eis; de applicatie geeft binnen 500 milliseconden na een gebruikersactie zichtbare feedback over de status van de verwerking. Dit betreft met name acties zoals inloggen, navigeren binnen het platform, opslaan of indienen van gegevens, bevestigen van keuzes, en het openen of bijwerken van schermen met kernfunctionaliteit. De opsomming is niet limitatief; het uitgangspunt is dat alle interactieve handelingen die de gebruiker als direct en synchroon ervaart onder deze definitie vallen. De exacte afbakening kan in overleg bij contractering en in de SLA nader worden geconcretiseerd.
- **Niet-kritieke verwerking (synchroon),** gebruikersgestarte acties zonder directe urgentie. Niet-kritieke gebruikersacties die synchroon worden uitgevoerd, worden in ten minste 95% van de gevallen binnen 2 seconden afgerond.
- **Langdurige verwerking (asynchroon), verwerkingen** met een verwachte duur langer dan 2 seconden (zoals imports, exports, rapportages). Verwerkingen met een verwachte doorlooptijd van meer dan 2 seconden worden asynchroon uitgevoerd en:
    - starten met een bevestiging aan de gebruiker binnen 1 seconde;
    - voorzien de gebruiker van inzicht in de voortgang of status;
    - leveren het eindresultaat via de applicatie en/of notificatie.

2.1.3 Energie-efficiëntie en duurzaamheid

De opdrachtnemer draagt zorg voor een energie-efficiënte hosting en exploitatie van het IT-platform.

- De energieprestatie van de gebruikte datacenteromgeving wordt periodiek inzichtelijk gemaakt voor DSH.
- Als indicatieve maatstaf voor energie-efficiëntie wordt gebruikgemaakt van gangbare indicatoren zoals Power Usage Effectiveness (PUE) of een aantoonbaar gelijkwaardige maat. DSH hanteert hierbij een de eis PUE ≤ 1,5, of een onderbouwde afwijking, afhankelijk van type datacenter en aantoonbare duurzaamheidsmaatregelen.
- Richtwaarden, meetmethodiek en rapportagefrequentie worden bij contractering vastgesteld.

2.2. Incidentbeheer en continuïteit

2.2.1. Incidentclassificatie

Incidenten worden geclassificeerd op basis van impact en urgentie, bijvoorbeeld:

- kritiek (platform niet beschikbaar of security-incident);
- hoog (kernfunctionaliteit beperkt beschikbaar);

- middel / laag.

De exacte classificatie en prioritering worden vastgelegd bij contractering.

2.2.2. Hersteltijden (RTO) en dataverlies (RPO)

- Richtwaarde hersteltijd (RTO): maximaal 4 uur tijdens kantooruren.
- Richtwaarde maximaal dataverlies (RPO): maximaal 1 uur, of aantoonbaar gelijkwaardig.

2.2.3. Back-ups en herstel

- Dagelijkse back-ups van data en configuratie.
- Back-ups worden veilig opgeslagen en periodiek getest.
- Data-export ten behoeve van continuïteit en exit is mogelijk in het landelijk dataformat.

2.2.4 Risicomanagement en evaluatie

De opdrachtnemer ondersteunt de jaarlijks door DSH uit te voeren platform-specifieke risicoanalyse door tijdige en transparante informatievoorziening over relevante beveiligingsrisico's.
Dit omvat onder andere:

- nieuwe of gewijzigde dreigingen en kwetsbaarheden;
- wijzigingen in architectuur, infrastructuur, tooling of leverancierskеten die het risicoprofiel beïnvloeden;
- inzichten uit incidenten, beveiligingstesten en audits;
- voorgestelde mitigerende maatregelen en hun impact.

2.3. Monitoring, logging en security operations

2.3.1. Monitoring

De opdrachtnemer monitort continu de beschikbaarheid, performance en technische gezondheid van het platform. Bij verstoringen worden automatische meldingen gegenereerd en gedeeld. Monitoringinformatie is op verzoek inzichtelijk voor DSH.

2.3.2. Logging

- Kritieke acties en wijzigingen worden gelogd.
- Loggegevens zijn herleidbaar tot individuele accounts.
- Eis bewaartermijn logs: 24 maanden.

