Bijlage 1 – Programma van Eisen

Het Programma van Eisen vormt een bijlage bij het Beschrijvend document voor de Europese aanbesteding ‘Thesaurusbeheersysteem’ van de KB. Het Programma van Eisen betreft enkel eisen aan de uitvoering van de Opdracht.

De met hoofdletter geschreven woorden refereren naar de definities zoals opgenomen in het “Beschrijvend Document”.

Inhoudsopgave

1 ALGEMENE EISEN 2

2. OPLOSSING 2

3. BEHEER METADATA TERMEN 3

4. VALIDATIE METADATA TERMEN 5

5. ZOEKEN EN NAVIGEREN 5

6. WORKFLOW EN SAMENWERKEN 6

7. KOPPELVLAK 6

8. TOEGANKELIJKHEID 7

9. AUTHENTICATIE EN AUTORISATIE 8

10. SCHAALBAARHEID EN PERFORMANCE 10

11. SECURITY 11

12. SERVICEMANAGEMENT 22

13. SLA 27

14. DAP 32

15. EXIT 32

16. PRIVACY 34

17. FACTURATIE 35

1	Algemene eisen	
E 1.1.	Taal	Alle communicatie, documenten en correspondentie in het kader van deze Opdracht en de Nadere Opdrachten moeten in de Nederlandse of Engelse taal worden gevoerd en/of opgesteld.
E 1.2.	Vast contactper-soon	Opdrachtnemer stelt, ten behoeve van alle zaken met betrekking tot de uitvoering van de Opdracht één vaste contactpersoon beschikbaar voor de gehele duur van de Opdracht en meldt een wijziging daarvan uiterlijk 10 werkdagen vooraf aan de KB. Deze persoon beheerst uitstekend de Nederlandse taal in woord en geschrift.
E 1.3.	Bereikbaarheid	Opdrachtnemer is voor de KB telefonisch en per e-mail bereikbaar op werkdagen tussen 08:00 uur en 18:00 uur.
E 1.4.	Professionele aanpak	Opdrachtnemer brengt de KB, zodra Opdrachtnemer weet of behoort te weten dat de nakoming van de Opdracht niet of niet tijdig of niet naar behoren plaatsvindt, onmiddellijk schriftelijk én telefonisch op de hoogte onder vermelding van de omstandigheden.
E 1.5.	Communicatie-uitingen	Opdrachtnemer zal geen communicatie-uitingen doen over de Raamovereenkomst of de relatie met de KB zonder schriftelijke toestemming van de KB.
E 1.6.	Voorwaarden	De algemene en/of verkoopvoorwaarden van de Inschrijver worden nadrukkelijk van de hand gewezen. In de Inschrijving van de Inschrijver wordt niet (deels) naar andere juridische voorwaarden verwezen

2.	Oplossing	
E 2.1.	SaaS	De geboden Oplossing moet een integrale webbased SaaS (Software as a Service) Oplossing zijn voor de beschreven functionaliteiten.
E 2.2.	Standaard-programmatuur	De software waarop de Oplossing is gebaseerd betreft standaardprogrammatuur: voor algemeen gebruik ontwikkelde Programmatuur die niet exclusief aan de KB beschikbaar wordt gesteld. Opdrachtnemer dient geen Maatwerk te ontwikkelen om de gewenste functionaliteit te bieden. Hiervan kan eventueel bij

		dringende noodzaak en in overleg met de KB afgeweken worden, bijvoorbeeld voor het inlezen van een bijzonder dataformaat.
E 2.3.	Bestaande programmatuur	Opdrachtnemer biedt, gedurende de contractperiode, altijd de meest actuele ondersteunde versie (ingevoerd volgens de afgesproken releaseprocedure) van de Oplossing aan, waarbij deze de werking van alle functionaliteiten garandeert. Inschrijven op basis van toekomstige releases is niet toegestaan.
E 2.4.	Dienstverlening	Opdrachtnemer is vanuit het oogpunt van de KB verantwoordelijk voor de gehele Oplossing. Als er gebruik wordt gemaakt van dienstverlening van derden (bijvoorbeeld voor datacenterdienstverlening of trainingen/opleidingen) is Opdrachtnemer alsnog het aanspreekpunt en kan er niet worden doorverwezen naar derden.

3. Beheer metadata termen

E 3.1.	Meerdere thesauri	De Oplossing biedt ondersteuning voor meerdere thesauri met verschillende datamodellen in één omgeving.
E 3.2.	Migratie identifiers	Op het moment van migratie is de mapping tussen 'oude' identifiers en de (persistente) identifiers in de Oplossing bevroren. Deze mapping tussen de oude identifiers (zoals PPN voor de NTA) en nieuwe identifiers wordt bewaard en beheerd in deze Oplossing. Zodanig dat ook met oude identifiers kan worden gezocht bijvoorbeeld om de vertaling van oude naar nieuwe identifiers te kunnen maken.
E 3.3.	RDF	De metamodel van de Oplossing is gebaseerd op de RDF (Resource Description Framework) standaard.
E 3.4.	Termbeheer	De Oplossing ondersteunt het aanmaken, wijzigen en verwijderen van termen.
E 3.5.	Configuratie velden	De beheerder heeft de mogelijkheid om de velden per terminologiebron te configureren.
E 3.6.	Verplichte velden	Het is mogelijk om verplichte velden per terminologiebron te definiëren.
E 3.7.	Samenvoegen	Het is mogelijk om twee termen samen te voegen. De Oplossing zorgt ervoor dat de persistente *identifier* van de vervallen term verwijst naar de persistente *identifier* van de aangehouden term.
E 3.8.	Hiërarchische relaties	De Oplossing ondersteunt hiërarchische relaties (BT/NT), het leggen van relaties naar bredere en nauwere termen.

3. Beheer metadata termen

E 3.9.	Polyhiërarchie	De Oplossing ondersteunt meerdere bredere termen voor één term.
E 3.10.	Equivalente relaties	De Oplossing ondersteunt equivalente relaties (USE/UF), het definiëren van voorkeursterm en niet-voorkeurstermen (synoniemen).
E 3.11.	Associatieve relaties	De Oplossing ondersteunt associatieve (RT/RT) relaties, het leggen van relaties naar gerelateerde termen.
E 3.12.	Wederkerigheid	De Oplossing ondersteunt automatische wederkerigheid van relaties.
E 3.13.	Eigen relaties	Het is mogelijk om zelf gedefinieerde wederkerige relaties tussen de termen te leggen.
E 3.14.	Onbeperkte relaties	Er bestaat geen beperking voor het aantal relaties voor een term.
E 3.15.	Verborgen termen	De Oplossing biedt de mogelijkheid om bepaalde termen te verbergen, maar nog wel vindbaar te houden.
E 3.16.	Verborgen velden	De Oplossing biedt de mogelijkheid om op recordniveau handmatig specifieke velden (zoals een geboortejaar) af te schermen, zodat deze velden uitsluitend zichtbaar zijn voor interne systeemgebruikers en verborgen blijven bij het publiceren van records.
E 3.17.	"Kapstokterm"	Het is mogelijk om bepaalde termen als kapstokterm te markeren. Een kapstokterm (*guide term* in AAT, *node label* in ISO 25964) dient als verzamelterm om onderliggende, specifiekere termen logisch te groeperen en wordt zelf niet gebruikt om te catalogiseren.
E 3.18.	Categorieën	Het is mogelijk om termen te groeperen op basis van een kenmerk.
E 3.19.	Scope notes	Het is mogelijk om scope notes toe te voegen bij een term.
E 3.20.	Interne notitie	Het is mogelijk om een interne notitie te plaatsen bij een term.
E 3.21.	Termgeschiedenis	De Oplossing biedt de mogelijkheid om geschiedenis van de term vast te leggen, conform skos:historyNote.
E 3.22.	Identifiers	Het is mogelijk om *persistent identifiers* uit verschillende terminologiebronnen bij een term vast te leggen.
E 3.23.	Unicode standaard	De Oplossing kan alle tekens uit de Unicode-standaard correct opslaan, indexeren, doorzoeken en weergeven.
E 3.24.	Tekstrichtingen	De beheerinterface ondersteunt invoer en weergave van beide tekstrichtingen.
E 3.25.	Hyperlinks	In de beheerinterface zijn opgenomen hyperlinks klikbaar.

4. Validatie metadata termen

E 4.1.	Eén voorkeursterm	Er is alleen één voorkeursterm per taallabel toegestaan.
E 4.2.	Dubbelingen	De Oplossing heeft de mogelijkheid om dubbel ingevoerde termen te signaleren.
E 4.3.	Circulaire verwijzingen	De Oplossing staat circulaire verwijzingen niet toe.
E 4.4.	Exclusieve relaties	De Oplossing staat niet toe dat twee termen tegelijkertijd een hiërarchische (BT/NT) én een associatieve (RT) relatie met elkaar hebben.
E 4.5.	Propagatie	De Oplossing voert het wijzigen of verwijderen van een term door op alle relaties van de betreffende term binnen de terminologiebron.

5. Zoeken en navigeren

E 5.1.	Zoekfunctionaliteit	De Oplossing biedt de mogelijkheid om te kunnen zoeken op alle metadata en meta-metadata velden.
E 5.2.	*Wildcards*	De Oplossing biedt de mogelijkheid om te zoeken met jokertekens (*wildcards*).
E 5.3.	Operatoren	De Oplossing biedt de mogelijkheid om te zoeken met Booleaanse operatoren.
E 5.4.	*Auto-completion*	Tijdens het typen in een zoekveld vult de Oplossing automatisch de zoekvraag aan op basis van zowel voorkeurstermen als synoniemen.
E 5.5.	Sorteren	De Oplossing sorteert de gevonden termen op basis van relevantie: de termen die de zoekvraag waarschijnlijk het beste beantwoorden worden als eerste teruggegeven.
E 5.6.	Filteren	De Oplossing ondersteunt het filteren van zoekresultaten.
E 5.7.	Zoekresultaat	Bij het weergeven van een zoekresultaat toont de Oplossing ook de onderliggende en gerelateerde termen.
E 5.8.	Hiërarchie inzichtelijk	De Oplossing geeft inzichtelijk de hiërarchische context van een term weer, inclusief de gerelateerde termen.
E 5.9.	Bladeren	Het is mogelijk te bladeren door de terminologiebron.

