

Bestek dataplatform voor monitoring en toezicht in de garnalenvisserij

Maart 2023, versie 1.0

Ministerie van Landbouw, Natuur en Voedselkwaliteit

Inhoud

1.	Inleiding	3
2.	Projectinformatie	3
2.1	Projectscope, -aanpak, -planning en -kosten	4
2.2	Functionele vereisten	4
2.2.1	Verzamelen en organiseren van data	4
2.2.2	Verwerking van de data	6
2.2.3	Portaalfunctie	7
2.2.4	Data-onderzoek	8
2.3	Niet-functionele vereisten	9
2.3.1	Portabiliteit	9
2.3.2	Modulariteit	9
2.3.3	Beveiliging, privacy en recovery	10
2.4	Productkwaliteit	10
2.5	Kwaliteit van dienstverlening	12

1. Inleiding

Voor toezicht en monitoring in de garnalenvisserij is een dataplatform nodig dat data uit zogenaamde black box-systemen opslaat en verwerkt. Dit dataplatform heeft als doel te monitoren of een schip bepaalde grenswaarden heeft overschreden, zoals varen en vissen in bepaalde gebieden of op bepaalde momenten.

Gebruikers van het systeem zijn vergunningverleners (ministerie LNV), toezichthouders (NVWA en Waddenunit), de kustwacht (een samenwerkingsverband waarin ook de NVWA vertegenwoordigd is), producentenorganisaties en schippers.

Zonder een goed functionerende black box-systeem met dataverwerking is een goede controle en handhaving van de garnalenvisserij in onze kustwateren en meer specifiek in de Natura 2000-gebieden niet of nauwelijks mogelijk.

2. Projectinformatie

Aan boord van garnalenvissersschepen worden ten behoeve van handhaving sensoren ingezet, met name in de vorm van black box-systemen gebaseerd op NTA 8390-1_2022¹. Deze systemen leveren onder meer locatiedata en scheepsidentificatie. In de toekomst wordt de datastroom mogelijk uitgebreid met meetdata van motor, radiobakens of andere sensoren (deze doorontwikkeling maakt geen deel uit van dit bestek).

Dit project betreft ontwikkeling van een dataplatform die deze data opslaat en verwerkt, met als doel om te bepalen of een schip op een bepaald tijdstip aan het vissen of aan het varen is. Het dataplatform dient zowel ruwe als geïnterpreteerde data beschikbaar te maken voor monitorende en handhavende instanties en ook voor schippers.

Het gaat om private gegevens van de ondernemers die in een database moeten komen die door de vergunningverleners (ministerie LNV) en de handhavers (NVWA, Kustwacht, Waddenunit) kunnen worden gebruikt en/of ingezien, en ook door de producentenorganisaties en de schippers.

Data wordt momenteel per GSM aangeleverd en is daardoor niet altijd voor alle schepen real time beschikbaar. Het betekent ook dat als een schip langer buiten GSM-bereik is geweest er een upload van veel data op een moment plaatsvindt. Het systeem moet daarin kunnen voorzien. Het is de bedoeling dat via algoritmes automatisch uit de data wordt afgeleid of een schip bepaalde grenswaarden overschrijdt, zoals vissen in een gesloten gebied, overschrijding van het maximale aantal visuren, de tijd binnen/buiten een haven. In de toekomst wordt dit mogelijk uitgebreid met meetwaarden en begrenzingen met betrekking tot stikstofuitstoot (deze doorontwikkeling maakt geen deel uit van dit bestek).

Het is de bedoeling dat aan de handhavende instantie en de schipper een notificatie wordt gestuurd wanneer een schip tevoren bepaalde grenswaarden overschrijdt.

¹ <https://www.nen.nl/nta-8390-1-2022-nl-302400>

LNV, NVWA, Waddenunit, producentenorganisaties en schippers moeten toegang krijgen tot dit systeem. Mogelijk worden hieraan in de toekomst meer personen of instanties toegevoegd.

2.1 Projectscope, -aanpak, -planning en -kosten

De scope van het project betreft:

- de ontwikkeling en ingebruikname van het systeem volgens dit bestek;
- exploitatie en beheer volgens dit bestek voor een periode van twee jaar vanaf ingebruikname.