2.3.3. Beveiliging en patching

De opdrachtnemer past reguliere updates en beveiligingspatches toe. Kritieke beveiligingsupdates worden met prioriteit uitgevoerd. Beveiligingsmaatregelen zijn conform actuele marktstandaarden en relevante overheidsadviezen.

2.3.4. Security testing & assurance

Ter borging van de beveiliging van het platform worden periodiek beveiligingstesten uitgevoerd.

- **Pentesten**
  DSH behoudt zich het recht voor om jaarlijks een penetratietest (pentest) te laten uitvoeren door een externe partij. De opdrachtnemer verleent hieraan medewerking en stelt daartoe relevante documentatie en testomgevingen beschikbaar. De scope en frequentie van pentesten worden in overleg vastgesteld.
- **OWASP-controles**
  Binnen het ontwikkel- en releaseproces worden gangbare beveiligingscontroles toegepast door de opdrachtnemer, zoals checks gebaseerd op de OWASP of een vergelijkbaar raamwerk. Bevindingen die hieruit voortkomen worden, afhankelijk van ernst en impact, opgepakt binnen de afgesproken onderhouds- en wijzigingsprocessen.

Uitgevoerde beveiligingstesten en opvolging van bevindingen worden aantoonbaar vastgelegd.

2.3.5 Informatiebeveiligingsmanagement (ISMS) en rapportage

De opdrachtnemer werkt aantoonbaar met een Information Security Management System (ISMS) gebaseerd op ISO/IEC 27001 (of aantoonbaar gelijkwaardig) en past dit ISMS expliciet toe op de dienstverlening aan DSH.

- De opdrachtnemer rapporteert **tweemaal per jaar** aan DSH over de status van informatiebeveiliging binnen de DSH-dienstverlening.

- Deze rapportage vindt plaats op basis van een door DSH vastgesteld leveranciersbeoordelingsformat en bevat minimaal:
    - relevante bevindingen uit management reviews die de DSH-dienstverlening raken;
    - status van belangrijke beveiligingsmaatregelen;
    - relevante verbetermaatregelen en voortgang daarop.

De opdrachtnemer wijst een vast security-aanspreekpunt (en vervanger) aan voor de dienstverlening aan DSH, de CISO. Escalatielijnen (operationeel en managementniveau) worden vastgelegd in de SLA en periodiek geactualiseerd.

2.4. Onderhoud, releases en wijzigingsbeheer

2.4.1. Onderhoud

Opdrachtnemer is verantwoordelijk voor onderhoud aan het platform. Onderhoud omvat alle activiteiten die nodig zijn om het platform veilig, stabiel en actueel te houden. Hieronder vallen onder andere:

- het herstellen van fouten in de software;
- preventief onderhoud en optimalisaties;
- het toepassen van beveiligingsupdates en patches;
- het bijwerken en onderhouden van gebruikte plugins, libraries, frameworks, API-koppelingen en overige externe afhankelijkheden;
- het verhelpen van kwetsbaarheden in gebruikte componenten.
- opvolgen en mitigeren van bevindingen uit beveiligingstesten, waaronder pentesten en OWASP-gebaseerde controles

Onderhoudswerkzaamheden vinden plaats binnen de kaders van deze SLA en worden uitgevoerd zonder onnodige verstoring van de dienstverlening.

2.4.2. Releases, omgevingen en gepland onderhoud

Releases vinden gecontroleerd, herhaalbaar en volgens een afgesproken releaseproces plaats. De opdrachtnemer werkt volgens een gestructureerde ontwikkelmethodiek (bijv. agile of vergelijkbaar), met duidelijke fasering (bijvoorbeeld volgens het OTAP-principe of een vergelijkbare werkwijze), verantwoordelijkheden en vaste overlegstructuren. De opdrachtnemer richt een gestructureerde ontwikkel- en uitrolstraat in waarin minimaal de volgende omgevingen beschikbaar zijn:

- een testomgeving;
- een acceptatie-/stagingomgeving;
- een productieomgeving.