6. Workflow en samenwerken

E 6.1.	Workflow	De Oplossing ondersteunt de inrichting van een workflow voor het beheren van een thesaurus, ook wanneer deze gezamenlijk beheerd wordt met netwerkpartners.
E 6.2.	Configuraties	De Oplossing ondersteunt verschillende workflow configuraties per terminologiebron.
E 6.3.	Rollen	De workflow-inrichting sluit aan bij de rollen zoals die in rolgebaseerde toegang (RBAC, zijn gedefinieerd. Minimaal de volgende rollen worden ondersteund: raadpleger, editor, reviewer en administrator
E 6.4.	Levenscyclus	De Oplossing ondersteunt een redactionele workflow met minimaal de volgende statussen: voorgesteld, goedgekeurd, afgekeurd, gepubliceerd en vervallen.
E 6.5.	Concurrency	De Oplossing biedt een mechanisme om conflicterende updates te voorkomen.
E 6.6.	Audit trail	De Oplossing logt elke mutatie met tijdstempel, gebruikers-ID en de wijziging.
E 6.7.	Versieherstel	Het is mogelijk om een eerdere versie van een term terug te zetten.

7. Koppelvlak

E 7.1.	API	De Oplossing beschikt over een goed gedocumenteerde, volledig functionele op REST gebaseerde API die de te koppelen systemen kunnen gebruiken om toegang te krijgen tot alle functionaliteit van de (backend) van de Oplossing
E 7.2.	OAI-PMH	De Oplossing heeft een OAI-PMH-interface waarmee een volledige termenset geharvest kan worden, volledig en incrementeel (volgens de gangbare werkwijze met behulp van *resumption tokens*).
E 7.3.	REST Harvesting	De REST-API biedt dezelfde harvest-functionaliteit als die OAI-PMH-interface ook aan, dus met ondersteuning voor incrementele harvesting en een schaalbare paginering.
E 7.4.	Update-notificaties	De Oplossing biedt voorzieningen waarmee nieuw toegevoegde of gewijzigde termen zo snel mogelijk in meerdere, vooraf niet gekende, catalogiseersystemen beschikbaar is. Dit kan bijvoorbeeld gerealiseerd zijn via een *pub-sub* voorziening of een *observer-pattern*.

7. Koppelvlak

E 7.5.	Gebruik van *persistente identifiers*	De Oplossing ondersteunt *persistente identifiers* voor een nieuwe term. Het beoogde systeem moet deze *identifiers* ook kunnen gebruiken als ingang voor het opvragen van de data via de API en andere interfaces. In de API willen we met deze *identifier* de resource kunnen opvragen.
E 7.6.	Uitgeven van *persistente identifiers*	De Oplossing is in staat om voor het toekennen van 'persistent identifiers' gebruik te maken van een externe dienst voor het 'munten' van die *persistente identifiers*.
E 7.7.	*Persistente Identifiers*	Data die buiten de Oplossing wordt gepubliceerd maakt gebruik van toegekende *persistente identifiers*, zodat de afhankelijkheid voor door de Oplossing gegenereerde systeemidentifiers wordt geminimaliseerd.
E 7.8.	Import	De Oplossing ondersteunt het importeren van gangbare representaties van RDF, zoals RDF-XML, JSON-LD en Turtle.
E 7.9.	Import van MARCXML	De Oplossing ondersteunt het importeren van MARCXML.
E 7.10.	Export	De Oplossing ondersteunt het exporteren naar de gangbare representaties van RDF, zoals RDF-XML, JSON-LD en Turtle.
E 7.11.	Export naar MARCXML	De Oplossing ondersteunt het exporteren naar MARCXML.
E 7.12.	Bulk edits	De Oplossing ondersteunt bulk wijzigingen van thesaurirecords.

8. Toegankelijkheid

E 8.1.	Intuïtief	De Oplossing werkt intuïtief voor niet-technische gebruikers.
E 8.2.	Visualisatie	De Oplossing heeft de mogelijkheid om termrelaties te visualiseren.
E 8.3.	Handleiding	Er is een gebruikershandleiding beschikbaar.
E 8.4.	Helpfunctie	Er is een contextuele helpfunctie beschikbaar.
E 8.5.	Webapplicatie	De Oplossing ondersteunt de gangbare browsers voor de user-interface, is gebaseerd op webstandaarden en niet op browser-specifieke mogelijkheden

8. Toegankelijkheid

E 8.6.	Digitale toegankelijkheid - WCAG	De dienst die door Opdrachtnemer wordt geleverd, wordt digitaal toegankelijk by design ontwikkeld. De dienst voldoet aantoonbaar aan de eisen voor digitale toegankelijkheid zoals omschreven in de Europese standaard EN 301 549 (meest recente versie), waarvan de internationale richtlijnen voor toegankelijkheid, de Web Content Accessibility Guidelines (WCAG), deel uitmaken. De dienst is ontwikkeld volgens de meest recente WCAG-richtlijnen, niveau A en AA.
E 8.7.	Digitale toegankelijkheid - WCAG-EM	Opdrachtnemer levert bij oplevering een audit rapport waaruit blijkt dat getest is volgens een betrouwbare evaluatiemethode: WCAG-EM of een gelijkwaardige methode. Indien Opdrachtnemer niet volledig voldoet aan alle punten, dan garandeert Opdrachtnemer door het akkoord gaan met deze eis dat binnen het eerste jaar van de overeenkomst volledig zal worden voldaan aan de gestelde toegankelijkheidseisen.
E 8.8.	Digitale toegankelijkheid - Auditrapport	Iedere 3 jaar levert de leverancier opnieuw een auditrapport volgens de WCAG-EM. Leverancier rapporteert minimaal halfjaarlijks over de oplostermijn en implementatie van de resterende geaccepteerde verbeterpunten, en over eventuele nieuwe verbeterpunten na uitbreiding van de dienst.

9. Authenticatie en autorisatie

E 9.1.	Authenticatie	De Oplossing authenticeert gebruikers van netwerkpartners van de KB uitsluitend via de centrale authenticatievoorziening van de KB (EenLogin), die als Identity Provider (IdP) fungeert.
E 9.2.	Authenticatie	De Oplossing ondersteunt koppeling met de IdP via OpenID Connect 1.0 of SAML 2.0, conform de authenticatie-standaarden op de comply or explain van Forum Standaardisatie (OpenID.NLGov / SAML).
E 9.3.	Authenticatie	Alle IdP-instellingen (onder andere issuer/metadata-URL, client-ID, client-credentials, scopes, logout-URL) zijn configureerbaar zonder codewijziging.
E 9.4.	Authenticatie	De Oplossing ondersteunt OIDC Discovery (/.well-known/openid-configuration) en/of SAML-metadata.
E 9.5.	Authenticatie	De Oplossing dwingt geen eigen, aanvullende MFA af voor gebruikers die via de IdP zijn geauthenticeerd. MFA wordt door de IdP uitgevoerd.

9. Authenticatie en autorisatie

E 9.6.	Protocol- en tokenbeveiliging	De Oplossing ondersteunt (automatische) sleutelrotatie (*key rollover*) van de IdP door de *signing keys* periodiek uit de JWKS- of metadata-URL op te halen. Er worden geen certificaten of sleutels hard gecodeerd.
E 9.7.	Protocol- en tokenbeveiliging	De Oplossing ondersteunt sleutelrotaties via het PKCE-proces. Er worden geen *client secrets* uitgedeeld.
E 9.8.	Identiteit, gegevens en autorisatie	De Oplossing biedt role-based access control (RBAC) dat door functioneel beheerders van de KB zelf wordt uitgevoerd. In de Oplossing worden rollen gekoppeld aan de via EenLogin geauthenticeerde identiteit.
E 9.9.	Identiteit, gegevens en autorisatie	Alle communicatie tussen browser, Oplossing en IdP verloopt via TLS conform de actuele ICT-beveiligingsrichtlijnen voor TLS van het NCSC. Redirect-URI's zijn exacte HTTPS-URL's zonder wildcards.
E 9.10.	Sessies en levenscyclus van gebruikersaccounts	De applicatiesessie van de Oplossing kent een configureerbare *inactivity time-out* en een configureerbare maximale sessieduur. Na afloop moet de gebruiker opnieuw via EenLogin authenticeren. De sessieduur is standaard niet langer dan 9 uur.
E 9.11.	Sessies en levenscyclus van gebruikersaccounts	De Oplossing verwijdert automatisch gebruikersaccounts die gedurende een configureerbare periode, met een maximum van het aantal dagen dat de IdP zelf hanteert) niet succesvol hebben geauthenticeerd. Hierover is een rapportage beschikbaar voor functioneel beheer van de KB.
E 9.12.	Sessies en levenscyclus van gebruikersaccounts	Een functioneel beheerder van de KB kan een gebruiker direct blokkeren. Actieve sessies van die gebruiker worden daarbij binnen specifieke en configureerbare tijd beëindigd.
E 9.13.	Sessies en levenscyclus van gebruikersaccounts	Functioneel beheer van de KB kan een overzicht exporteren van alle gebruikers met hun rollen, organisatie en datum van laatste aanmelding, ten behoeve van periodieke autorisatiereview.
E 9.14.	Gebruikerservaring	De aanmeldpagina van de Oplossing leidt de gebruiker direct (of via één duidelijke knop "Inloggen met EenLogin") door naar EenLogin, in het Nederlands en zonder alternatieve aanmeldopties voor reguliere gebruikers.