Het beoogde dataplatform dient ontwikkeld en in gebruik genomen te zijn binnen 22 weken na gunning van de opdracht. Gunning wordt voorzien in de maand maart van 2023.

Ontwikkeling en twee jaar beheer en exploitatie is mogen in totaal niet meer kosten dan €135.000, =

Dit bestek is een belangrijke leidraad voor kaderstelling, geen uitputtend gedetailleerde specificatie. Tijdens de realisatie van het dataplatform en het opstellen van de SLA zullen keuzen en detaillering nog zijn in nauw overleg met de product owner van LNV.

Zeker gelet op de combinatie van beperkte doorlooptijd, financiële begrenzing en benodigde afstemming is agile ontwikkelwijze een vereiste.

Uitgangspunt is dat realisatie in maximaal 10 sprints van twee weken zal plaatsvinden. Voorafgaand aan elke sprint stemmen opdrachtnemer en product owner de – haalbare – doelen af. Na afloop van elke sprint valideren zij samen de resultaten en blikken vooruit naar de komende sprint. Hiermee hebben we korte iteraties en kunnen is het mogelijk indien nodig snel bij te sturen.

Gezien de gewenste opleverdatum en het beperkte aantal sprints zal naast de tweewekelijkse sprintplanning en -demo's tenminste wekelijks afstemming met tussen opdrachtgever en opdrachtnemer plaatsvinden.

Bovenstaande aanpak is een vertrekpunt: het staat de aanbieder vrij een alternatieve aanpak voor te stellen, zolang deze maar agile van aard is, met name in korte iteraties waardoor nauwe afstemming en snelle bijsturing mogelijk zijn.

De voertaal in het project is Nederlands, zowel in de ontwikkel- als de beheer- en exploitatiefase. Ook correspondentie, documentatie en dergelijke dient in het Nederlands te gebeuren.

2.2 Functionele vereisten

2.2.1 Verzamelen en organiseren van data

Voornaamste input voor het dataplatform omvat black box-data (w.o. positie en identificatie van schepen) en data met betrekking tot bepaalde begrenzingen waaraan een schip zich

dient te houden. Deze begrenzungen omvatten in welke gebieden en op welke momenten de garnaalschepen mogen varen en vissen), zoals de omlijning van bepaalde gebieden binnen een Natura 2000-zon en de maximale hoeveelheid visuren voor schepen.

Zodra de data van de momenteel drie typen black box-systemen wordt ontvangen, dient deze op het dataplatform te worden gestroomlijnd. De verschillende datastromen uit de verschillende black boxen, in totaal ca. 170 stuks, komen zo in de database terecht in één gestandaardiseerd formaat. De database-structuur moet op zo'n manier worden opgezet dat later (buiten scope van dit project) nieuwe typen black box-systemen en nieuwe typen (sensor-)data kunnen worden toegevoegd, zonder dat dit de structuur van de oude data aantast.

Het dataplatform dient in de toekomst uitbreidbaar te zijn met data uit nieuwe externe bronnen, zoals met stikstofmetingen en informatiesystemen van bijvoorbeeld RVO, LNV en EZ. De uitbreidbaarheid is een projecteis, de toekomstige uitbreidingen als zodanig (bijvoorbeeld data met betrekking tot getijden en weer) vallen buiten de scope van dit project.

Voor de component "Verzamelen en organiseren data" geldt verder:

1. Een bedrijfszeker, controleerbaar en herhaalbaar proces voor ontvangst, opslag en verwerking van (initieel) de volgende data:
 - a. Uit externe bronnen:
 - i. Black box-data:
 1. Scheepsidentificatie
 2. Tijd en datum
 3. Geografische positie
 4. Wel/niet vissen
 5. Wel/niet functionerende black box
 - ii. Extern geregistreeerde geodata, waaronder gebieden waarvoor restricties gelden, zoals Natura 2000-gebieden;
 - b. Via het portaal (zie paragraaf 3.2.3):
 - i. Data van schepen, waaronder scheepsidentificatie, naam, thuishaven, schippers;
 - ii. Data van schippers, waaronder contactgegevens;
 - iii. Geodata, waaronder havenlocaties en gebieden waarvoor restricties gelden;
 - iv. Restricties met grenswaarden voor locaties en gebieden;
 - v. Begrenzungen en quota met betrekking tot uitstoot en vis- en vaaruren, zowel voor individuele schepen als voor groepen schepen;
 - c. Opslag en archivering van de resultaten van dataverwerking, waaronder:
 - i. Analyse- en berekeningsresultaten, waaronder kwaliteitscontrole en fraudedetectie met betrekking tot ontvangen data;
 - ii. Overschrijding van grenswaarden;
 - iii. Notificaties;
 - iv. Historie;
 - v. Procesdata;
 - vi. Auditlogging;

