Dienst Publiek en Communicatie
Ministerie van Algemene Zaken

SELECTIELEIDRAAD

Europese niet-openbare aanbesteding

Online Community Tooling
Aanbestedingsnummer: Ea0070
TenderNed-kenmerk: 275152
Referentie: 4138768

Van het ministerie van Algemene Zaken
Dienst Publiek en Communicatie

CPV-code: 72000000-5,48000000-8,
48200000-0, 48220000-6,
48500000-3,

INHOUDSOPGAVE

1 INLEIDING

Het doel van deze Europese niet-openbare aanbesteding is het sluiten van een raamovereenkomst tussen de aanbestedende dienst en één opdrachtnemer voor het leveren van licenties voor community tooling software en dienstverlening op het gebied van community management. De aankondiging van opdracht is op dinsdag 28 juli 2020 gepubliceerd op TenderNed.

De aanbestedende dienst vertegenwoordigt voor deze aanbesteding een aantal andere onderdelen van de Rijksoverheid zoals beschreven in bijlage 6 Lijst Deelnemende organisaties. Dit betekent dat de behoefte van deze organisaties onderdeel uitmaakt van de opdracht zoals beschreven in hoofdstuk 2.

De aanbestedende dienst nodigt gegadigde uit om een verzoek tot deelneming in te dienen op basis van de procedure en voorwaarden zoals beschreven in deze selectieleidraad en onder toepassing van de aanbestedingswet 2012, Wet van 1 juli 2016 tot wijziging van de aanbestedingswet 2012 ter implementatie van de Europese aanbestedingsrichtlijn 2014/23/EU, 2014/24/EU en 2014/25/EU (hierna: Aanbestedingswet). De beoordeling van alle verzoeken tot deelneming zal er toe leiden dat maximaal 5 gegadigden zullen worden uitgenodigd voor de gunningsfase van deze aanbesteding.

1.1 Aanbestedende dienst

De aanbestedende dienst is de Staat der Nederlanden, ministerie van Algemene Zaken, meer in het bijzonder de Dienst Publiek en Communicatie (hierna: de Aanbestedende dienst). De Dienst Publiek en Communicatie (DPC) is een agentschap van het ministerie van Algemene Zaken en ondersteunt de Rijksoverheid in de communicatie met publiek en professionals. Dit doet DPC door het uitvoeren van een aantal rijksbrede communicatietaken en het leveren van gemeenschappelijke communicatiediensten, zoals beschreven op http://www.rijksoverheid.nl/dpc.

DPC is voor de Rijksoverheid tevens het inkoopuitvoeringscentrum voor communicatie. In deze rol koopt DPC namens de Rijksoverheid communicatiediensten en –producten en worden ruim vijfentwintig, veelal rijksbrede, (raam)overeenkomsten beheerd.

1.2 Opbouw van de selectieleidraad

Deze selectieleidraad bestaat uit de volgende onderdelen:

- Hoofdstuk 2: omschrijving van de opdracht.
- Hoofdstuk 3: omschrijving van de aanbestedingsprocedure.
- Hoofdstuk 4: beoordeling formele eisen.
- Hoofdstuk 5: omschrijving uitsluitingsgronden en geschiktheidseisen
- Hoofdstuk 6: omschrijving selectiecriteria

1.3 Persoonsgegevens van gegadigden

Voor deze aanbesteding en het sluiten van de beoogde overeenkomst verwerkt de Aanbestedende dienst persoonsgegevens. Op deze verwerking is de privacyverklaring van toepassing van het ministerie van Algemene Zaken: https://www.rijksoverheid.nl/ministeries/ministerie-van-algemene-zaken/privacy/privacyverklaring-inkoop-en-aanbesteding.

1.4 Klachtenprocedure

De Aanbestedende dienst heeft een klachtenmeldpunt ingericht waar belanghebbenden klachten kunnen melden met betrekking tot de aanbestedingsprocedure. Gegadigde kan klachten schriftelijk indienen bij het klachtenmeldpunt van de Aanbestedende dienst met gebruikmaking van het volgende e-mailadres: klachtaanbestedingdpc@minaz.nl.