9. Authenticatie en autorisatie

E 9.15.	Gebruikerservaring	Bij fouten in de authenticatieketen (zoals IdP niet bereikbaar, geweigerd token, gebruiker zonder rechten) toont de Oplossing een begrijpelijke foutmelding met correlatie-ID en valt de Oplossing niet terug op een alternatieve authenticatiemethode.
E 9.16.	Aansluiting en wijzigingen	Inschrijver ondersteunt wijzigingen in de IdP-koppeling die voortkomen uit wijzigingen aan de kant van de KB (onder meer migratie van EenLogin naar een ander platform, nieuwe endpoints, nieuwe claims en/of nieuwe certificaten) binnen 8 weken (of anders, als anders overeengekomen) na verzoek, als onderdeel van de reguliere (onderhouds)vergoeding.

10. Schaalbaarheid en performance

E 10.1.	Schaalbaarheid publicatie	De publicatiefunctie van de Oplossing (het uitsluitend lezend raadplegen van gegevens vanuit afnemende systemen en eventuele publieksinterface) is horizontaal schaalbaar zonder architecturale bovengrens.
E 10.2.	Schaalbaarheid data-omvang	De Oplossing schaalt, met behoud van performance, tot een data-omvang van ordegrootte 10-tallen miljoenen records.
E 10.3.	Backup	De Oplossing biedt voldoende backup-mogelijkheden, ook naar externe locaties, zodat de KB steeds kan beschikken over een volledig bijgewerkte kopie (in lijn met eis E11.54) van alle opgeslagen data op een locatie die leveranciers-onafhankelijk toegankelijk is.
E 10.4.	Responstijd	De userinterface heeft een responsetijd van maximaal 400 milliseconden voor een gebruikersactie. Wanneer dat inherent niet mogelijk is, bijvoorbeeld bij langdurende zoekopdrachten, grote exports en rapportages, dan biedt de Oplossing een betekenisvolle voortgangsindicator

11. Security		
E 11.1.	Security governance	Opdrachtnemer stelt één centraal aanspreekpunt aan voor informatiebeveiliging. Opdrachtnemer zorgt dat de KB te allen tijde beschikt over de contactgegevens (minimaal: email-adres en telefoonnummer) voor het centrale aanspreekpunt. Opdrachtnemer geeft wijzigingen in deze contactgegevens tijdig door.
E 11.2.	Compliance & audit	Opdrachtnemer beschikt over, dan wel levert na 1 jaar na inbeheername van de Oplossing, een onafhankelijke Service Organization Control (SOC) 2 Type 2 dan wel SOC 3 rapportage of een ISAE 3402 type II verklaring om aan te tonen in control te zijn. De rapportage of verklaring omvat de dienstverlening die aan De KB wordt geleverd. De rapportage of verklaring toont aan dat Opdrachtnemer aan alle eisen voldoet in opzet, bestaan en werking. Hierbij is expliciet aandacht voor de toeleveringsketen en hoe de Opdrachtnemer zijn Opdrachtnemersmanagement heeft ingeregeld. Opdrachtnemer zorgt ervoor dat de Assurance-verklaring onderhouden wordt en kan dit jaarlijks aantonen.
E 11.3.	Compliance & audit	De KB heeft het recht om periodiek bij Opdrachtnemer een (onafhankelijke) audit uit te (laten) voeren naar de opzet, het bestaan en de werking van privacy- en informatiebeveiligingsmaatregelen. Opdrachtnemer gaat akkoord met een audit door een medewerker van de KB of een door de KB ingehuurd accountants- of onderzoeksbureau. Opdrachtnemer werkt hier volledig aan mee, onder meer door gevraagde documentatie aan te leveren en toegang te verlenen tot de gegevensbestanden en systemen waarbinnen de gegevens verwerkt worden. Opdrachtnemer heeft de mogelijkheid om een audit rapport van een onafhankelijke 3rd-party auditor te overleggen.

11. Security		
E 11.4.	Keten van toeleveranciers	Opdrachtnemer houdt een overzicht bij van zijn keten van toeleveranciers. Voorgaand aan het afsluiten van de overeenkomst geeft de opdrachtnemer een initieel overzicht en de eventuele risico's daarin. De KB beoordeelt of de risico's acceptabel zijn. Veranderingen in de keten, inclusief de risico's daarin, worden gedurende de looptijd doorgegeven aan de KB. Dit omvat minimaal kwetsbaarheden en informatiebeveiligingsincidenten die de dienstverlening aan de KB kunnen raken.
E 11.5.	Keten van toeleveranciers	De Opdrachtnemer zorgt dat de eisen, inclusief exit-eisen, onverminderd van toepassing zijn op de keten van toeleveranciers, tenzij die eisen niet relevant zijn gezien de aard van de dienstverlening door de toeleverancier. Als specifieke eisen zijn uitgesloten, maakt de Opdrachtnemer dat inzichtelijk, inclusief een onderbouwing.
E 11.6.	Web Application Firewall	Opdrachtnemer implementeert een Web Application Firewall (WAF) voor alle internet-facing endpoints van de applicatie en alle bijbgehorende API's. De WAF is geconfigureerd om kwaadaardige pogingen te blokkeren én te registreren. De WAF maakt gebruik van een adequate configuratie om veelvoorkomende aanvallen op applicatieniveau te blokkeren.
E 11.7.	Veilige softwareontwikkeling	Opdrachtnemer past aantoonbaar de preventieve maatregelen zoals beschreven in de meest recente OWASP Top 10 'by design' toe tijdens het softwareontwikkelproces. Indien er gedurende het ontwikkeltraject een recentere versie door OWASP wordt gepubliceerd, borgt de Opdrachtnemer dat te allen tijde de meest recente versie van de OWASP Top 10 aantoonbaar wordt toegepast in haar ontwikkelproces.
E 11.8.	Veilige softwareontwikkeling	Opdrachtnemer maakt gebruik van een veilige code repository. De code repository beschermt broncode ten minste tegen ongeautoriseerde toegang, wijzigingen of het verwijderen van broncode. De code repository beschikt daarnaast over versionering en mogelijkheden de code te scannen op kwetsbaarheden.
E 11.9.	Veilige softwareontwikkeling	Opdrachtnemer scant broncode tijdens de ontwikkelcyclus regelmatig op kwetsbaarheden. Hierbij wordt gebruikgemaakt van ten minste een Static Application Security Testing (SAST) tool.

11. Security		
E 11.10.	Veilige softwareontwikkeling	Opdrachtnemer zorgt ervoor dat wijzigingen in broncode te allen tijde worden gereviewd middels een peer-review. Broncode mag slechts worden gepubliceerd naar productie na toepassen van het vierogenprincipe.
E 11.11.	Scheiding	Opdrachtnemer zorgt ervoor dat er minimaal een virtuele scheiding aanwezig is tussen de (productie)omgeving van de KB en andere (klant)omgevingen.
E 11.12.	Scheiding	Opdrachtnemer zorgt ervoor dat de gegevens van de KB tijdens transport, bewerking en opslag duurzaam geïsoleerd zijn van beheerfuncties en anderen die gebruikmaken van dezelfde infrastructuur. Opdrachtnemer voorkomt dat de KB performance hinder ondervindt bij eventueel inzet van gedeelde componenten.
E 11.13.	Cookies	Waar in de Oplossing gebruik wordt gemaakt van cookies dienen deze voorzien te zijn van de 'secure' en 'httponly' flags. Tevens bevatten cookies geen persoonlijke informatie en vindt de uitwisseling altijd via een beveiligde verbinding (HTTPS) plaats. De Oplossing is vrij van tracking cookies.
E 11.14.	Beveiligingstesten & het verhelpen van kwetsbaarheden	Minimaal eens per jaar worden alle webapplicaties in scope van de dienstverlening onderworpen aan een penetratietest uitgevoerd door een gekwalificeerde externe partij. Opdrachtnemer stelt op verzoek van de KB de rapportage van de penetratietest beschikbaar.
E 11.15.	Beveiligingstesten & het verhelpen van kwetsbaarheden	Minimaal eens per jaar worden alle API's in scope van de dienstverlening onderworpen aan een penetratietest uitgevoerd door een gekwalificeerde externe partij. Opdrachtnemer stelt op verzoek van de KB de rapportage van de penetratietest beschikbaar.
E 11.16.	Beveiligingstesten & het verhelpen van kwetsbaarheden	Minimaal eens per kwartaal wordt de digitale infrastructuur van de Oplossing gecontroleerd door Opdrachtnemer op zwakheden door middel van een vulnerability scan. Opdrachtnemer stelt op verzoek van de KB de rapportage van de vulnerability scan beschikbaar.