Daarnaast richt de opdrachtnemer een afzonderlijke demo-omgeving in. Deze demo-omgeving:

- bevat geen productiegegevens;
- maakt uitsluitend gebruik van dummy- of gesynthetiseerde data;
- wordt gebruikt voor demonstraties, presentaties en onboarding van (nieuwe) deelnemers;
- wordt periodiek opgeschoond voor overzichtelijkheid

De demo-omgeving dient functioneel gelijkwaardig te zijn aan de productieomgeving en mag geen productiegegevens bevatten; uitsluitend dummy- of gesynthetiseerde data wordt gebruikt. Nadere specificaties over publieke bereikbaarheid, aantallen gebruikers en beschikbaarheidsvensters maken geen onderdeel uit van de minimumeisen en worden in overleg bij contractering vastgesteld. Daarbij kan als uitgangspunt worden gehanteerd dat de demo-omgeving geschikt is voor gebruik door maximaal 100 gebruikers gelijktijdig, een richtwaarde voor beschikbaarheid van 95% kent en functioneel dezelfde eisen ondersteunt als de productieomgeving. Ten aanzien van non-functionele eisen kunnen, in overleg met DSH, proportionele concessies worden gedaan indien deze aantoonbaar kostenverlagend werken en geen afbreuk doen aan veiligheid en functionaliteit.

Releases die (tijdelijk) impact hebben op de beschikbaarheid van het platform worden bij voorkeur buiten kantooruren uitgevoerd, tenzij anders overeengekomen. Gepland onderhoud en eventuele downtime worden vooraf aangekondigd, afgestemd met DSH en gecommuniceerd met deelnemers, en vinden plaats binnen de afgesproken servicevensters en met inachtneming van de overeengekomen beschikbaarheidsafspraken.
Rollback naar een stabiele versie moet te allen tijde mogelijk zijn.

2.4.3. Wijzigingsbeheer

Wijzigingen aan het platform worden uitgevoerd binnen een transparant wijzigingsproces, waarin de opdrachtnemer verantwoordelijk is voor:

- het plannen en coördineren van wijzigingen;
- het organiseren en faciliteren van overlegmomenten met DSH;
- het vastleggen van besluiten, acties en wijzigingen (bijvoorbeeld in wijzigingslogs of notulen).

Richtwaarden voor afhandeling zijn:
- beveiligingsupdates: binnen 24 uur na vaststelling;
- blokkerende bugs: binnen 3 werkdagen;
- overige wijzigingen: in overleg, doorgaans binnen enkele weken.

Wijzigingen worden pas naar de productieomgeving gebracht na succesvolle test en acceptatie in de daarvoor ingerichte omgevingen. Bevindingen uit beveiligingstesten worden, afhankelijk van ernst en impact, geclassificeerd als beveiligingsupdate of bugfix en opgepakt conform de hiervoor geldende doorlooptijden.

2.5. Ondersteuning en servicedesk

Eerstelijnsondersteuning voor eindgebruikers (hulpvragen, registratie, etc.) wordt verzorgd door DSH. Tweedelijnsondersteuning (bugs, en/of indien wij vragen niet zelf kunnen beantwoorden) wordt geleverd door de opdrachtnemer. De opdrachtnemer hanteert een **duidelijke incidentclassificatie**, waarbij onderscheid wordt gemaakt tussen reguliere incidenten en security-incidenten met verschillende ernstniveaus.

- **Supporturen**: kantooruren (ma–vr, 09:00–17:00), voor security incidenten (hoog/kritiek) ma-zo, 8:00-22:00
- Incidentclassificatie en reactietijden (richtwaarden)
    - **Reguliere incidenten**. Incidenten zonder directe impact op vertrouwelijkheid, integriteit of beschikbaarheid van data. *Richtwaarde reactietijd:* binnen 8 uur.
    - **Security-incidenten (laag/middel)**. Beveiligingsgerelateerde bevindingen zonder directe of acute dreiging (bijvoorbeeld verdachte logs, kwetsbaarheden zonder actieve exploitatie). *Richtwaarde reactietijd:* binnen 8 uur of in overleg met DSH.
    - **Security-incidenten (hoog/kritiek)**. Incidenten met (mogelijke) directe impact op vertrouwelijkheid, integriteit of beschikbaarheid van data of systemen (bijvoorbeeld datalekken, actieve aanvallen, misbruik van accounts). *Richtwaarde reactietijd:* binnen 1 uur.

De exacte classificatiecriteria, opvolging en communicatie bij incidenten worden bij contractering nader vastgelegd. De opdrachtnemer informeert DSH tijdig en adequaat over de aard, voortgang en afhandeling van incidenten.