Om de onafhankelijkheid en objectiviteit te waarborgen, zullen eventuele klachten behandeld worden door een niet direct bij de aanbesteding betrokken projectleider en een jurist van de Aanbestedende dienst, op basis van onderstaande procedure:

- Bij het indienen van een klacht dient gegadigde duidelijk te maken dat het over een klacht gaat en waarover hij klaagt en hoe het knelpunt volgens hem verholpen zou kunnen worden. De klacht bevat verder de dagtekening, naam en adres van gegadigde en de aanduiding van deze aanbesteding Online Community Tooling, Ea0074.
- Nadat de klacht is binnengekomen bij het klachtenmeldpunt, ontvangt gegadigde hiervan per omgaande een ontvangstbevestiging.
- Het klachtenmeldpunt onderzoekt vervolgens, eventueel aan de hand van aanvullend verstrekte gegevens, of de klacht binnen de reikwijdte van de Klachtenregeling aanbesteden valt (zie https://www.pianoo.nl/nl/document/7583/advies-klachtafhandeling-bij-aanbesteden) en terecht is.
- Wanneer de Aanbestedende dienst na het onderzoek door het klachtenmeldpunt tot de conclusie komt dat de klacht terecht is en de Aanbestedende dienst corrigerende en/of preventieve maatregelen neemt, dan deelt de Aanbestedende dienst dit zo spoedig mogelijk schriftelijk aan gegadigde mee. Ook de andere gegadigden worden op de hoogte gesteld.
- Wanneer de Aanbestedende dienst na het onderzoek tot de conclusie komt dat de klacht niet terecht is, dan ontvangt gegadigde een gemotiveerde afwijzing op zijn klacht.
- Als de Aanbestedende dienst heeft laten weten hoe hij de klacht afhandelt en gegadigde het hier niet mee eens is of als de Aanbestedende dienst nalaat om binnen een redelijke termijn op de klacht te reageren, dan kan gegadigde de klacht aan de Commissie van Aanbestedingsexperts voorleggen. Gegadigde kan zijn klacht bij de Commissie van Aanbestedingsexperts indienen door het invullen van het formulier op de website www.commissievanaanbestedingsexperts.nl.

2 OMSCHRIJVING VAN DE OPDRACHT

In dit hoofdstuk is de opdracht van deze aanbesteding beknopt omschreven. Om gegadigden een zo goed mogelijk beeld te geven van de opdracht is als bijlage 5 (concept-)Programma van Eisen een lijst met technische en functionele eisen opgenomen waaraan de tooling minimaal moet voldoen. Dit concept-programma van eisen dient in beginsel als kader voor de huidige selectiefase op basis waarvan gegadigden een inschatting kunnen maken of ze aan de gevraagde dienstverlening kunnen voldoen. De Aanbestedende dienst behoudt zich het recht voor om, in de gunningsfase, aanvullingen of verduidelijkingen aan te brengen in dit programma van eisen. Deze aanvullingen/verduidelijkingen zullen geen fundamentele wijziging van de opdracht omvatten. De volledige (aanvullende) opdrachtomschrijving en de contractuele condities waaronder deze moet worden uitgevoerd, zullen uitsluitend worden verstrekt aan de gegadigden die op basis van deze selectieleidraad worden geselecteerd en uitgenodigd voor de gunningsfase.

2.1 Omschrijving van de opdracht

De opdracht omvat de levering, inrichting en advisering met betrekking tot tooling voor het faciliteren van verschillende online communities voor de deelnemende organisaties binnen de Rijksoverheid. Deze tool dient de onderlinge samenwerking binnen het Rijk te faciliteren, maar ook de samenwerking tussen het Rijk en externe organisaties/burgers.

Een online community is een groep mensen met een gezamenlijk doel, belang of interesse waarvan de leden elkaar primair online treffen op een speciaal daarvoor bedoeld (afgeschermd) platform. Een online community kan los van organisatiegrenzen functioneren. De leden van de community communiceren of werken met elkaar om samen meer te weten of te kunnen dan ieder afzonderlijk.

De community tool is nadrukkelijk geen sociaal intranet, want een intranet dient andere doelen, zoals het (top-down) informeren van mensen binnen één organisatie.

Ook heeft de online community een ander doel dan een research community (waarvoor reeds een rijksbrede raamovereenkomst bestaat). Een research community is een instrument waarbij antwoord verkregen wordt op een (communicatie)vraagstuk, door een zorgvuldig geselecteerde groep mensen via een online platform verschillende taken uit te laten voeren en vragen te laten beantwoorden. Een afgeschermd online discussieforum dus, meestal kortdurend.

De community tool kan voor verschillende doelen worden ingezet, met als kernwoorden samenwerken, kennis delen en virtueel ontmoeten. Bijvoorbeeld:

- netwerk opbouwen, verbinden (online is het startpunt, maar niet het eindpunt);
- bestaande relaties versterken;
- beter geïnformeerde professionals, kennis opbouwen;
- makkelijker (samen)werken over minder schijven;
- klantenonderzoek: online klantinzichten ophalen;
- ideeëngeneratie, inspiratiebron;
- burgerparticipatie;
- ideeën toetsen.