11. Security		
E 11.17.	Beveiligingstesten & het verhelpen van kwetsbaarheden	Opdrachtnemer zorgt dat kwetsbaarheden zoals geïdentificeerd via een vulnerability scan (of via een ander medium) tijdig worden verholpen aan de hand van een door de KB geaccordeerd verbeterplan. Voor het oplossen van kwetsbaarheden worden geen aanvullende kosten in rekening gebracht door Opdrachtnemer.
E 11.18.	Beveiligingstesten & het verhelpen van kwetsbaarheden	Geïdentificeerde kwetsbaarheden met een prioriteit 'Hoog' zoals aangegeven door het Nationaal Cyber Security Centrum (NCSC) of een CVSS v4 score van 9 of hoger worden onmiddellijk na constatering door opdrachtnemer of na melding door de KB, door de Opdrachtnemer verholpen conform het beveiligingsadvies van het NCSC of de Opdrachtnemer.
E 11.19.	Beveiligingstesten & het verhelpen van kwetsbaarheden	Opdrachtnemer rapporteert maandelijks (zie E 13.11.) over de staat van kwetsbaarheden van toepassing op alle Componenten gebruikt voor het leveren van de Oplossing. De rapportage omvat minimaal het aantal kwetsbaarheden, type kwetsbaarheid, component waarop de kwetsbaarheid van toepassing is, de CVE-code, CVSS-score en de status van het toepassen van mitigerende maatregelen.
E 11.20.	API-beveiliging	Opdrachtnemer past aantoonbaar de preventieve maatregelen zoals beschreven in de meest recente OWASP Top 10 API Security Risks (versie 2023) 'by design' toe tijdens het ontwikkelproces. Indien er gedurende het ontwikkeltraject een recentere versie door OWASP wordt gepubliceerd, borgt de Opdrachtnemer dat te allen tijde de meest recente versie van de OWASP Top 10 API Security Risks aantoonbaar wordt toegepast in haar ontwikkelproces.
E 11.21.	API-beveiliging	Opdrachtnemer beveiligt alle API's in overeenstemming met de OWASP REST Security Cheat Sheet of de OWASP GraphQL Cheat Sheet.
E 11.22.	API-beveiliging	Opdrachtnemer zorgt dat alle API's worden voorzien van sterke authenticatie en autorisatie. Het Oauth 2.0 autorisatie framework wordt bij voorkeur ondersteund.
E 11.23.	Endpoint-beveiliging	Opdrachtnemer zorgt dat alle internet-facing endpoints, inclusief API's, worden beschermd tegen overbelasting, brute-force-aanvallen en enumeratie, door het toepassen van rate limiting en throttling.

11. Security		
E 11.24.	API-beveiliging	Het gebruik van API-gateways en validatiemechanismen is verplicht om injectieaanvallen te voorkomen en veilige communicatie te waarborgen.
E 11.25.	API-beveiliging	Voor API's die niet op basis van het OAuth 2.0 autorisatie framework worden beschermd en waarbij er sprake is van voorspelbare afnemers (de API is slechts voor een voorspelbare groep systemen of gebruikers bedoeld), dient de toegang tot de API te worden beperkt door middel van IP-whitelisting. Hiermee wordt het aanvalsvlak beperkt door ongeautoriseerde toegang te minimaliseren, ook wanneer een API-sleutel is gecompromitteerd.
E 11.26.	API-beveiliging	Opdrachtnemer zorgt dat API keys op een veilige wijze worden beheerd en opgeslagen. De volgende eisen zijn hierop van toepassing: - API keys worden op een veilige manier gegenereerd, bij voorkeur in een passende beveiligde omgeving; - API keys worden versleuteld bewaard; - API keys worden bewaard en beheerd in beveiligde omgeving (zoals Azure Key Vault, AWS Secrets Manager, of vergelijkbaar). API keys worden nooit hard-coded in broncode of configuratiebestanden bewaard; - API keys worden voorzien van een key rotation policy. Alle keys worden voorzien van een vervaldatum om te voorkomen dat deze niet oneindig gebruikt kunnen worden. Nieuwe keys worden gegenereerd zodra de oude keys verlopen; - Er is een mechanisme waarmee API keys onmiddellijk kunnen worden ingetrokken zodra ze gecompromitteerd of niet langer nodig zijn; - Gebruik van API keys wordt gelogd, zodat ongeautoriseerd gebruik of misbruik kan worden gedetecteerd. Automatische waarschuwingen worden ingesteld om misbruik tijdig te detecteren.

11. Security		
E 11.27.	Hardening	Componenten waaruit de Oplossing bestaat (zoals maar niet beperkt tot (Cloud)platforms, hypervisors, containerplatforms, (besturings)systemen, database platforms, (virtuele) servers) dienen door Opdrachtnemer afdoende te zijn gehardened aan de hand van CIS benchmarks of vergelijkbare voorschriften van de fabrikant (aan de hand van het comply or explain principe).
E 11.28.	Hardening	Opdrachtnemer rapporteert maandelijks (zie E 13.11.) over de staat van compliance op het gebied van hardening aan de hand van CIS benchmarks of vergelijkbare voorschriften van de fabrikant (op basis van het comply or explain principe).
E 11.29.	Patchmanagement	De Opdrachtnemer dient conform een gedocumenteerd Patch Management beleid en proces met een passende frequentie alle bij de Oplossing betrokken ICT-componenten (inclusief firmware, besturingssystemen en applicaties) tijdig te voorzien van de laatste (beveiligings-)patches en updates. Voorafgaand aan het toepassen van een update of patch worden de implementatierisico's beoordeeld. Updates of patches worden eerst getest in een niet-productieomgeving alvorens deze worden toegepast in een productieomgeving. Security patches of hotfixes om kwetsbaarheden met een prioriteit 'Hoog' zoals aangegeven door het Nationaal Cyber Security Centrum (NCSC) of een CVSS v4 score van 9 of hoger worden onmiddellijk toegepast door de Opdrachtnemer conform het beveiligingsadvies van het NCSC of de Opdrachtnemer. Opdrachtnemer dient indien geen (beveiligings-)patch c.q. update beschikbaar is gepaste mitigerende maatregelen te implementeren opdat het restrisico tot een acceptabel niveau wordt teruggebracht.
E 11.30.	Patchmanagement	Opdrachtnemer draagt zorg dat een lifecycle management proces is gedocumenteerd en geïmplementeerd voor alle componenten waaruit de Oplossing bestaat. Het lifecycle management proces omvat in elk hoe Opdrachtnemer de beveiliging en juiste werking van IT-componenten waarborgt gedurende de levenscyclus ieder component. Het doel is om beveiligingsrisico's voortkomend uit verouderde of niet langer ondersteunde hard- of software te voorkomen.

11. Security		
E 11.31.	Patchmanagement	Opdrachtnemer borgt dat uitsluitend gebruik wordt gemaakt van hard- en softwarecomponenten die actief door de leverancier van deze componenten worden ondersteund.
E 11.32.	Patchmanagement	Opdrachtnemer rapporteert jaarlijks over het patchniveau van alle Componenten gebruikt voor het leveren van de Oplossing. Opdrachtnemer informeert de KB tijdig indien één of meerdere Componenten 'out of support' of 'end of life' raken.
E 11.33.	Training en bewustwording	Opdrachtnemer zorgt dat alle medewerkers met toegang tot faciliteiten waar gegevens van de KB worden verwerkt zijn getraind op het gebied van informatiebeveiliging en zich houden aan de gedragscode van de KB.
E 11.34.	Toegangsbeveiliging	Opdrachtnemer houdt bij welke personen namens Opdrachtnemer toegang hebben tot de Oplossing en kan op verzoek van de KB een overzicht hiervan verschaffen aan de KB.
E 11.35.	Toegangsbeveiliging	Opdrachtnemer borgt dat medewerkers van Opdrachtnemer zich uitsluitend kunnen authenticeren bij onderdelen van de Oplossing met behulp van Single Sign On (SSO) die loopt via de authenticatie management oplossing van de KB. Toegang tot het informatiesysteem is uitsluitend mogelijk na succesvolle login en Multi Factor Authenticatie (MFA).
E 11.36.	Toegangsbeveiliging	Opdrachtnemer zorgt ervoor dat wachtwoorden die ten behoeve van het informatiesysteem worden opgeslagen, welke niet worden beheerd binnen de authenticatie management Oplossing van de KB, op adequate en actuele wijze worden versleuteld. De versleutelde opslag maakt uitsluitend gebruik van adequate encryptiestandaarden naar de stand van de techniek.
E 11.37.	Toegangsbeveiliging	Opdrachtnemer borgt dat meerfactorauthenticatie wordt afgedwongen voor alle internet-facing inlogportalen. Uitzonderingen worden uitsluitend tijdelijk toegestaan na een schriftelijke motivatie van Opdrachtnemer en goedkeuring van de KB.

11. Security		
E 11.38.	Toegangsbeveiliging	Opdrachtnemer zorgt voor een sterk proces voor het aanvragen, wijzigen en wegnemen van toegangsrechten voor medewerkers die toegang nodig hebben tot broncode of infrastructuur voor het informatiesysteem. Opdrachtnemer zorgt te allen tijde dat de toegang tot onderdelen van het informatiesysteem wordt weggenomen voor medewerkers die geen toegang meer nodig hebben tot onderdelen van het informatiesysteem.
E 11.39.	Toegangsbeveiliging	Secrets, zoals gebruikt voor authenticatie, certificaten en encryptie, worden veilig bewaard in een 'key vault' of vergelijkbare toepassing. Secrets worden bij voorkeur automatisch geroteerd om de kans op misbruik te verkleinen.
E 11.40.	Toegangsbeveiliging	De Oplossing biedt de mogelijkheid om bij beëindiging van het dienstverband de toegekende autorisaties aan Gebruikers automatisch te laten vervallen.
E 11.41.	Toegangsbeveiliging	Opdrachtnemer zorgt dat de 'principle of least privilege', 'segregation of duties' en 'need to know' aantoonbaar worden toegepast in de geïmplementeerde autorisaties, zowel in applicaties als in de infrastructuur en hosting. Accounts krijgen niet meer rechten dan nodig, kunnen alleen informatie inzien die ze nodig hebben en bezitten geen rechten die conflicteren met de beoogde functiescheiding. Deze eis geldt zowel voor alle relevante persoonsgebonden accounts alsook voor alle relevante niet-persoonsgebonden accounts (zoals service-accounts en API-toegang).
E 11.42.	E-mail beveiliging	Waar in de Oplossing gebruik wordt gemaakt van e-mail die namens de KB wordt verstuurd of ingelezen, dan wordt daarvoor aangesloten op de Microsoft Graph API en vindt autorisatie plaats op basis van OpenID Connect (Oauth 2.0) om toegang te verkrijgen tot het e-mailplatform Exchange Online van de KB voor het verzenden of uitlezen van e-mail. In het geval dat een e-mailvoorziening wordt toegepast die niet verloopt via het e-mailplatform van de KB, dan zorgt Opdrachtnemer ervoor dat de e-mail herkenbaar is, op basis van domeinnaam van de KB, als e-mail van de KB.