- d. Metadata, waaronder de betekenis van data (uniforme definities);
2. Mutatie, waaronder correctie, van data (bijvoorbeeld met betrekking tot begrenzing van een gesloten gebied) wordt aangeleverd en verwerkt op dezelfde wijze als de oorspronkelijk aangeleverde data. Verwerking van mutaties met terugwerkende kracht (update op de historie) moet mogelijk zijn. Dergelijke mutaties moeten nog wel als zodanig herkenbaar zijn;
3. De eigenaar van een gegevensbron is verantwoordelijk voor tijdige en complete data-aanlevering, datakwaliteit en aanlevering van eventueel benodigde correcties;
4. Nieuwe databronnen dienen te kunnen worden ontvangen en opgeslagen binnen drie maanden vanaf het moment dat de uitbreiding met opdrachtnemer is afgestemd. Deze uitbreidbaarheidseis is onderdeel van dit project, uitbreiding met nieuwe bronnen als zodanig valt uiteraard buiten de scope;
5. Wijzigingen in bestaande databronnen dienen te worden kunnen worden gerealiseerd binnen een maand vanaf het moment dat de eigenaar de databron de wijziging met opdrachtnemer heeft afgestemd en bekrachtigd. Deze eis voor de beheer- & exploitatiefase is in scope van het project.

2.2.2 Verwerking van de data

Wanneer bovengenoemde data is verzameld in de database van het dataplatform, moet de data verwerkt worden. Dit gebeurt door middel van relatief simpele algoritmes.

Voor iedere black box wordt op basis van de reeks doorgegeven locatie/tijdstip-combinaties bepaald op welke momenten is gevaren, met welke snelheid. Locatie, tijdstip en snelheid worden vervolgens vergeleken met begrenzingen om vast te stellen of die zijn overschreden. Begrenzingen omvatten tijdstippen dat schepen in de haven moeten zijn, gesloten gebieden, quota met betrekking tot vis- en vaaruren en in het bijzonder de omstandigheden die bepalen of er is gevist. Bijvoorbeeld: langer dan 5 minuten varen met een snelheid lager is dan 3,5 knopen² betekent dat er is gevist.

Door de locatie/tijdstip-combinaties en de berekende snelheid te vergelijken met deze begrenzing wordt vastgesteld wanneer is gevist. Een aanvullende bepaling wanneer is gevist gebeurt op basis van de black box-data: per locatie/tijdstip-combinaties wordt door de black box geregistreerd of er is gevist.

Ook wordt gesignaleerd op welke momenten de black box niet functioneert. De periode van niet-functioneren wordt geregistreerd, inclusief de black box-data van 10 minuten voorafgaand en 10 minuten na het niet-functioneren.

Deze dataverwerking betreft nadrukkelijk het signaleren van overschreden grenswaarden. Het is aan de handhavende instantie (vooralsnog de NVWA) om te bepalen of een overschrijding een overtreding betreft.

Signalering van grensoverschrijdingen kan gaan over het vissen in gesloten gebieden, het overschrijden van het toegestane aantal visuren in een bepaald gebied of vissen in een

² De precieze waarden van deze begrenzing wordt nog beproefd en dient door de vergunningverlener te kunnen worden aangepast met behoud van historie.

gesloten tijd (bijvoorbeeld weekendverbod). Gesignaleerde overschrijdingen dienen ook op het dataplatform te worden opgeslagen zodat hieraan gerefereerd kan worden. Dit kan door een nieuwe variabele toe te voegen in de dataset of door een nieuwe dataset op te bouwen.