2.1.1 Scope

De scope van de raamovereenkomst omvat de volgende onderdelen:

1. <u>De SAAS community tool:</u>

   1a) Leveren van licenties voor gebruik van de tool:

   De licenties voor gebruik van de tool omvat standaard minimaal de vereiste functionaliteiten en voldoen standaard aan de gestelde kwaliteitseisen, beveiligingseisen en richtlijnen. Binnen deze standaard hebben opdrachtgevers de mogelijkheid om de community naar eigen inzicht te configureren. De configuratie ziet bijvoorbeeld op het aan- en uitzetten van bepaalde functionaliteiten of het toepassen van bepaalde vormgeving (binnen de Rijkshuisstijl).

   1b) Kwaliteitseisen, beveiligingseisen en (Rijks)richtlijnen:

   De tooling, hosting, beheer en onderhoud moet voldoen aan de standaard kwaliteitseisen, beveiligingseisen, en richtlijnen. Denk hierbij onder andere aan de BIO (BBN2), toegankelijkheidseisen en de Rijkshuisstijl.

   1c) Functionaliteiten:

   In bijlage 5 concept-Programma van Eisen is een beschrijving van de technische en functionele eisen opgenomen waar de tool standaard en minimaal aan moet voldoen.

   1d) Hosting, beheertaken en gebruikersondersteuning

   Bij het leveren van de SAAS community tool beschouwt opdrachtgever het leveren van nieuwe releases, zowel met nieuwe functionaliteit als met oplossingen voor (security) problemen, onderdeel van de te leveren tooling.

   De werkzaamheden die bij gebruikersondersteuning horen zijn:
   - Beantwoorden van eerstelijnsvragen en registratie
   - Communicatie over beschikbaarheid
   - Communicatie in geval van incidenten en calamiteiten
   - Beschikbaar stellen van een handleiding
   - Account- en autorisatiebeheer

   Gestelde (en aanvullende) eisen en aanvullende afspraken worden vastgelegd in een Service Level Agreement (SLA), waarvoor een voorstel wordt opgesteld door de opdrachtnemer, binnen 1 maand na gunning doen van de opdracht.

2. <u>Implementatie en migratie:</u>

   2a) Implementatie van communities

   Als een organisatie een community licentie afneemt, dan zorgt opdrachtnemer ervoor dat deze beschikbaar komt binnen de in de SLA overeengekomen termijn.

   Vanwege uiteenlopende doeleinden waarvoor communities door deelnemende organisaties worden ingezet, wordt van de opdrachtnemer verwacht dat in de inrichting van de community bepaalde functionaliteiten aan- en uitgezet kunnen worden. Zo zijn bepaalde communities alleen bedoeld voor rijksambtenaren (intern), maar andere communities bestaan juist uit een netwerk met professionals of burgers (externen). Dit betekent een andere rechtenstructuur en beveiliging.

Een ander voorbeeld is dat bij een interne community het wel is toegestaan om een bepaald bestandsformat en –grootte te uploaden, terwijl bij een community met externe gebruikers door beveiligingsrisico's ingegeven, door opdrachtnemers kan worden gekozen voor minder formats en lagere groottes.

Dergelijke vrijheden in de configuratie en inrichting van functionaliteiten maakt dan ook onderdeel uit van de te leveren tooling. Van opdrachtnemer wordt, als onderdeel van een implementatietraject, een servicegerichte rol verwacht en dient opdrachtnemer de opdrachtgevers te adviseren over te maken keuzes (bijvoorbeeld op het gebied van gebruik van de tool, het aan- en uitzetten van functionaliteiten en inrichting).

2b) Migratie van bestaande communities
Naast de deelnemende organisaties die een community willen opstarten zijn er diverse organisaties in beeld die een reeds bestaande community zullen moeten migreren naar een nieuwe omgeving. Deelnemende organisaties willen hierbij zoveel mogelijk worden ontzorgd. Deze bestaande communities dienen zoveel als mogelijk één-op-één te migreren.

Ook voor een migratie traject geldt dat van opdrachtnemer een servicegerichte rol wordt verwacht. Opdrachtnemer dient opdrachtgevers te adviseren over te maken keuzes en uit te voeren handelingen.

2c) Coaching Community management
Ook na implementatie en/of migratie wordt van opdrachtnemer verwacht beschikbaar te zijn voor coaching over succesvol community management. Dat wil zeggen dat opdrachtnemer zijn expertise op het gebied van community management in brede zin deelt met opdrachtgevers. Denk hierbij bijvoorbeeld (maar niet uitsluitend) aan advies over het verhogen van engagement binnen groepen, de inrichting van diverse groepen en organisatie van het community management.

3. <u>Exit-strategie</u>
3a) Opstellen van een exit-strategie op basis van minimale eisen en afstemming met opdrachtgever
Om een migratietraject na afloop van de raamovereenkomst en een eventuele nieuw gecontracteerde leverancier zo goed mogelijk te laten verlopen wordt van opdrachtnemer gevraagd om (zonder meerkosten), een exit-strategie op te stellen en mee te werken aan de uitvoering van dit exit-strategie. Deze strategie wordt in overleg met de Aanbestedende dienst afgestemd. Hierbij wordt van opdrachtnemer de medewerking vereist zowel voor, tijdens en na afloop van de raamovereenkomst.