11. Security		
E 11.43.	E-mail beveiliging	Waar de Oplossing gebruik maakt van e-mailverkeer dat namens de KB plaatsvindt (intern dan wel extern) voldoet de implementatie blijvend aan aanvullende beveiligingsmaatregelen als SPF, DKIM, DMARC en DANE (eventueel na implementatie door Microsoft).
E 11.44.	Versleuteling	Opdrachtnemer zorgt dat alle netwerkverbindingen zijn voorzien van adequate versleuteling. Bij voorkeur wordt gebruikgemaakt van HTTPS of vergelijkbare marktconforme versleutelingstechnieken die passen bij het netwerkprotocol. Netwerkverbindingen omvatten zowel verbindingen van en naar de internet-facing interfaces, alsmede de netwerkverbindingen binnen de hosting-infrastructuur.
E 11.45.	Versleuteling	De Oplossing maakt standaard gebruik van veilige communicatieprotocollen zoals HTTPS, SSH en SFTP. Waar HTTPS wordt toegepast, vindt dit plaats conform de 'Transport Layer Security (TLS) Beveiligingsrichtlijnen' versie 2025-05 van het NCSC, wat onder andere betekent dat minimaal TLS 1.2 en bij voorkeur TLS 1.3 (dan wel nieuwer) wordt toegepast. Voorts wordt HSTS gehanteerd.
E 11.46.	Logging en monitoring	Opdrachtnemer borgt dat security- en auditlogging wordt bijgehouden voor ieder component dat onderdeel uitmaakt van de Oplossing. De componenten omvatten zowel de infrastructuur gebruikt voor de hosting alsmede de API's, webapplicatie en de AI-componenten.
E 11.47.	Logging en monitoring	Opdrachtnemer borgt dat security- en auditlogging minimaal de volgende acties omvatten: 1. Aan- en afmeldpogingen (geslaagd en niet geslaagde pogingen) 2. Wijzigingen in gebruikersrechten 3. Het lezen, wijzigen of verwijderen van gevoelige gegevens 4. Systeemwaarschuwingen, fouten en crashes 5. Wijzigingen in configuraties en instellingen gemaakt door beheerders/gebruikers met hoge rechten 6. Handmatige lees, schrijf en verwijderhandelingen op logbestanden 7. Voor alle internet-facing systemen: alle verzoeken en responses (zoals GET en POST verzoeken).

11. Security		
E 11.48.	Logging en monitoring	Logregels bevatten minimaal de volgende informatie: datum, tijd, bron, gebruikers-ID, actie of handeling en het resultaat van de actie of handeling.
E 11.49.	Logging en monitoring	Opdrachtnemer zorgt dat security monitoring wordt uitgevoerd door een gekwalificeerd Security Operations Centre (SOC) voor alle onderdelen van de Oplossing. Opdrachtnemer informeert de KB onmiddellijk bij het voordoen van een gebeurtenis waarbij een risico bestaat dat de beschikbaarheid, integriteit of vertrouwelijkheid van de gegevens verwerkt in de Oplossing kan worden geschaad.
E 11.50.	Logging en monitoring	Opdrachtnemer zorgt voor monitoring van de beschikbaarheid en performance van de Oplossing en zorgt dat de KB binnen de gestelde responsetijden wordt geïnformeerd bij onder andere (niet uitputtend): uitval, performanceproblemen, (Distributed) Denial of Service aanvallen en onverklaarbaar hoog netwerkverkeer.
E 11.51.	Logging en monitoring	Opdrachtnemer zorgt dat security- en auditlogging te allen tijde wordt bewaard op een wijze waarbij de beschikbaarheid en integriteit zijn gewaarborgd. Bij uitval of verstoring van een systeem gaan logbestanden niet verloren.
E 11.52.	Uptime en beschikbaarheid	Failover en Redundantie: Er moeten (in lijn met de uptime vereisten in de eis E 13.1.) mechanismen zijn om te waarborgen dat de applicatie beschikbaar blijft bij hardware- of softwarestoringen. Bijvoorbeeld clustering of een hot standby. De Hypervisor waar de applicatie op draait kan ook afdoende zijn.
E 11.53.	Back-up en herstel	Opdrachtnemer ontwikkelt of configureert een backup- en herstelvoorziening waarmee invulling wordt gegeven aan de beschikbaarheidseisen en genoemde hersteltijden (Recovery Point Objective = 30 uur; Recovery Time Objective = 40 uur).
E 11.54.	Back-up en herstel	Opdrachtnemer controleert minimaal maandelijks op bruikbaarheid, correctheid en volledigheid van de gemaakte back-ups. Deze controle wordt geregistreerd en gedocumenteerd.

11. Security		
E 11.55.	Back-up en herstel	Opdrachtnemer voert minimaal jaarlijks een back-up hersteltest uit, waarbij wordt getest of back-ups tijdig kunnen worden hersteld. Deze test en de testresultaten worden gedocumenteerd door de Opdrachtnemer. Opdrachtnemer stelt deze documentatie ter beschikking op aanvraag van de KB.
E 11.56.	Back-up en herstel	Opdrachtnemer stelt in afstemming met de KB een 'Disaster Recovery Plan' op en zorgt dan de inhoud actueel wordt gehouden. Het Disaster Recovery Plan beschrijft hoe de dienstverlening die aan de KB wordt geleverd wordt hersteld bij een ramp of andersoortig incident.
E 11.57.	Back-up en herstel	Opdrachtnemer test minimaal jaarlijks de werking van het Disaster Recovery Plan. Opdrachtnemer deelt een gedocumenteerde evaluatie van de Disaster Recovery Plan test met de KB.
E 11.58.	Back-up en herstel	Opdrachtnemer bewaart back-ups op meerdere fysieke locaties om bescherming te bieden tegen lokale uitval. De 3-2-1-1-0 regel wordt toegepast: Er dienen ten minste 3 kopieën van data te zijn (1 primaire kopie en twee extra kopieën) op 2 verschillende media waarvan ten minste 1 kopie buiten de primaire locatie wordt opgeslagen en ten minste 1 kopie van de data offline (air gapped) wordt opgeslagen. Er mogen geen (0) fouten in de backup aanwezig zijn.
E 11.59.	Back-up en herstel	Er is ten minste één immutable back-up beschikbaar conform het WORM-principe (write-once, read-many).
E 11.60.	Incidentafhandeling	Bij het voordoen van een potentieel informatiebeveiligingsincident met een impact op data, systemen of medewerkers van de KB meldt de Opdrachtnemer dit onverwijld aan de KB via het CSIRT-KB.
E 11.61.	Toekomstige beveiligingseisen bij vermoeden van een koppeling	Indien Opdrachtnemer een koppeling wenst te realiseren met een KB informatiesysteem, worden aanvullende informatiebeveiligingseisen door de KB gesteld aan Opdrachtnemer. Opdrachtnemer mag pas een koppeling tot stand brengen nadat de informatiebeveiligingseisen aantoonbaar zijn geïmplementeerd.

12. Servicemanagement

E 12.1.	Uitwerking in SLA, DAP en Exitplan	Opdrachtnemer legt de uitwerking van de niet-functionele eisen uit dit Programma van Eisen, waaronder servicemanagement, beveiliging, privacy en digitale toegankelijkheid, vast in een Service Level Agreement (SLA), een Dossier Afspraken en Procedures (DAP) en een Exitplan. De SLA bevat de serviceniveaus. Het DAP omvat alle verantwoordelijkheden, procedures en overige beheerafspraken. De SLA en het DAP vormen de basis voor rapportage, evaluatie en bijsturing van de dienstverlening.
E 12.2.	Uitwerking in SLA, DAP en Exitplan	De KB en Opdrachtnemer stellen na gunning en vóór ondertekening van de Overeenkomst de SLA en een eerste versie van het Exitplan vast, op basis van de versies die de voorlopig winnende Inschrijver heeft uitgewerkt, en ondertekenen de SLA. In dezelfde periode levert Opdrachtnemer een eerste versie van het DAP aan, die de KB vóór ondertekening van de Overeenkomst goedkeurt. Daarna stemmen de KB en Opdrachtnemer het DAP nader af voor gebruik in de operatie; uiterlijk 20 werkdagen vóór inbeheername stellen zij de definitieve versie van het DAP vast en ondertekenen deze. De definitieve versie van het Exitplan wordt uiterlijk 20 werkdagen na inbeheername vastgesteld en ondertekend.
E 12.3.	Inbeheername	Vóór inbeheername richt Opdrachtnemer de meldkanalen uit de eis Ondersteuningstijden in, waaronder een meldportaal als dat wordt gebruikt, en test de KB deze samen met Opdrachtnemer. In de implementatieperiode voeren de KB en Opdrachtnemer droogzwemsessies uit met de betrokken partijen, waarin de procedures uit het DAP worden doorlopen; de planning daarvan stemmen zij vooraf af. Inbeheername vindt plaats nadat de KB heeft vastgesteld dat beide zijn afgerond.