2.6. Documentatie en kennisbeheer

De opdrachtnemer draagt zorg voor actuele, volledige en toegankelijke documentatie van het IT-platform. De documentatie geeft op ieder moment inzicht in de werking, opzet en wijzigingen van het platform en is noodzakelijk voor beheer, doorontwikkeling, auditing en overdraagbaarheid.

Het is voor DSH van belang dat:
- de beschrijving van het platform en de architectuur te allen tijde up-to-date is;
- bij wijzigingen aantoonbaar wordt getest dat nieuwe of aangepaste functionaliteiten geen ongewenste neveneffecten of regressies veroorzaken;
- er altijd release notes beschikbaar zijn en gedeeld worden waarin wijzigingen inzichtelijk worden gemaakt.
- beveiligingsrelevante besluiten, risico-afwegingen en verbetermaatregelen aantoonbaar zijn vastgelegd en herleidbaar zijn voor auditdoeleinden.

Documentatie per release
Per release worden documentatie en rapportages opgeleverd die inzicht geven in:
- de inhoud en impact van de release;
- de uitgevoerde testen en testresultaten;
- eventuele aandachtspunten of bekende beperkingen.

De wijze waarop deze documentatie wordt ingericht en vormgegeven wordt in overleg met de leverancier bepaald. Hierbij kunnen gangbare documentatiestandaarden als referentie worden gebruikt, bijvoorbeeld J-STD-016-1995 of een vergelijkbare aanpak, mits de inhoud voldoende inzicht biedt in ontwerp, testen en kwaliteit.

Indicatieve documentatie-onderdelen
Afhankelijk van aard en omvang van de release kunnen onder meer de volgende documentatie-onderdelen worden opgeleverd, waarbij de inhoud overeenkomt met de genoemde J-STD-016-1995 documenttypen:

Ontwerp (bij wijziging van ontwerp of architectuur):

- System/Subsystem Design Description (SSDD) – beschrijving van het systeemontwerp;
- Interface Design Description (IDD) – beschrijving van interfaces;
- Database Design Description (DBDD) – beschrijving van de database en datamodellen.

Testdocumentatie (met name bij grotere of risicovolle releases):

- Software Test Plan (STP) – plan voor het uitvoeren van kwalificerende testen;
- Software Test Description (STD) – testcases en testprocedures;
- Software Test Report (STR) – resultaten van de uitgevoerde testen.

Release-informatie (bij elke release):

- Software Version Description (SVD) – release notes met overzicht van opgeleverde wijzigingen, bestanden en relevante aandachtspunten.

2.7. Exit en overdraagbaarheid

De continuïteit en onafhankelijkheid van het IT-platform zijn van groot belang voor Stichting Data Safe House (DSH). Om deze reden hecht DSH waarde aan een oplossing die overdraagbaar en onafhankelijk beheersbaar is, zonder onredelijke afhankelijkheden van één specifieke leverancier.

De opdrachtnemer stelt en onderhoudt daarom een exitplan, waarin wordt beschreven hoe bij beëindiging van de overeenkomst een ordentelijke overdracht kan plaatsvinden van:

- data;
- documentatie;
- broncode (voor zover van toepassing);
- relevante infrastructuur- en configuratiedefinities.

De wijze waarop overdraagbaarheid en continuïteit worden geborgd, wordt in samenspraak tussen DSH en opdrachtnemer vastgesteld. Hierbij kunnen, afhankelijk van de gekozen oplossing, passende maatregelen worden getroffen, zoals:

- het onderbrengen van (maatwerk)broncode in een escrow-regeling of een vergelijkbare constructie;
- het borgen van toegang tot gebruikte standaardsoftware, libraries en configuraties;
- het beschikbaar stellen van voldoende documentatie en kennis om beheer en doorontwikkeling door een derde partij mogelijk te maken.

De overdracht dient plaats te vinden zonder onredelijke belemmeringen voor DSH of een opvolgende partij. Tijdelijke ondersteuning na contractbeëindiging kan onderdeel uitmaken van de afspraken. DSH behoudt het recht om het exitplan inclusief overdracht te laten testen.

2.8. Evaluatie en bijstelling

De SLA wordt periodiek geëvalueerd door DSH en de opdrachtnemer. Op basis van voortschrijdend inzicht of gewijzigde omstandigheden kan de SLA in onderling overleg worden aangepast, mits dit past binnen de kaders van de overeenkomst en de aanbesteding.