In de exit-strategie komen minimaal de volgende zaken aan bod:
- welke operationele afdelingen en contactpersonen binnen de organisatie van opdrachtnemer worden belast met de afbouw van de rechten en verplichtingen die voortvloeien uit de Raamovereenkomst;
- de wijze waarop gegevens uit de community worden aangeleverd en het moment waarop de (persoons)gegevens worden verwijderd;
- de wijze waarop continuïteit en kwaliteit bij overgang naar een nieuwe leverancier geborgd worden;
- wijze van interactie en communicatie tussen exitteam en nieuwe opdrachtnemer(s);

- de wijze waarop controle wordt uitgeoefend op de voortgang van de exit-strategie;
- planning van de gespecificeerde activiteiten van de exit.

2.2 Omvang en looptijd van de raamovereenkomst

De deelnemende organisaties hebben uiteenlopende behoeftes. Dat betekent dat er zowel grote als kleine communities moeten worden opgezet. Op dit moment zijn er circa 5-10 bestaande communities die gemigreerd moeten worden naar een nieuwe omgeving. Van deze bestaande communities zijn er circa 4 relatief groot en groeiend (500+ gebruikers). Gezien de uiteenlopende behoeftes zal er gedurende de looptijd van de raamovereenkomst bij deelnemende organisaties ook vraag zijn naar implementatie van zowel grotere als kleinere communities. De verwachting is dat er zeker 10-20 kleinere communities (50-150 gebruikers) zullen worden afgenomen gedurende de looptijd van de raamovereenkomst en circa 5-10 grotere communities.

Het maken van een nauwkeurige raming is lastig, aangezien een groot aantal opdrachtgevers voor het eerst voornemens is om communities te gaan inzetten. De deelnemende organisaties die al actieve communities hebben, geven een wil om te groeien aan. De mate van groei (de hoeveelheid gebruikers per community) hangt veelal af van het doel/onderwerp en de kwaliteit van het community management. De Aanbestedende dienst schat op basis van kennis van de markt en ervaring op het gebied van community management in dat één opdrachtnemer kan voorzien in de geschatte omvang en de eventueel (geleidelijke) groeiende behoefte bij deelnemende organisaties.

Op basis van inzichten op dit moment heeft de Aanbestedende dienst de (grove) inschatting gemaakt dat de gemiddelde omvang voor deze raamovereenkomst uit zal komen op circa € 325.000,- exclusief btw per jaar.

Met deze ramingen wil de Aanbestedende dienst een zo goed mogelijk beeld geven van de omvang van de raamovereenkomst. Gegadigde kan geen enkel recht ontlenen aan deze inschatting.

Maximale geraamde waarde
Het is voor de Aanbestedende dienst niet mogelijk een zinvol maximum op te geven voor de onderhavige raamovereenkomst.

Het verloop van de omvang van de onderhavige raamovereenkomst is onvoorspelbaar. Dit komt enerzijds doordat een aantal deelnemende organisaties nog niet eerder op deze wijze gewerkt heeft met communities. Van deze partijen zijn dus geen 'ervaringscijfers' beschikbaar om de omvang te bepalen. De omvang bij deelnemers die op dit moment wel communities hebben, zou bovendien (zoals hierboven al aangegeven) kunnen gaan groeien, maar onduidelijk is nog hoeveel. Er bestaat derhalve een kans dat de omvang sterk stijgt ten opzichte van hetgeen op dit moment wordt ingeschat (zie hierboven).

Om die reden is het niet mogelijk een reële maximum waarde vooraf te bepalen.

Door politieke, economische, budgettaire, bestuurlijke of organisatorische omstandigheden binnen de Rijksoverheid kan de positie of taak van de deelnemende organisaties zoals bedoeld in bijlage 6 Lijst Deelnemende organisaties veranderen. Het gevolg kan zijn dat de lijst van deelnemende organisaties hierdoor wijzigt gedurende de aanbesteding en looptijd van de overeenkomst.

Looptijd van de raamovereenkomst
De looptijd van de raamovereenkomst is vier (4) jaar.

2.3 Werkzaamheden buiten de opdracht

De volgende werkzaamheden vallen uitdrukkelijk niet onder de opdrachtomschrijving van deze aanbesteding en worden in voorkomend geval niet gegund aan de toekomstige opdrachtnemer:

- Redactioneel beheer van content voor communities. Dit wordt verzorgd door medewerkers van opdrachtgevers.
- Inhuur communicatieprofessionals (voor het leveren van tijdelijke communicatiecapaciteit aan de Rijksoverheid bestaat een Rijksbrede raamovereenkomst).