12. Servicemanagement

E 12.4.	Uitwerking in SLA, DAP en Exitplan	De KB en Opdrachtnemer voeren minimaal jaarlijks, en daarnaast bij relevante wijzigingen in de dienstverlening, een review uit van de SLA, het DAP en het Exitplan, en actualiseren deze waar nodig. Het DAP is een levend document: Opdrachtnemer en de KB werken het DAP bij zodra ervaringen in de operatie, wijzigingen in processen of organisatie, of wijzigingen in wet- en regelgeving daartoe aanleiding geven.
E 12.5.	Serviceniveaus	Opdrachtnemer voldoet aan de overeengekomen serviceniveaus. Deze omvatten ten minste: beschikbaarheid, performance, bereikbaarheid van de servicedesk, reactie-, update- en oplostijden van incidenten per prioriteit, doorlooptijden van serviceverzoeken en wijzigingsverzoeken, en de hersteltijd (Recovery Time Objective, RTO) en het maximale dataverlies (Recovery Point Objective, RPO) bij calamiteiten.
E 12.6.	Serviceniveaus	De normen staan in de SLA-eisen van dit Programma van Eisen, de eis Responstijd en de security-eis Back-up en herstel (RPO/RTO) E 11.53. Deze normen vormen de ondergrens voor de SLA; de SLA, het DAP en het Exitplan doen geen afbreuk aan dit Programma van Eisen. Alle serviceniveaus zijn resultaatverplichtingen.
E 12.7.	Taal	Opdrachtnemer biedt de servicedesk, de servicerapportages, de release-informatie en de gebruikersdocumentatie aan (in het Nederlands of Engels).
E 12.8.	Meetbaarheid	Opdrachtnemer meet de serviceniveaus per kalendermaand, tenzij een eis in dit Programma van Eisen een andere periode noemt. De reactie-, update- en oplostijden gelden per incident. De meetmethode per serviceniveau wordt vastgelegd in de SLA. Opdrachtnemer geeft de KB op verzoek binnen 10 werkdagen inzage in de onderliggende meetgegevens.

12. Servicemanagement		
E 12.9.	Afwijkingen	Opdrachtnemer bewaakt de naleving van alle serviceniveaus uit dit Programma van Eisen en de SLA, en monitort beschikbaarheid en performance volgens de security-eis Logging en monitoring (monitoring van beschikbaarheid en performance) E 11.50. Uitval en performanceproblemen meldt Opdrachtnemer als incident, binnen de reactietermijn uit de eis Reactie-, update- en oplostijden. Afwijkingen van de overige serviceniveaus meldt Opdrachtnemer binnen 2 werkdagen aan de KB. Bij elke melding geeft Opdrachtnemer de verwachte hersteltijd en de herstelmaatregelen.
E 12.10.	Ketensamenwerking	De Oplossing wordt gebruikt door de KB en de netwerkpartners, elk met eigen processen en koppelingen. Opdrachtnemer richt de dienstverlening zo in dat de KB de netwerkpartners kan informeren, raadplegen en betrekken bij incidenten, wijzigingen, releases, onderhoud en evaluaties. Daarvoor gelden de termijnen uit de eisen Reactie-, update- en oplostijden, Wijzigingen dienstverlening, Roadmap en releases, Release-informatie, Testomgeving, API-wijzigingen, Statusinformatie, Onderhoud zonder downtime, Gepland onderhoud met downtime, Spoedonderhoud en Periodieke evaluatie. Opdrachtnemer levert meldingen en rapportages zonder vertrouwelijke gegevens van Opdrachtnemer of andere klanten, zodat de KB deze zonder bewerking kan doorsturen aan de netwerkpartners.
E 12.11.	Rollen en escalatie	Opdrachtnemer legt in het DAP de verantwoordelijkheden, contactpunten, meldroutes en escalatieniveaus vast, met ten minste een operationeel niveau en een managementniveau. De KB is voor Opdrachtnemer het aanspreekpunt voor prioriteiten, wijzigingsverzoeken en afspraken over onderhoud en releases. Opdrachtnemer wijst een vast aanspreekpunt aan voor de dienstverlening en meldt een wijziging daarvan uiterlijk 10 werkdagen vooraf aan de KB.

12. Servicemanagement

E 12.12.	Rollen en escalatie	Netwerkpartners melden incidenten en serviceverzoeken via het aanspreekpunt van de KB, niet rechtstreeks bij Opdrachtnemer; dit wordt vastgelegd in het DAP. Opdrachtnemer ondersteunt een andere inrichting als de KB daartoe gedurende de looptijd besluit. Kosten voor een wijziging van de inrichting brengt Opdrachtnemer alleen in rekening als deze vooraf zijn onderbouwd en de KB daarvoor schriftelijk akkoord heeft gegeven. Verzoeken die Opdrachtnemer rechtstreeks van een netwerkpartner ontvangt, legt Opdrachtnemer binnen 1 werkdag voor aan de KB.
E 12.13.	Wijzigingen dienstverlening	Opdrachtnemer kondigt wijzigingen met materiële gevolgen voor kwaliteit, continuïteit, beschikbaarheid, beveiliging, privacy, digitale toegankelijkheid, koppelingen of beheer schriftelijk aan bij de KB, met een beschrijving van de wijziging en de gevolgen. Wijzigingen met gevolgen voor koppelingen, werkprocessen of functionaliteit kondigt Opdrachtnemer uiterlijk 40 werkdagen vooraf aan; overige materiële wijzigingen uiterlijk 20 werkdagen vooraf. Deze termijnen gelden ook voor releases en onderhoud met deze gevolgen.
E 12.14.	Wijzigingen dienstverlening	Voor foutherstel binnen de oplostijden geldt de eis Reactie-, update- en oplostijden, en voor dringende beveiligingsupdates de eis Spoedonderhoud. Een wijziging doet geen afbreuk aan de eisen uit dit Programma van Eisen. Vervalt of vermindert functionaliteit die de KB gebruikt, dan kondigt Opdrachtnemer dat minimaal 6 maanden vooraf aan en vraagt daarvoor schriftelijk akkoord van de KB.
E 12.15.	Roadmap en releases	Opdrachtnemer maakt bekend hoe vaak en op welke manier releases van de Oplossing worden uitgebracht, en deelt minimaal elk kwartaal een roadmap met de KB, met de geplande functionele wijzigingen en de wijzigingen aan de API en koppelvlakken voor de komende 6 maanden. Wijzigingen in de roadmap deelt Opdrachtnemer binnen 5 werkdagen na het besluit daarover met de KB. Releases met alleen foutherstel, zonder gevolgen voor koppelingen, werkprocessen of functionaliteit, hoeven niet in de roadmap te staan.

12. Servicemanagement

E 12.16.	Release-informatie	Opdrachtnemer levert bij elke release met functionele wijzigingen of wijzigingen aan de API of koppelvlakken uiterlijk 20 werkdagen vóór inbeheername release-informatie aan de KB, met ten minste: de functionele wijzigingen, wijzigingen aan de API en koppelvlakken, opgeloste en bekende fouten, en de gevolgen voor configuratie en koppelingen. Bij overige releases levert Opdrachtnemer deze informatie uiterlijk bij inbeheername. Opdrachtnemer stelt op verzoek van de KB binnen 5 werkdagen een samenvatting beschikbaar van de door Opdrachtnemer uitgevoerde tests.
E 12.17.	Testomgeving	Opdrachtnemer stelt gedurende de looptijd een test- of acceptatieomgeving beschikbaar, met dezelfde configuratie als de productieomgeving en een representatieve dataset. Releases met functionele wijzigingen of wijzigingen aan de API of koppelvlakken zijn daarin uiterlijk 10 werkdagen vóór inbeheername beschikbaar, zodat de KB en de netwerkpartners koppelingen kunnen testen.
E 12.18.	Regressietests	Opdrachtnemer voert vóór elke release regressietests uit, inclusief de API en de koppelvlakken, en bij wijzigingen aan de user-interface ook op digitale toegankelijkheid volgens de eis WCAG. Een release doet geen afbreuk aan de bestaande functionaliteit, de koppelingen, en het niveau van beveiliging, privacy en digitale toegankelijkheid volgens dit Programma van Eisen. Een regressie op een van deze punten behandelt Opdrachtnemer als incident volgens de eis Prioriteitsindeling incidenten.
E 12.19.	Statusinformatie	Opdrachtnemer biedt de KB 24 uur per dag, 7 dagen per week informatie over de status van de dienstverlening, waaronder lopende incidenten (verstoringen van de dienstverlening), gepland onderhoud en aangekondigde releases, bijvoorbeeld via een statuspagina. Opdrachtnemer werkt de status van een incident bij binnen de reactie- en updatetermijnen uit de eis Reactie-, update- en oplostijden.
E 12.20.	Periodieke evaluatie	De KB en Opdrachtnemer evalueren minimaal jaarlijks de kwaliteit en prestaties van de dienstverlening, inclusief de samenwerking in de keten van de KB en de netwerkpartners. Daarnaast voeren zij minimaal elk kwartaal serviceoverleg; de deelnemers worden vastgelegd in het DAP.