3. Overige contractuele afspraken (indicatief kader)

Dit hoofdstuk beschrijft het indicatieve kader voor de overige contractuele afspraken die onderdeel zullen uitmaken van de dienstverleningsovereenkomst. Waar mogelijk zijn deze afspraken geformuleerd als uitgangspunten of eisen die richtinggevend zijn voor de contractvorming. Op onderdelen waar bewust ruimte wordt gelaten voor nadere invulling, zijn deze als open vraag gesteld.

De overeenkomst heeft het karakter van een dienstverleningsovereenkomst, waarbij onderdelen van de dienstverleningsovereenkomst het karakter hebben van een raamovereenkomst. Dit betreft met name de afname van uren en/of nadere opdrachten tegen een vaste prijs in het kader van doorontwikkeling.

3.1. Aansprakelijkheid en verzekeringen

DSH streeft naar een evenwichtige en proportionele verdeling van risico's die past bij de aard van de dienstverlening, de publieke rol van de stichting en de gevoeligheid van de data. Aansprakelijkheid moet bijdragen aan zorgvuldige uitvoering, zonder innovatie of samenwerking onnodig te belemmeren.

Eisen

- De opdrachtnemer is aansprakelijk voor schade als gevolg van toerekenbare tekortkomingen in de uitvoering van de overeenkomst.
- De opdrachtnemer beschikt over passende verzekeringen, waaronder ten minste een bedrijfsaansprakelijkheidsverzekering en, gezien de aard van de dienstverlening, een cyberverzekering.

Zie ook paragraaf 3.4.1 van de Leidraad.

3.2. Intellectueel eigendom (IE) en gebruiksrechten

DSH hecht groot belang aan onafhankelijkheid en het voorkomen van vendor lock-in. Het platform vervult een neutrale en publieke rol en moet duurzaam beheersbaar en overdraagbaar zijn, ook buiten de relatie met één specifieke leverancier.

Eisen

- Het intellectueel eigendom van maatwerksoftware, broncode, documentatie, datamodellen en configuraties die in het kader van de opdracht worden ontwikkeld, berust bij DSH.
- Voor generieke modules, libraries of componenten die de leverancier reeds heeft ontwikkeld en die breder worden ingezet, kan worden volstaan met het verlenen van een onbeperkt, onherroepelijk en overdraagbaar gebruiksrecht, mits dit DSH in staat stelt het platform zelfstandig te beheren, door te ontwikkelen en over te dragen aan een derde partij zonder aanvullende beperkingen.

Open punten / nadere uitwerking

- Contractuele uitwerking van IE-overdracht en licentievoorwaarden.
- Afspraken over hergebruik van generieke componenten door de leverancier.

3.3. Geheimhouding en gegevensbescherming (AVG/GDPR)

DSH verwerkt gevoelige data en opereert als onafhankelijke stichting. Vertrouwelijkheid, dataveiligheid en naleving van wet- en regelgeving zijn daarom randvoorwaardelijk voor de samenwerking met leveranciers.

Eisen

- Volledige naleving van de AVG/GDPR.
- Sluiten van een verwerkersovereenkomst als onderdeel van de contractvorming.
- Strikte geheimhouding van alle vertrouwelijke informatie van DSH en haar deelnemers.
- Leverancier ondersteunt DSH bij het voldoen aan relevante verplichtingen rondom incidentmelding en datalekken (waaronder tijdige signalering, opvolging en documentatie).

Open punten / nadere uitwerking

- Concrete afspraken over (sub)verwerkers, verwerkersregister en meldplichten.

3.4 Juridische soevereiniteit en EU-rechtsmacht (EU law only)

DSH hanteert het uitgangspunt dat opslag, verwerking en toegang tot data uitsluitend plaatsvindt binnen de juridische en bestuurlijke context van de Europese Unie ("EU law only"), passend bij de publieke rol van DSH en de gevoeligheid van de data.

Eisen

- Dataopslag, -verwerking en -toegang vinden uitsluitend plaats onder EU-rechtsmacht.
- Hosting en kerninfrastructuur worden geleverd door een Europese cloud service provider (EU CSP).
- Toegang tot data op basis van wetgeving van derde landen (zoals de CLOUD Act of vergelijkbare extraterritoriale regimes) is uitgesloten, zowel direct als indirect via (sub)verwerkers.
- Verwerkersovereenkomsten en sub-processorafspraken zijn expliciet ingericht op EU-rechtsmacht en "EU law only"
- Wijzigingen in (sub)verwerkers of hostinglocaties worden vooraf gemeld aan DSH.