Voor de component “Verwerking van de data” geldt verder dat signalering dient plaats te vinden binnen 5 minuten na ontvangst van de betreffende brondata.

2.2.3 Portaalfunctie

Voor toegang tot het portaal moeten er verschillende autorisatieniveaus zijn, zoals schipper, toezichthouder, producentenorganisatie en administrator. Gedurende het project worden door opdrachtgever in overleg met betrokken partijen toegangsrechten vastgesteld voor de verschillende partijen.

Het portaal biedt functionaliteit voor het geautoriseerd invoeren, muteren en raadplegen van:

- Data van schepen, waaronder scheepsidentificatie, naam, thuishaven, schippers;
- Data van schippers, waaronder contactgegevens;
- Geodata, waaronder havenlocaties en gebieden waarvoor restricties gelden;
- Restricties met grenswaarden voor locaties en gebieden;
- Begrenzings en quota met betrekking tot uitstoot en vis- en vaaruren, zowel voor individuele schepen als voor groepen schepen;
- Analyse- en berekeningsresultaten, waaronder kwaliteitscontrole en fraudedetectie met betrekking tot ontvangen black box-data.

Daarnaast kunnen resultaten uit eerdergenoemde componenten (eventueel voorafgegaan door een notificatie) via de portaalfunctie door geautoriseerden worden geraadpleegd, waaronder:

- Metadata;
- Overschrijding van grenswaarden;
- Notificaties;
- Historie;
- Procesdata;
- Auditlogging.

Van gesignaleerde overschrijdingen wordt een notificatie aan de handhavende instantie gestuurd. Zodra er op het dataplatform wordt vastgesteld dat er een overschrijding heeft plaatsgevonden treedt een protocol in werking dat toezichthouders en de schippers op de hoogte stelt. Dit protocol bestaat uit een notificatie met een verwijzing naar het portaal, waar een melding van de overschrijding is te raadplegen. Bijvoorbeeld: “Er is op 1 januari 2023, van 3:30 tot 4:10 uur gevist in gesloten gebied (naam van het gesloten gebied)”. Een notificatie zelf bevat geen inhoudelijke informatie, slechts de verwijzing naar het portaal, bijvoorbeeld: “Er is een melding voor u, raadpleeg het portaal.”

Op het portaal dient data als geodata ook gevisualiseerd (reis-/trackingkaart) te worden, zodat deze breed toegankelijk is. Denk aan een kaart waar relevante gebieden op worden geprojecteerd op worden geprojecteerd en waarop vaar- en visgedrag te zien is.

Voor de component “Portaalfunctie” geldt verder:

1. In het portaal is instelbaar welke partij welk type notificaties dient te ontvangen. De volgende partijen dienen genotificeerd te kunnen worden:
 - a. handhavers (NVWA, Kustwacht, Waddenunit;
 - b. schippers;
 - c. vergunningverleners (ministerie LNV);
 - d. producentenorganisaties.
2. Bij geconstateerde overschrijdingen wordt een notificatie verzonden.
3. Bij niet-functioneren van de black box wordt een notificatie verzonden.
4. Het is een gegeven dat notificeren soms beperkt mogelijk is door beperkte communicatiefaciliteiten op zee (GSM).
5. Een notificatie bevat uitsluitend een verwijzing naar het portaal, waar de melding van de overschrijding is te raadplegen;
6. Communicatiekanalen voor notificaties zijn email en SMS, eventuele alternatieven kunnen in overleg tussen product owner van LNV en opdrachtnemer gedurende het project worden bepaald;
7. Het portaal verschaft op basis van autorisatie inzicht in de beschikbare data aan (in eerste instantie) vergunningverleners (ministerie LNV), handhavers (NVWA, Kustwacht, Waddenunit), producentenorganisaties en schippers. Dit inzicht wordt gerealiseerd door middel van:
 - a. Visualisatie;
 - b. Reguliere (kwantitatieve) rapportages en dashboards;
 - c. Export van datasets voor belanghebbenden voor ad hoc rapportages;
 - d. Export van datasets t.b.v. analyse en onderzoek;
 - e. De betekenis van data (uniforme definities);
8. Met behoud van historie invoeren, muteren en verwijderen van grenswaarden en condities, waaronder havenlocaties, gesloten gebieden, gebiedsbepalingen, begrenzingen en quota met betrekking tot uitstoot ³en vis- en vaaruren.