12. Servicemanagement

E 12.21.	Periodieke evaluatie	Op verzoek van de KB maakt Opdrachtnemer het mogelijk dat netwerkpartners deelnemen aan het serviceoverleg of de evaluatie. Opdrachtnemer legt de afspraken en verbeterpunten uit elk overleg vast en levert het verslag binnen 5 werkdagen aan de KB.
E 12.22.	API-wijzigingen	Opdrachtnemer houdt wijzigingen aan de API en de overige koppelvlakken, zoals de OAI-PMH-interface, achterwaarts compatibel. Is dat niet mogelijk, dan kondigt Opdrachtnemer de wijziging minimaal 6 maanden vóór inbeheername aan en blijft de vorige versie tot minimaal 6 maanden na inbeheername van de nieuwe versie werken.
E 12.23.	SLA en Exitplan bij inschrijving	Inschrijver gaat bij de Inschrijving akkoord met de templates van de KB voor de SLA en het Exitplan (Bijlage 7 en Bijlage 9). **Voor het DAP stelt de KB geen apart template beschikbaar; de minimale inhoud van het DAP staat in bijlage A van de SLA.** De voorlopig winnende Inschrijver werkt op basis van deze templates een eerste versie van de SLA en van het Exitplan uit. Het Exitplan beschrijft ten minste hoe beëindiging, migratie en overdracht worden ondersteund, inclusief de overdracht van gegevens en de continuïteit tijdens de transitie. De eisen uit dit Programma van Eisen gaan voor op deze versies.

13. SLA

E 13.1.	Beschikbaarheid	De Oplossing, inclusief de beheerinterface, de publieksinterface en alle koppelvlakken, zoals de API en de OAI-PMH-interface, is per kalendermaand minimaal 99% van de tijd beschikbaar, gemeten 24 uur per dag, 7 dagen per week. Een onderdeel is onbeschikbaar als het niet bereikbaar is of als de KB er geen termen mee kan raadplegen, zoeken of vastleggen. Gepland onderhoud volgens de eis Gepland onderhoud met downtime telt niet mee als onbeschikbaarheid.

13. SLA		
E 13.2.	Performance	De API van de Oplossing beantwoordt per kalendermaand minimaal 95% van de verzoeken om een term of een zoekresultaat op te vragen binnen 1 seconde, gemeten bij het koppelvlak van Opdrachtnemer. De responstijden van de API, en de responstijd van de user-interface volgens de eis Responstijd, worden gehaald bij een belasting van 50 gelijktijdige gebruikers en 200 API-verzoeken per minuut.
E 13.3.	Ondersteuningstijden	De servicedesk van Opdrachtnemer is bereikbaar op werkdagen van 08:00 tot 18:00 uur Nederlandse tijd, per telefoon en daarnaast per e-mail of via een meldportaal. Binnen deze ondersteuningstijden lopen de reactie-, update- en oplostijden voor incidenten met prioriteit 2 tot en met 4, en de termijnen voor serviceverzoeken en wijzigingsverzoeken. Incidenten met prioriteit 1 kan de KB 24 uur per dag, 7 dagen per week telefonisch melden; Opdrachtnemer handelt deze ook buiten de ondersteuningstijden af.
E 13.4.	Prioriteitsindeling incidenten	Opdrachtnemer deelt incidenten in vier prioriteiten in op basis van impact en urgentie, niet op basis van wie het incident meldt. De KB stelt bij de melding de prioriteit vast.
E 13.5.	Prioriteitsindeling incidenten	Daarbij geldt ten minste: - prioriteit 1: de Oplossing, de API of een ander koppelvlak van de Oplossing is niet beschikbaar voor de KB en/of voor een of meer netwerkpartners, of gegevens zijn verloren of aangetast; - prioriteit 2: een functie voor raadplegen, zoeken of vastleggen van termen werkt niet, of de normen uit de eisen Performance of Responstijd worden niet gehaald, zonder workaround; - prioriteit 3: een functie werkt niet volgens de eisen, met een workaround; - prioriteit 4: overige verstoringen zonder directe gevolgen voor het werk.

13. SLA		
E 13.6.	Reactie-, update- en oplostijden	Opdrachtnemer reageert op incidenten, geeft updates en lost incidenten op binnen de volgende termijnen, gerekend vanaf de melding: - prioriteit 1: reactie binnen 1 uur, update elk uur, opgelost binnen 4 uur; - prioriteit 2: reactie binnen 2 uur, update elke 4 uur, opgelost binnen 8 uur; - prioriteit 3: reactie binnen 1 werkdag, update elke 2 werkdagen, opgelost binnen 5 werkdagen; - prioriteit 4: reactie binnen 3 werkdagen, update elke 5 werkdagen, opgelost binnen 20 werkdagen, ook als de oplossing in een release wordt meegenomen. Voor prioriteit 1 lopen de termijnen 24 uur per dag, 7 dagen per week; voor prioriteit 2 tot en met 4 binnen de ondersteuningstijden.
E 13.7.	Reactie-, update- en oplostijden	Reactie betekent: Opdrachtnemer bevestigt de melding en de prioriteit en is met de behandeling begonnen. Update betekent: Opdrachtnemer informeert de KB over de stand van zaken en de verwachte oplostijd. Opgelost betekent: de dienstverlening werkt weer volgens dit Programma van Eisen en de SLA.
E 13.8.	Reactie-, update- en oplostijden	Een tijdelijke oplossing (workaround) stopt de oplostijd alleen als de KB daarmee instemt. Het incident krijgt dan de prioriteit die past bij de resterende impact, en Opdrachtnemer lost het structureel op binnen de oplostijd van die prioriteit. Incidenten die Opdrachtnemer zelf vaststelt, meldt Opdrachtnemer binnen de reactietermijn van de betreffende prioriteit aan de KB, met een voorlopige prioriteit; de KB kan deze prioriteit wijzigen.

13. SLA		
E 13.9.	Serviceverzoeken en wijzigingsverzoeken	Opdrachtnemer handelt de standaard serviceverzoeken uit het DAP af binnen 5 werkdagen. Op een wijzigingsverzoek van de KB, waaronder doorontwikkeling zoals een nieuwe koppeling of een nieuwe thesaurus (non-standard change), levert Opdrachtnemer binnen 10 werkdagen een impactanalyse met planning en, als er kosten zijn, de kosten; de KB besluit over de uitvoering. Op een verzoek van de KB om advies of ondersteuning levert Opdrachtnemer binnen 5 werkdagen een voorstel met de inzet, de planning en de kosten op basis van de uurtarieven uit het Prijzenblad; de KB besluit over de uitvoering. Zolang een van deze verzoeken openstaat, geeft Opdrachtnemer de KB minimaal elke 5 werkdagen een update over de voortgang.
E 13.10.	Oorzaakanalyse	Na elk incident met prioriteit 1, na 3 incidenten met dezelfde oorzaak binnen 3 maanden, en op verzoek van de KB, levert Opdrachtnemer binnen 10 werkdagen na het oplossen van het incident een rapportage aan de KB met de oorzaak, de gevolgen, de genomen maatregelen en de maatregelen om herhaling te voorkomen.
E 13.11.	Inhoud en frequentie servicerapportage	Opdrachtnemer levert maandelijks, uiterlijk 10 werkdagen na afloop van de periode, een servicerapportage aan de KB over de naleving van de serviceniveaus uit dit Programma van Eisen en de SLA, en over de afspraken uit het DAP. De rapportage bevat ten minste: de behaalde beschikbaarheid en performance, incidenten per prioriteit met de reactie-, update- en oplostijden, serviceverzoeken en wijzigingsverzoeken met hun status, uitgevoerd en gepland onderhoud, afwijkingen van de serviceniveaus met de herstelmaatregelen, de oorzaakanalyses, de roadmap en de rapportages volgens de security-eisen ‘Beveiligingstesten & het verhelpen van kwetsbaarheden’ (E 11.19.) en ‘Hardening’ (E 11.28.).
E 13.12.	Verbeterplan	Haalt Opdrachtnemer een serviceniveau in een kalendermaand niet, dan levert Opdrachtnemer binnen 10 werkdagen na de servicerapportage een verbeterplan aan de KB, met de maatregelen en de datum waarop de norm weer wordt gehaald. Opdrachtnemer voert het verbeterplan uit en rapporteert over de voortgang in de servicerapportage.

13. SLA		
E 13.13.	Onderhoud zonder downtime	Opdrachtnemer voert releases en regulier onderhoud uit zonder downtime van de Oplossing. Onderhoud met downtime is alleen toegestaan als uitzondering, onder de voorwaarden van de eis Gepland onderhoud met downtime. Onderhoud zonder downtime maar met tijdelijke gevolgen voor koppelingen of werkprocessen kondigt Opdrachtnemer uiterlijk 10 werkdagen vooraf aan; overig onderhoud uiterlijk 5 werkdagen vooraf. Voor blijvende gevolgen geldt de eis Wijzigingen dienstverlening.
E 13.14.	Gepland onderhoud met downtime	Gepland onderhoud met downtime kondigt Opdrachtnemer uiterlijk 10 werkdagen vooraf schriftelijk aan bij de KB, met de datum, het tijdstip, de verwachte duur en de gevolgen. Het onderhoud vindt plaats binnen een vast onderhoudsvenster (op werkdagen tussen 22:00 en 06:00 uur Nederlandse tijd, of in het weekend), tenzij de KB vooraf instemt met een ander moment. Geplande downtime bedraagt maximaal 8 uur per kalendermaand; downtime boven dit maximum telt als onbeschikbaarheid. Onderhoud buiten het onderhoudsvenster zonder instemming van de KB, en downtime door spoedonderhoud, tellen ook als onbeschikbaarheid.
E 13.15.	Spoedonderhoud	Dringende beveiligingsupdates volgens de security-eis Patchmanagement E 11.29., en spoedonderhoud om een incident met prioriteit 1 of 2 te voorkomen of op te lossen, mag Opdrachtnemer uitvoeren zonder de aankondigingstermijnen uit de eisen Wijzigingen dienstverlening, Onderhoud zonder downtime en Gepland onderhoud met downtime. Opdrachtnemer informeert de KB zo snel mogelijk vooraf, en uiterlijk 1 werkdag na afloop schriftelijk over de reden, de uitgevoerde werkzaamheden en de gevolgen.