2.4 Clustering

Bij deze Europese aanbesteding worden de opdrachten van verschillende aanbestedende diensten samengevoegd omdat er gelijksoortige behoeften zijn geconstateerd.

Het samenvoegen van de opdrachten van verschillende onderdelen van de Rijksoverheid leidt tot een aanzienlijke besparing op aanbestedings- en apparaatskosten. De Rijksoverheid beperkt het aantal (Europese) aanbestedingen, bespaart op capaciteit in zowel de aanbestedings- als de contractbeheerfase, verkort de doorlooptijden van opdrachten, behaalt schaalvoordelen en verbetert de regie op kwaliteit. Dit vergroot de maatschappelijke waarde van de publieke middelen die gemoeid zijn met aanbesteding en uitvoering.

Het samenvoegen van de opdrachten van verschillende onderdelen van de Rijksoverheid beperkt de offerte-inspanning van de markt die eenmaal in een Europese aanbesteding in concurrentie wordt geroepen. De samenvoeging van de opdrachten heeft geen gevolgen voor de toegankelijkheid van het MKB voor deze Europese aanbesteding. Marktonderzoek wijst uit dat er voldoende partijen zijn die zich bezighouden met online community tooling en tot het MKB behoren. Deze kunnen zelfstandig dan wel in combinatie of met de inzet van onderaannemer(s) het totale pakket van de gevraagde dienstverlening aanbieden.

2.5 Percelen

Deze opdracht wordt niet verdeeld in percelen. Het opdelen van de opdracht in percelen is niet mogelijk, de gevraagde levering en dienstverlening wordt in de markt in zijn geheel aangeboden. Het is niet mogelijk om de dienstverlening op een efficiënte en logische manier op te knippen.

Het niet opdelen in percelen heeft geen gevolgen voor de toegankelijkheid van het MKB. De marktpartijen die in aanmerking kunnen komen voor deze opdracht, betreffen (veelal) MKB partijen. De Aanbestedende dienst stelt ook geen eisen aan omvang of omzet van potentiële inschrijvers.

2.6 Informatiebeveiliging

Het informatiebeveiligingsbeleid van het ministerie van Algemene Zaken heeft tot doel om ongeautoriseerde toegang tot systemen en informatie tegen te gaan, vertrouwelijke informatie te beveiligen, de integriteit van informatie te garanderen, privacy te waarborgen en de continuïteit van de dienstverlening te garanderen.

- Op deze aanbesteding is het Basis Beveiligingsniveau 2 van toepassing zoals beschreven in de Baseline Informatiebeveiliging Overheid versie 1.04 (BIO). De BIO beschrijft de invulling van NEN/ISO27001 en NEN/ISO27002 voor de overheid.
- Bij gebruik van clouddiensten door de toekomstige opdrachtnemer bij de uitvoering van diensten, is het DPC-cloudbeleid van toepassing (bijlage 7) en kunnen normen op basis van ISO/IEC 27017 en ISO/IEC 27018 van toepassing zijn.

- Indien toekomstige opdrachtnemer als verwerkingsverantwoordelijke en/of verwerker, als beschreven in de (U)AVG optreedt, kunnen normen op basis van ISO/IEC 27701:2019 Annex A en ISO/IEC 27701:2019 Annex B van toepassing zijn.

Alle bovengenoemde normen moeten toegepast en aantoonbaar nageleefd worden bij uitvoering van de raamovereenkomst. Dit geldt ook voor eventuele onderaannemers en/of derde partijen gedurende de looptijd van de Raamovereenkomst.

Opdrachtnemer levert binnen zes (6) weken na de mededeling van de gunningsbeslissing een volledig ingevulde fit/gap-analyse aan met daarin de wijze waarop hij invulling geeft aan de normen van de BIO. Dit document geeft inzage in de mate waarin al wordt voldaan aan de BIO. Tevens geeft het inzage in de haalbaarheid, eventueel te nemen maatregelen en de bijbehorende oplostijd (af te ronden vóór start dienstverlening) van de normen waaraan nog niet is voldaan.

Aanbestedende dienst adviseert inschrijvers die nog niet bekend zijn met de BIO voor het inleveren van een verzoek tot deelneming goed te controleren of tijdig voldaan kan worden aan de gestelde eisen betreffende de informatiebeveiliging. Het kan aanbevelingswaardig zijn om een deskundige op het gebied van informatiebeveiliging in te schakelen die de fit/gap-analyse en daaruit voortvloeiende verbetermaatregelen tijdig kan implementeren binnen uw organisatie. De fit/gap-analyse is ter informatie toegevoegd aan deze selectieleidraad als bijlage 8.