2.2.4 Data-onderzoek

Voor een beperkt aantal geautoriseerde gebruikers dient de data volledig, maar ook in subsets exporteerbaar te zijn voor extern data-onderzoek. Dit onderzoek dient voor kwaliteitsverbetering door detectie van patronen, mogelijke fraude en overschrijdingen die nog niet in de standaardwijze van dataverwerking worden signaleerd.

Het data-onderzoek als zodanig maakt *geen* onderdeel uit van dit bestek. Wel dient (buiten het dataplatform) geconstateerde fraude met betrekking tot aangeleverde data te worden geregistreerd door de betreffende data te *flaggen* met tijdstip, bron en omschrijving van de fraudedetectie.

³ Voor uitstoot zijn alleen grenswaarden en condities in scope. Ontvangst en registratie van meetwaarden is een mogelijk toekomstige uitbreiding, evenals registratie van afwijkingen t.o.v. de grenswaarden en condities.

2.3 Niet-functionele vereisten

Vanwege gewenste flexibiliteit met betrekking tot beheer en exploitatie van het dataplatform dient deze zo overdraagbaar mogelijk te zijn. Mogelijk wordt het dataplatform op termijn in beheer genomen door een overheidsinstantie. Daarom is de Nederlandse overheid referentie-architectuur (NORA) het architectuurraster voor het dataplatform. De NORA kent tien basisprincipes en 38 daarvan afgeleide principes. Vanwege de leesbaarheid zijn in dit document zijn alleen de NORA-aspecten opgenomen die het meest bepalend zijn voor de realisatie van het dataplatform. Voor alle overige uitgangspunten verwijzen we naar de NORA zelf.

2.3.1 Portabiliteit

Elke van de componenten (verzamelen en organiseren van data, verwerking van data, portaalfunctie) moet in zijn geheel kunnen worden overgedragen aan een andere eigenaar, kunnen worden overgezet naar een andere omgeving of kunnen worden vervangen zonder dat de werking van de functionaliteit voor afnemende applicaties daardoor wijzigt.

2.3.2 Modulariteit

Ten behoeve van flexibiliteit, bestendigheid en aanpasbaarheid dient complexiteit te worden beheerst door toepassing van eenvoud als primair ontwerpcriterium.

Maatwerk maakt upgraden naar nieuwe versies van software ingewikkelder en duurder en beperkt de flexibiliteit. Om maatwerk te voorkomen dient in pakketsoftware ontbrekende functionaliteit in aparte component(en) te worden opgelost.

Componenten zijn, zo mogelijk, infrastructuur- en omgevingsafhankelijk.

Componenten maken zo veel mogelijk gebruik van herbruikbare functies voor logging, rapportage e.d. Dat betekent dat alle logging centraal beschikbaar is, niet op diverse plaatsen binnen de oplossing. Hetzelfde geldt voor rapportage.

Services dienen één functionele verantwoordelijkheid te hebben. Eventueel maatwerk in componenten dient flexibel te worden opgezet: met parameters configureerbaar.

Een goed gekozen modulaire opbouw dient de complexiteit van het systeem te beperken. Het maakt beheer, onderhoud en doorontwikkeling van de componenten en services overzichtelijker en eenvoudiger. Het maakt het mogelijk om er één te vervangen zonder dat de werking van andere daardoor wijzigt.

Services dienen ontkoppeld te zijn. Ontkoppelen houdt in dat de afhankelijkheid van componenten en services van andere componenten en services zoveel mogelijk beperkt is.

Communicatie tussen systemen en hun componenten dient te gebeuren op basis van webservices. Dankzij communicatie op basis van afgesproken protocol en berichtformaat, is

de wijze waarop deze services gerealiseerd worden niet van belang. Ook wordt eenvoudiger uitwisseling gerealiseerd en wordt herbruikbaarheid van functies en gegevens vergroot.