Open punten / nadere uitwerking

- Wijze van aantoonbaarheid (bijv. contractuele garanties, assurance-verklaring, auditrapport, of gelijkwaardig bewijs).
- vormen van bewijs (contractuele garantie, assurance-verklaring, auditrapport, attest van CSP, etc.).
- Exacte definities/criteria voor "EU CSP" en toepasselijke controles.

3.5. Prijsmodellen en facturering

DSH streeft naar een transparant, schaalbaar en voorspelbaar prijsmodel dat past bij een platform met een maatschappelijke functie en groeiend gebruik. Beheerkosten moeten losstaan van het aantal gebruikers.

De beheerprijs ziet op beheer/onderhoud van de oplossing. Infrastructuurkosten worden transparant en onderbouwd 1-op-1 doorgelegd (zonder opslag) indien de inschrijver deze contracteert. Inschrijvers dienen wel hun infra-behoefte en ontwerpkeuzes te onderbouwen (o.a. i.v.m. overdraagbaarheid/exit), maar infra-kosten worden niet als opslag in de beheerkosten verwerkt.

De kwalificatie of kosten als IT-infrastructuur mogen worden doorgelegd, dan wel onderdeel zijn van de beheerkosten, wordt bepaald door de functionele rol van de betreffende dienst. Generieke CSP-platformdiensten die noodzakelijk zijn voor hosting en runtime van het platform kunnen 1-op-1 worden doorgelegd. Applicatie-specifieke software, beheer- en ontwikkeltooling en ondersteunende diensten die de opdrachtnemer inzet ten behoeve van beheer en onderhoud vallen onder de maandelijkse beheerkosten, ongeacht of deze technisch via de CSP worden afgenomen.

Eisen

- Prijsafspraken zijn transparant en toetsbaar.
- Beheerkosten staan los van het aantal gebruikers.
- Beheerkosten starten nadat deel 1 van de applicatie operationeel is voor alle gebruikers.
- Doorontwikkeling vindt plaats binnen het kader van de overeenkomst, met nadere opdrachten of offertes conform afgesproken kostenramingen.
- Meerwerkafspraken worden expliciet vastgelegd.

Open punten / nadere uitwerking

- Nadere invulling van vaste prijzen, uurtarieven en indexatie.
- Concrete plafondafspraken.

3.6. Contractduur en opzegvoorwaarden

DSH kiest bewust voor een contractstructuur die stabiliteit biedt, maar tegelijkertijd voldoende flexibiliteit laat om regie te houden en afhankelijkheden te beperken.

Eisen

- De overeenkomst kent een initiële looptijd van 48 maanden.
- Na afloop van de initiële looptijd wordt de overeenkomst stilzwijgend verlengd met 12 maanden per keer.
- Indien de opdrachtnemer niet wenst te verlengen, dient dit 12 maanden voorafgaand aan het einde van de lopende termijn schriftelijk te worden gemeld.

Open punten / nadere uitwerking

- Operationele afspraken over afwikkeling bij beëindiging worden vastgelegd in de overeenkomst en het exitplan.

3.7. Escalatie- en Conflictmanagement

Een constructieve samenwerking vraagt om heldere afspraken over escalatie en geschiloplossing, met behoud van bestuurlijke regie door DSH.

Eisen

- Er wordt een duidelijke escalatieprocedure ingericht met aanspreekpunten aan beide zijden.

Open punten / nadere uitwerking

- Nadere uitwerking van escalatieniveaus en termijnen.
- Inzet van mediation voorafgaand aan juridische stappen.

3.8. Compliance, audits en Certificeringen

DSH verwacht van leveranciers een professioneel en aantoonbaar volwassen niveau van kwaliteitsmanagement en informatiebeveiliging, passend bij de publieke rol van het platform en de gevoeligheid van de verwerkte data. Certificeringen worden hierbij gezien als middel om dit niveau aan te tonen, niet als doel op zich.
Bij de ontwikkeling, implementatie en het beheer van het IT-platform past de opdrachtnemer passende beveiligingsmaatregelen toe die zijn gebaseerd op gangbare en erkende normen en best practices.