3 AANBESTEDINGSPROCEDURE

In dit hoofdstuk wordt een beschrijving gegeven van het aanbestedingsproces en de formele vereisten waaraan gegadigde moet voldoen om een geldig verzoek tot deelneming in te dienen. De inhoudelijke eisen die worden gesteld aan het verzoek tot deelneming staan beschreven in hoofdstuk 4 en 5.

3.1 Digitaal aanbesteden via TenderNed

De aanbestedingsprocedure wordt uitsluitend digitaal uitgevoerd via het elektronisch systeem voor aanbestedingen: TenderNed (www.tenderned.nl). Dit betekent dat verzoeken tot deelneming alleen via TenderNed ingediend kunnen worden. Voor deelneming aan de aanbestedingsprocedure dient een ondernemer als gebruiker te zijn geregistreerd bij TenderNed. Voor het registreren en deelnemen in TenderNed is eHerkenning verplicht. eHerkenning regelt de digitale herkenning (authenticatie) en controleert de digitale bevoegdheid (autorisatie) van personen die online een dienst bij de overheid willen afnemen. Zie voor meer informatie: https://www.tenderned.nl/tenderned-voor-ondernemingen-0/eherkenning-en-tenderned.

Alle communicatie over deze aanbesteding verloopt via de berichtenmodule van TenderNed. Communiceert gegadigde over deze aanbesteding met andere medewerkers van de Aanbestedende dienst of via andere kanalen, dan kan dat voor Aanbestedende dienst reden zijn om gegadigde uit te sluiten van deelname. Gegadigde kan zich niet beroepen op informatie die op een andere wijze dan hiervoor beschreven is verstrekt. Van een gegadigde wordt verwacht dat deze alle benodigde kennis heeft om op een correcte wijze een aanbestedingsprocedure te kunnen doorlopen in TenderNed. Zie voor handleidingen www.tenderned.nl/egids.

Aanbestedende dienst maakt gebruik van de volgende onderdelen van TenderNed:

- De berichtenmodule voor alle communicatie over deze aanbesteding.
- De vragenmodule voor alle vragen in het kader van deze aanbesteding.
- De digitale kluis voor het indienen van het verzoek tot deelneming.

Gebruik van TenderNed is geheel voor rekening en risico van de gegadigde. De Aanbestedende dienst is niet verantwoordelijk voor storingen van de website www.tenderned.nl. Aanbestedende dienst adviseert gegadigde om tijdig de gevraagde documenten te uploaden in TenderNed en hiermee niet tot het laatste moment te wachten.

Indien gegadigde zich op TenderNed heeft geregistreerd en bij het downloaden van de aanbestedingsdocumenten van deze aanbesteding het vinkje ‘houdt mij op de hoogte van deze aanbesteding’ aanvinkt, dan ontvangt gegadigde een notificatie van TenderNed als er nieuwe documenten door Aanbestedende dienst zijn geplaatst. Gegadigden die zich niet hebben geregistreerd op TenderNed, of niet het betreffende vinkje hebben aangevinkt, ontvangen geen notificatie.

3.2 Planning

Fase	Datum
Publicatie van de aanbesteding	Dinsdag 28 juli 2020
Sluitingsdatum stellen van vragen	Dinsdag 4 augustus 2020 om 12.00 uur
Uiterste datum publiceren van antwoorden op vragen (nota van inlichtingen)	Donderdag 13 augustus 2020
Sluitingsdatum indienen verzoek tot deelneming	**Donderdag 3 september 2020, 11.00 uur**
Mededeling selectiebeslissing	Zo spoedig mogelijk na beoordeling
Standstill periode	Twintig kalenderdagen na mededeling gunningsbeslissing
Versturen Beschrijvend document naar geselecteerde partijen	Eind oktober 2020
Inlichtingenbijeenkomst	Begin november 2020
Sluitingsdatum aanleveren Inschrijvingen	Begin december 2020
Start dienstverlening	Medio april 2020

De bovenstaande planning is indicatief. De Aanbestedende dienst is gerechtigd eenzijdig de planning aan te passen indien zij die noodzakelijk acht.

3.3 Gelegenheid tot het stellen van vragen

Eventuele vragen over de inhoud en het proces van deze aanbesteding kan gegadigde tot uiterlijk **dinsdag 4 augustus 2020, 12.00 uur** stellen. Gegadigde moet daarvoor de vragenmodule van TenderNed gebruiken.

Vragen die op een andere manier worden ingediend dan via de vragenmodule van TenderNed beantwoordt de Aanbestedende dienst niet. Alle vragen, de antwoorden daarop en eventueel geconstateerde onvolkomenheden of tegenstrijdigheden maakt de Aanbestedende dienst geanonimiseerd bekend aan alle gegadigden in een nota van inlichtingen. De nota van inlichtingen wordt uiterlijk op **donderdag 13 augustus 2020** gepubliceerd op www.tenderned.nl. Gegadigden moeten de nota van inlichtingen zelf van deze website downloaden.