2.3.3 Beveiliging, privacy en recovery

Als dienstverlener garandeert opdrachtnemer dat informatie alleen toegankelijk is voor bevoegden. Die bevoegden zijn er verantwoordelijk voor dat data alleen wordt gebruikt voor het doel waarvoor het is verzameld. Dit principe geldt niet alleen voor informatie over personen, ook voor informatie over organisaties.

Voor databeveiliging geldt:

1. Berichtuitwisseling is onweerlegbaar door borging dat het ontvangen bericht afkomstig is van de afzender en dat de inhoud niet door derden is beïnvloed. Het moet achteraf altijd herleidbaar zijn welk inkomende en uitgaande bericht aanleiding was tot een actie. Acties zijn herleidbaar tot een persoon of systeem. Voor elk gegevensmutatie wordt bijgehouden wie, wanneer en hoe. Gegevens worden niet verwijderd, maar gemarkeerd als verwijderd. Er wordt auditing-informatie op recordniveau bijgehouden van gegevensmutaties;
2. Het beveiligingsniveau dient te voldoen aan het ISO 27002-normenkader dat onder meer betrekking heeft op, beveiligingsbeleid en -organisatie, personeel, beheer van bedrijfsmiddelen, toegangsbeveiliging, cryptografie, fysieke beveiliging, toegangsbeveiliging, operationele beveiliging inclusief (audit-)logging, communicatiebeveiliging, inkoop/ontwikkeling en onderhoud van systemen, leveranciersrelaties, incidentenbeheer, continuïteitsbeheer en compliance;
3. Autorisatie – alleen toegang tot data en diensten voor geautoriseerden;
4. Voor alle data zal door opdrachtgever dataclassificatie worden uitgevoerd, inclusief een *privacy impact assessment*;
5. Back-up en recovery dienen volgens een vastgelegd proces aantoonbaar beheersbaar te kunnen worden uitgevoerd;
6. Oplossing en dienstverlening zijn volgens het (public) cloud-beleid van de overheid.

2.4 Productkwaliteit

Voor de software productkwaliteit van het dataplatform geldt de veelgebruikte standaard ISO25010 (opvolger van ISO9126), onderdeel van de SQuaRE (Softwareproduct Quality Requirements and Evaluation) serie van standaarden. Dit is de reeks ISO 250xx standaarden.

Deze paragraaf bevat de belangrijkste eisen aan het dataplatform in dit kader ten aanzien van prestatie-efficiëntie, uitwisselbaarheid, betrouwbaarheid, beveiligbaarheid, verantwoording, onderhoudbaarheid en overdraagbaarheid.

Prestatie-efficiëntie

1. Mogelijk wordt prestatie-efficiëntie beïnvloed door trage communicatielijnen vanaf schepen. Opdrachtnemer kan echter voor de prestatie-eisen echter uitgaan van normale omstandigheden.
2. Vanwege het gebruik vanaf schepen (met zal de opdrachtnemer niet kunnen garanderen dat hier altijd aan voldaan wordt).

3. De responsetijd van de webinterface voor pagina's met eenvoudige verwerking bedraagt maximaal 0,5 seconde voor 80% van de schermen, maximaal 3 seconden voor 95% van de schermen;
4. De responsetijd van de webinterface voor pagina's met complexe verwerking bedraagt maximaal 1,0 seconde voor 80% van de schermen, maximaal 5 seconden voor 95% van de schermen;
5. Als een eenvoudige of complexe verwerking langer duurt dan respectievelijk 3 of 5 seconden wordt feedback aan de gebruiker gegeven;
6. Tijdens openstelling kan het dataplatform op enig moment gelijktijdig 200 interactieve gebruikers bedienen;
7. De throughput van het dataplatform bedraagt minimaal gelijktijdige verwerking van black box-data van 340 schepen (200% van huidige aantal);
8. De latency (responstijd) van een service (intern en extern) bedraagt maximaal 0,5 seconden voor 90% van de serviceaanroepen;
9. Bij toevoegen van verwerkingscapaciteit neemt de daadwerkelijke verwerking vrijwel lineair toe.

Uitwisselbaarheid

1. Softwarecomponenten kunnen binnen redelijke tijd (1 à 2 weken) worden aangepast om op een willekeurig cloudplatform te draaien door middel van containertechnologie (12factor.net richtlijn). De afhankelijkheden dienen in kaart te zijn gebracht.