14. DAP		
E 14.1.	Inhoud DAP	Het DAP beschrijft ten minste: de contactgegevens; de procedures voor incidenten, serviceverzoeken, wijzigingen, releases en onderhoud; de meldroutes en escalatie; het beheer van accounts en rollen; de rapportage en het serviceoverleg; de afhankelijkheden van de koppelingen; en de operationele uitwerking van de eisen over beveiliging, privacy en digitale toegankelijkheid.
E 14.2.	Inhoud DAP	Het DAP beschrijft daarnaast de procedure bij calamiteiten: wie een calamiteit vaststelt en het herstel start, hoe en bij wie Opdrachtnemer meldt, hoe Opdrachtnemer de KB informeert tot het herstel is afgerond, en hoe Opdrachtnemer de uitkomsten van hersteltests met de KB deelt.
E 14.3.	RACI en demarcatie	Het DAP bevat een RACI-matrix, waarin per taak staat wie uitvoert, wie eindverantwoordelijk is, wie wordt geraadpleegd en wie wordt geïnformeerd, en een demarcatie van de verantwoordelijkheden van Opdrachtnemer, de KB en, waar van toepassing, de netwerkpartners. Deze omvatten ten minste: de koppelingen en koppelvlakken, de monitoring, het melden en oplossen van incidenten, en het doorvoeren van wijzigingen en releases.

15. Exit		
E 15.1.	Voorkomen belemmeringen	Opdrachtnemer voorkomt afhankelijkheden, zoals eigen dataformaten of hulpmiddelen van Opdrachtnemer of derden, die een migratie of overdracht belemmeren. Afhankelijkheden die niet te voorkomen zijn, beschrijft Opdrachtnemer in het Exitplan, met de manier waarop deze bij exit worden opgelost.

15. Exit		
E 15.2.	Exitplan	Opdrachtnemer stelt samen met de KB een Exitplan op. Het Exitplan bevat ten minste: de scope; de activiteiten en verantwoordelijkheden van Opdrachtnemer, de KB en een opvolgend dienstverlener; de planning en afhankelijkheden; de overdracht van gegevens, inclusief formaat en controle op volledigheid; documentatie en configuraties; kennisoverdracht; toegangen en autorisaties; de gevolgen voor de koppelingen en de netwerkpartners; continuïteit tijdens de transitie; de verwijdering van gegevens; risico's; escalatie; en acceptatiecriteria. Voor de termijnen en de actualisatie geldt de eis Uitwerking in SLA, DAP en Exitplan.
E 15.3.	Medewerking overdracht	Opdrachtnemer verleent bij beëindiging van de Overeenkomst alle medewerking die nodig is voor een beheerste overdracht naar de KB of een door de KB aangewezen opvolgend dienstverlener, volgens het Exitplan, tegen de tarieven uit het Prijzenblad.
E 15.4.	Continuïteit tijdens exit	Op verzoek van de KB levert Opdrachtnemer na het einde van de Overeenkomst de dienstverlening door volgens dit Programma van Eisen, de SLA en het DAP, totdat de overdracht is afgerond, gedurende maximaal 12 maanden (transitieperiode), tegen de tarieven uit het Prijzenblad, inclusief indexatie. De KB doet dit verzoek uiterlijk 6 maanden vóór het einde van de Overeenkomst. Bij een onverwachte tussentijdse beëindiging van de Overeenkomst geldt deze termijn van 6 maanden niet. In dat geval kan de KB het verzoek tot doorlevering doen zodra de tussentijdse beëindiging bekend is.
E 15.5.	Gegevens bij exit	Opdrachtnemer levert bij beëindiging, en daarnaast op verzoek van de KB binnen 10 werkdagen, alle in de Oplossing vastgelegde gegevens volledig aan, inclusief termen, relaties, metadata, identifiers, termgeschiedenis, de audit trail en configuraties. Opdrachtnemer levert de gegevens in een open en gedocumenteerd formaat dat zonder hulpmiddelen van Opdrachtnemer bruikbaar is, in elk geval RDF/SKOS, en op verzoek van de KB ook in de formaten uit de eisen Export.

15. Exit		
E 15.6.	Verwijdering gegevens	Nadat de KB schriftelijk heeft bevestigd dat de overdracht volledig is, verwijdert Opdrachtnemer binnen 20 werkdagen alle gegevens van de KB uit de Oplossing, bij Opdrachtnemer en bij ingeschakelde derden, inclusief back-ups, en bevestigt dit schriftelijk aan de KB. Gegevens in back-ups die niet eerder te verwijderen zijn, verwijdert Opdrachtnemer uiterlijk 3 maanden na de bevestiging van de KB; tot die tijd gebruikt Opdrachtnemer ze niet. Offline back-ups vernietigt Opdrachtnemer aantoonbaar.

16. Privacy		
E 16.1.	Procedure	Opdrachtnemer heeft processen en procedures ingericht om te borgen dat de verwerkingen van persoonsgegevens in de Oplossing en door Opdrachtnemer conform de AVG en UAVG kunnen plaatsvinden. Opdrachtnemer garandeert naleving van de geldende wet- en regelgeving op het gebied van het gegevensbeschermingsrecht.
E 16.2.	Binnen de EER	Opdrachtnemer schrijft in via een Europese rechtspersoon. Opdrachtnemer en zijn subverwerkers, verwerken gegevens van de KB alleen binnen de EER (Europese Economische Ruimte).
E 16.3.	Verwerkingsovereenkomst	Indien Opdrachtnemer kwalificeert als Verwerker sluiten Partijen een verwerkersovereenkomst af. Voordat Opdrachtnemer overgaat tot het verwerken van persoonsgegevens van de KB, is de verwerkersovereenkomst afgesloten.
E 16.4.	Model	De KB-Model-Verwerkersovereenkomst is van toepassing (zoals bijgevoegd bij de aanbestedingsdocumenten).
E 16.5.	Procedure	Het verlenen van toegang tot persoonsgegevens aan medewerkers van de Opdrachtnemer wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.

16. Privacy

E 16.6.	Anonimiseren	Als het gaat om gegevens die in aanmerking komen voor anonimiseren (in het kader van en in de zin van de AVG), dan heeft de Oplossing de mogelijkheid om gegevens te kunnen anonimiseren en een rapport te genereren waaruit blijkt dat dit heeft plaatsgevonden.
E 16.7.	Datalek	Gegevens van de productie omgeving worden in beginsel niet gebruikt in een acceptatie/test of demo omgeving. Als voor bepaalde situaties productiegegevens toch nodig zijn in een andere omgeving, dan dient dit vooraf met de KB afgestemd te worden. Opdrachtnemer waarborgt dat bij het overzetten (uit de productieomgeving naar een andere omgeving) van de persoonsgegevens, deze worden geanonimiseerd, zodat gegevens niet meer te herleiden zijn naar natuurlijke personen.
E 16.8.	Verwerkingsdoeleinden	Opdrachtnemer is niet gerechtigd om de verkregen data, informatie en/of andere inzichten welke voortkomen uit het aangaan van deze Overeenkomst te gebruiken voor andere doeleinden (waaronder productverbetering) zonder nadrukkelijke schriftelijke toestemming door de KB.
E 16.9.	Assessment	Opdrachtnemer werkt -indien nodig- mee met het uitvoeren van een Data Protection Impact Assessment (DPIA) volgens het model van de KB.

17. Facturatie

E 17.1.	Facturatie	Opdrachtnemer verzendt, na volledige verrichting en acceptatie door de KB, onder vermelding van de Raamovereenkomst en het inkoopopdracht-nummer een factuur per uitgebrachte Nadere offerte met betrekking tot de (aanvullende) werkzaamheden.
E 17.2.	Betalingstermijn	De KB hanteert een betalingstermijn van dertig dagen na factuurdatum, mits de factuur onbetwist is.

17. Facturatie

E 17.3.	Gegevens	Een factuur bevat minimaal de volgende gegevens: **Gegevens Opdrachtnemer** • Bedrijfsnaam • Adres • Telefoonnummer • KvK-nummer • Btw-nummer • IBAN-rekeningnummer • Debiteurnummer **Gegevens KB** • Organisatienaam • Adres • Contractnummer **Factuur gegevens** • Factuurdatum • Factuurnummer • Inkoopordernummer • Periode waar de factuur betrekking op heeft • Totaal factuurbedrag exclusief btw • Btw-percentage • Btw-bedrag factuur • Totaal factuurbedrag inclusief btw • Kostenoverzicht als bijlage. De definitieve inhoud en opmaak van de verzamelfacturen wordt gedurende de implementatiefase in overleg tussen de KB en de Opdrachtnemer vastgesteld.
E 17.4.	E-factuur	Facturen worden uitsluitend onder vermelding van het inkoopordernummer als e-factuur, volgens de UBL 2.1 standaard, via Peppol of digitaal in pdf-formaat aan facturen@kb.nl verstuurd.

17. Facturatie		
E 17.5.	Afhandeling	Indien een factuur niet voldoet aan de aanbestedingsstukken genoemde voorwaarden wordt de Opdrachtnemer hiervan binnen 14 kalenderdagen na ontvangst schriftelijk op de hoogte gebracht. De betreffende factuur wordt pas in behandeling genomen op het moment dat deze voldoet aan de in de aanbestedingsstukken genoemde voorwaarden.
E 17.6.	Verrekening	De KB is gerechtigd om indien er sprake is van door de Opdrachtnemer verschuldigde bedragen (creditering(en)) deze te verrekenen met bedragen die Opdrachtnemer verschuldigd is aan de KB.