In verband met het geanonimiseerde karakter van de nota van inlichtingen verzoekt Aanbestedende dienst gegadigden - voor zover dat mogelijk is - in de vraagstelling het gebruik van organisatienamen, productnamen en andere aan zijn organisatie gerelateerde namen zoveel mogelijk te vermijden.

3.4 Sluitingsdatum

Het verzoek tot deelneming moet uiterlijk **donderdag 3 september 2020, 11.00 uur** ingediend zijn via de digitale kluis van TenderNed. Datum en tijd moeten als fatale termijn worden beschouwd, wat betekent dat verzoeken tot deelneming na genoemde datum en tijd niet meer kunnen worden ingediend in TenderNed. Het is niet toegestaan op andere wijze verzoeken tot deelneming in te dienen bij de Aanbestedende dienst.

Na de sluitingsdatum openen twee medewerkers van de Aanbestedende dienst de digitale kluis met de ingediende verzoeken tot deelneming op TenderNed. Er wordt een 'proces-verbaal van opening' gemaakt. Gegadigden kunnen niet bij de opening van de kluis aanwezig zijn.

3.5 Indienen van een verzoek tot deelneming

De gegadigde moet de volgende documenten en verklaringen uploaden in TenderNed in afzonderlijke bestanden (Word of PDF):

- Uniform Europees Aanbestedingsdocument (zie bijlage 1; NB: indien in combinatie wordt ingeschreven en/of met beroep op een derde, dienen meerdere Uniforme Europese Aanbestedingsdocumenten te worden ingediend, zie paragraaf 3.7 en paragraaf 3.8)
- Uittreksel Kamer van Koophandel (zie paragraaf 3.12)
- (eventueel) Terbeschikkingsverklaring derde (bijlage 2)
- Referentieformulieren (bijlage 3 en bijlage 4A en 4B)
- Uitwerking selectiecriteria (zie hoofdstuk 5 en de referentieformulieren in bijlage 4A en 4B)

Het verzoek tot deelneming moet volledig zijn en voldoen aan de bepalingen en gegevens in de aankondiging, de selectieleidraad en eventuele nota's van inlichtingen. De tekst van de verklaringen of bijlagen mag niet worden gewijzigd. Verzoeken tot deelneming worden alleen in behandeling genomen als ze volgens de voorschriften zijn opgemaakt en ingediend. Dit is om een eerlijke concurrentie te garanderen. Een verzoek tot deelneming die op een andere manier wordt aangeboden of die niet aan de voorwaarden voldoet, kan worden uitgesloten van verdere deelname aan de aanbesteding. In dat geval krijgt de gegadigde hierover bericht met vermelding van de reden.

3.6 Akkoordverklaring

Door het indienen van een verzoek tot deelneming verklaart gegadigde zich onvoorwaardelijk akkoord met de opzet en inhoud van de in deze selectieleidraad, inclusief bijlagen, beschreven aanbestedingsprocedure en voorwaarden.

3.7 Verzoek tot deelneming – zelfstandig of combinatie

Ondernemers kunnen zelfstandig of in combinatie met twee of meer ondernemingen een verzoek tot deelneming indienen. Een combinatie van ondernemers geldt als één gegadigde. Indien een gegadigde bestaat uit een combinatie, dan dienen alle ondernemers het Uniform Europees Aanbestedingsdocument (UEA) volledig in te vullen en rechtsgeldig te ondertekenen.

Hierbij wordt specifiek aandacht gevraagd voor het volgende:

- In deel IIA onder het kopje 'wijze van deelneming' moeten alle ondernemers van de combinatie worden benoemd, inclusief de rollen. Bepaal hierbij welke ondernemer binnen de combinatie als verantwoordelijk gevolmachtigde (penvoerder) optreedt namens de andere ondernemers.
- Voor alle ondernemers binnen de combinatie geldt individueel dat ze ingeschreven moeten zijn in het beroeps- of handelsregister of een buitenlandse variant daarvan volgens de wetgeving in het land van vestiging als bedoeld in paragraaf 3.12. Deze informatie moet in deel IIA worden ingevuld en het uittreksel van alle ondernemers moet zijn bijgevoegd bij het verzoek tot deelneming.
- Voor alle ondernemers binnen de combinatie geldt individueel dat de uitsluitingsgronden zoals aangegeven in deel III niet op hun van toepassing mogen zijn. De Aanbestedende dienst controleert de juistheid conform het gestelde in paragraaf 4.2
- Voor de combinatie als geheel geldt dat ze moet voldoen aan de geschiktheidseisen zoals beschreven in paragraaf 4.3 Dit betekent voor het UEA dat alle ondernemers deel IV moeten invullen. Voor het aanleveren van referenties betekent dat deze afkomstig mogen zijn van alle ondernemers binnen de combinatie.