Eisen

- De opdrachtnemer werkt aantoonbaar conform:
  - **NEN-ISO 9001:2015** (kwaliteitsmanagementsystemen) of aantoonbaar vergelijkbaar;
  - **NEN-ISO 27001:2015** (informatiebeveiligingsmanagement) of aantoonbaar vergelijkbaar;
  - **NEN-ISO 27002:2025** (maatregelen voor informatiebeveiliging) of aantoonbaar vergelijkbaar normenkader.
- Indien de opdrachtnemer (nog) niet gecertificeerd is, dient hij aannemelijk te maken dat hij aantoonbaar volgens deze normen werkt en dat certificering wordt behaald uiterlijk 1/1/2027.
- Voor zover de opdrachtnemer bij de uitvoering van de overeenkomst gebruikmaakt van een cloudprovider of andere onderaannemer voor hosting of technische infrastructuur, toont de opdrachtnemer aan dat deze partij beschikt over een aantoonbaar gelijkwaardig niveau van informatiebeveiliging, bijvoorbeeld door:
  - **SOC 2 Type II**;
  - **ISO/IEC 27001 in combinatie met ISO/IEC 27017**;
  - of een aantoonbaar gelijkwaardig normenkader.
- De opdrachtnemer verleent DSH auditrechten op de naleving van beveiligings- en compliance-eisen uit de overeenkomst en SLA, binnen redelijke grenzen.
- De opdrachtnemer faciliteert audits door DSH of een door DSH aangewezen onafhankelijke derde.
- Voor relevante onderaannemers en cloudproviders borgt de opdrachtnemer contractueel dat:
  - zij aantoonbaar voldoen aan gelijkwaardige beveiligingsnormen;
  - zij medewerking verlenen aan audits of assurance leveren via auditrapporten (bijv. SOC2, ISO).

De opdrachtnemer blijft te allen tijde verantwoordelijk voor naleving van de beveiligings- en compliance-eisen binnen de gehele keten.

DSH neemt de kosten voor het uitvoeren van audits, hetzij door DSH zelf hetzij door een door DSH aangewezen derde partij, voor haar rekening. Van de opdrachtnemer wordt verwacht dat zowel het platform als het ontwikkel- en beheerproces audit-ready worden ingericht, zodat het faciliteren van reguliere audits geen significante extra kosten met zich meebrengt. Indien DSH aanvullende of zwaardere audit-eisen stelt die verder gaan dan de in de aanbesteding opgenomen eisen, zullen de daaruit voortvloeiende meerkosten door DSH worden gedragen.

Open punten / nadere uitwerking

- De wijze waarop aantoonbaarheid wordt geleverd (bijvoorbeeld certificaat, auditrapport, assurance-verklaring of gelijkwaardig bewijs).
- De rol van aanvullende, optionele certificeringen of standaarden, zoals:
  - BIO (voor zover relevant);
  - ISO 14001;
  - CO_2-prestatieladder.

Deze aanvullende certificeringen kunnen als voorbeelden dienen, maar zijn geen verplicht onderdeel van de aanbesteding.

3.9 Organisatorische soevereiniteit en transparantie

DSH stelt eisen aan de zeggenschapsstructuur, eigendomsverhoudingen en transparantie van de opdrachtnemer en diens keten, passend bij de publieke en onafhankelijke rol van het platform.

Eisen (eigendom en zeggenschap)

- Ultimate Beneficial Owners (UBO's) zijn uitsluitend natuurlijke personen die kwalificeren als EU-onderdanen.
- Maximaal 24% eigendom per niet-EU entiteit.
- Gezamenlijk maximaal 39% eigendom door niet-EU entiteiten.
- Geen enkele niet-EU partij mag directe of indirecte feitelijke zeggenschap hebben over:
    - de dienstverlening;
    - de onderliggende infrastructuur;
    - de operationele besluitvorming.

Transparantie (keten en sub-processors)

- De opdrachtnemer verschaft volledige openheid over ingezette:
    - sub-processors;
    - toeleveranciers;
    - cloudproviders;
    - hun locatie en mate van soevereiniteit.
- Wijzigingen in de keten worden vooraf gemeld aan DSH.

Auditbaarheid

- DSH behoudt het recht om naleving van deze afspraken te laten toetsen, direct of via onafhankelijke audits.