Betrouwbaarheid en beschikbaarheid

1. Het service window in beheer en exploitatie is op werkdagen van 9:00-17:00 uur;
2. Binnen het service window is bij een calamiteit de RTO (recovery time objective) van 4 uur in 90% van de gevallen en 8 uur voor de overige 10%. Deze tijdsperiode geldt vanaf recoverybesluit tot vrijgave voor sanitytest;
3. Bij een calamiteit is de RPO (recovery point objective) 15 minuten in 90% van de gevallen.
4. Applicatiebeschikbaarheid (*) is 99,8% binnen het service window en 99,5 % daarbuiten, niet meegerekend ingepland en met product owner afgestemd (periodiek) onderhoud;
5. Platformbeschikbaarheid is 98,5% binnen het service window. Een volledige stilstand en weer opstarten van het dataplatform mag maximaal 30 minuten duren (incl. correct afsluiten van sessies).

Beveiliging

1. Er is een Information Security Management System volgens ISO 27001 ingericht;
2. Beveiligingsmaatregelen zijn volgens ISO27002 + BIO ⁴opgezet;
3. Privacy-maatregelen zijn volgens de AVG opgezet;
4. Opdrachtgever zorgt voor een Business Impact Analyse (of vergelijkbaar) met BIV-classificatie;
5. Externe communicatie op netwerkniveau is geheel TLS v1.3/HTTPS;
6. Webfacing componenten zijn hackproof volgens OWASP-normen (of aantoonbaar gelijkwaardig);
7. Softwarecode voldoet aan de secure coding richtlijnen van CIP en NCSC (of aantoonbaar gelijkwaardig);

⁴ https://bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf

8. Hashcodes ten behoeve van onweerlegbaarheid zijn minimaal SHA-256;
9. In overeenstemming met het NORA zoneringsmodel is er een duidelijke scheiding van vertrouwde en niet vertrouwde zones door middel van compartimentering op alle niveau's (netwerk tot applicatie).

Verantwoording

1. Mutaties en gebeurtenissen worden geregistreerd in auditlog (volgens H10.10 BIR2017/BIO H12);
2. Ieder in- en uitgaand bericht met rechtsgevolgen wordt gearchiveerd.

Onderhoudbaarheid

1. Codekwaliteit voldoet minimaal aan SIG 3,5⁵ of aantoonbaar vergelijkbaar;
2. Alle broncode moet met unit tests worden getest, tenzij de broncode op een andere manier automatisch getest wordt (bijvoorbeeld in systeemtest). Unittest coverage is minimaal 80%.

Overdraagbaarheid en toegankelijkheid

1. Een nieuwe installatie/deployment in een "schone" omgeving van een software-/standaardcomponent dient binnen 4 uur te kunnen worden uitgevoerd;
2. Er wordt gebruik gemaakt van volwassen en gangbare ontwikkeltechnologie met een breed ontwikkelaarsdraagvlak;
3. Softwarecomponenten die een frontend functionaliteit implementeren kunnen met een standaard browser ⁶op een workstation of mobiel apparaat worden uitgevoerd zonder dat de gebruiker hiervoor add- ons/plugin's hoeft te installeren;
4. UX voldoet aan de webrichtlijnen van de Nederlandse overheid⁷ en is voorbereid op de webrichtlijnen van de Europese Unie⁸, waaronder responsiveness.

2.5 Kwaliteit van dienstverlening

De opdracht omvat twee jaar beheer en exploitatie van het dataplatform. Deze periode start bij ingebruikname van het dataplatform. Beheer en exploitatie omvat technisch en functioneel beheer en beantwoording en registratie van kleine gebruikerswensen.

De beschikbaarheid en de kwaliteit van diensten dient te voldoen aan vooraf bepaalde normen. Door het platform aangeboden informatie dient bijvoorbeeld juist, authentiek, actueel en volledig te zijn. Daarbij kan opdrachtnemer er vanuit gaan dat aan het platform aangeleverde data dat ook is. De aan het dataplatform aanleverende partij is verantwoordelijk voor juiste, authentieke, actuele en volledige aanlevering van data. Processen zijn zodanig ingericht dat dit is gegarandeerd en monitoring van het kwaliteitsniveau plaatsvindt.

Ook dienen continuïteit en compliance in opzet en werking op alle niveaus (waaronder kwaliteitseisen, life-cycle management, beheer en exploitatie) te worden geborgd. Het

⁵ <https://www.softwareimprovementgroup.com>

⁶ <https://mijn.overheid.nl/geschikte-browsers/>

⁷ <https://www.rijksoverheid.nl/toegankelijkheid>

⁸ https://european-union.europa.eu/web-accessibility-policy_nl

voldoen aan wettelijke en andere (overheids)richtlijnen is integraal onderdeel van het dataplatform.

Om te kunnen valideren of services aan de gestelde kwaliteitseisen voldoen, moeten deze meetbaar zijn.

Alle stappen en mutaties worden geregistreerd ten behoeve van traceerbaarheid, het voldoen aan de niet-functionele eisen, verwerkings- en managementinformatie, kostenberekening, etc. Met deze meetgegevens kan worden vastgesteld of voldaan wordt aan het afgesproken serviceniveau. Hiervoor dient in overleg tussen product owner en opdrachtnemer een Service Level Agreement (SLA) te worden opgesteld.

Deze SLA omvat afspraken over de genoemde niet-functionele eisen met betrekking tot prestatie-efficiëntie, uitwisselbaarheid, betrouwbaarheid, beveiligbaarheid, verantwoording, onderhoudbaarheid en overdraagbaarheid.

Daarnaast omvat de SLA tenminste afspraken met betrekking tot servicedesk, incident management, change management en probleem management volgens ITIL, ASL en BiSL.

Over gebruikersvragen en gemelde problemen, fouten en instellingen vermeldt de SLA specifiek afspraken over prioriteit, reactietijd en oplostijden:

- Een gebruikersvraag is een vraag van een gebruiker van het dataplatform over hoe met de applicatie te werken. Bijvoorbeeld vragen als 'Waar kan ik...?' of 'Hoe doe ik...?'. Gebruikersvragen gaan niet over fouten in de applicatie en/of het doen van instellingen;
 - Prioriteit: laag
 - Reactietijd SLA: zo snel mogelijk, uiterlijk binnen 24 uur;
 - Oplostijd SLA: zo snel mogelijk, maar uiterlijk binnen 24 uur;
- Niet-blokkerende fout: een fout die optreedt in een deel van het dataplatform of in een koppeling met een andere applicatie, niet blokkerend, maar hinderlijk voor het uitvoeren van het werkproces van een groot deel van de gebruikers;
 - Prioriteit: middel
 - Reactietijd SLA: zo snel mogelijk, uiterlijk binnen 24 uur;
 - Oplostijd SLA: zodra releaseplanning leverancier dit toelaat, uiterlijk binnen 6 weken;
- Urgente fout: een fout in het dataplatform of in een koppeling met een andere applicatie waardoor het niet mogelijk is om de primaire functionaliteit uit te voeren. Bijvoorbeeld: het dataplatform is offline, pagina werkt niet, functionaliteit is niet beschikbaar;
 - Prioriteit: hoog
 - Reactietijd SLA: zo snel mogelijk, uiterlijk binnen 3 uur;
 - Oplostijd SLA: zo snel mogelijk, uiterlijk 8 uur, tenzij oplostijd afhankelijk is van externe partij, bijvoorbeeld de goedkeuring van een nieuwe release door Apple en/of Google playstore;
- Wens/idee: een verzoek van een gebruiker voor aanpassing van het dataplatform;
 - Prioriteit: laag
 - Reactietijd SLA: zo snel mogelijk, uiterlijk binnen 2 dagen;
 - Oplostijd SLA: niet van toepassing;
- Urgente instelling: een verzoek van een gebruiker voor instelling van het dataplatform die nodig is om ermee te kunnen werken. Bijvoorbeeld: gebruikers toevoegen. Gedurende het project worden hierover afspraken gemaakt door opdrachtgever in overleg met betrokken partijen.

- Prioriteit: hoog
- Reactietijd SLA: zo snel mogelijk, uiterlijk binnen 3 uur;
- Oplostijd SLA: zo snel mogelijk, uiterlijk 3 uur.