- Door deel te nemen aan een combinatie en het ondertekenen van het UEA verklaart elke ondernemer zich zowel gezamenlijk als hoofdelijk aansprakelijk voor nakoming van verplichtingen die voortvloeien uit het verzoek tot deelneming en in voorkomend geval de inschrijving en overeenkomst.

3.8 Beroep op derde

Indien de gegadigde een beroep wenst te doen op een derde om aan de geschiktheidseisen te voldoen zoals beschreven in hoofdstuk 4, dan dient gegadigde dat aan te geven in deel IIC van het UEA. Hierbij moet de gegadigde toelichten op welke specifieke technische bekwaamheid van de derde dan een beroep wordt gedaan om te kunnen voldoen aan de geschiktheidseisen.

Daarnaast dient er bij een beroep op een derde de volgende documenten te worden gevoegd bij het verzoek tot deelneming. Deze zijn afkomstig van de derde (!) en dienen door de derde rechtsgeldig te worden ondertekend:

- een UEA, waarbij deel IIA en B en deel III is ingevuld;
- een verklaring van de derde als bedoeld in bijlage 2Terbeschikkingsverklaring

De derde waar een beroep op wordt gedaan door gegadigde om te voldoen aan de geschiktheidseisen dient daadwerkelijk te worden ingezet tijdens de uitvoering van de raamovereenkomst. Het vervangen en/of niet langer inzetten van deze derde is uitsluitend toegestaan met voorafgaande schriftelijke toestemming van opdrachtgever.

3.9 Inzet van onderaannemers

Gegadigden kunnen bij de uitvoering van de opdracht werkzaamheden laten uitvoeren door één of meer onderaannemers. Als op het moment van indienen van het verzoek tot deelneming bekend is dat onderaannemers worden ingezet bij uitvoering van de opdracht, moet gegadigde dit aangeven in deel IID van het UEA. Gedurende de looptijd van de overeenkomst mag gegadigde onderaannemers slechts inzetten na toestemming van de opdrachtgever, zie artikel 23 ARBIT-2018.

3.10 Gegadigden van één concern

Als meerdere ondernemingen van één concern willen deelnemen (zelfstandig of als onderdeel van een combinatie) dan wel willen deelnemen als derde bedoeld in paragraaf 3.8, moeten zij – op verzoek van de Aanbestedende dienst – kunnen aantonen dat zij volstrekt onafhankelijk van elkaar opereren in het kader van deze aanbesteding en dat de mededinging hierdoor op geen enkele wijze is of zal worden beïnvloed.

Partijen die dit niet eenduidig en naar genoegen van de Aanbestedende dienst kunnen aantonen, kunnen worden uitgesloten van verdere deelname aan de aanbestedingsprocedure van de desbetreffende inschrijver.

Voor de toepassing van deze paragraaf in elk geval ondernemingen/(rechts)personen die voldoen aan de onderstaande voorwaarden als één concern beschouwd:

a. ondernemingen/(rechts)personen die aan elkaar zijn gelieerd op een wijze als bedoeld in artikel 24a van boek 2 van het Burgerlijk Wetboek; of
b. ondernemingen/(rechts)personen die met elkaar zijn verbonden in een groep als bedoeld in artikel 24b van boek 2 van het Burgerlijk Wetboek; of
c. ondernemingen/(rechts)personen die aan elkaar zijn gelieerd in aan sub a of sub b vergelijkbare rechtsvormen naar buitenlands recht.

3.11 Eén verzoek tot deelneming per onderneming

Een onderneming/(rechts)persoon kan slechts één verzoek tot deelneming indienen voor de aanbesteding. Dit betekent dat het ook niet is toegestaan *zowel* zelfstandig een verzoek tot deelname te doen *als* lid te zijn van een combinatie dan wel tevens deel te nemen als derde in de zin van paragraaf 3.8.

Indien een onderneming meerdere verzoeken tot deelneming indient (zelfstandig en als lid van een combinatie dan wel derde) zal de Aanbestedende dienst alleen het verzoek tot deelneming van de combinatie beoordelen.

3.12 Ondertekening

Alle door gegadigde te ondertekenen documenten, te weten bijlage 1 UEA en (indien van toepassing) bijlage 2, moeten voorzien zijn van handtekeningen van een bevoegd vertegenwoordiger van de gegadigde. De bevoegdheid van ondertekening moet blijken uit het uittreksel van de Kamer van Koophandel, een rechtsgeldige volmacht of inschrijving beroeps- of handelsregister in het land van vestiging of bij ontbreken daarvan een ander bewijsstuk als bedoeld in artikel 2.98 Aanbestedingswet. Wanneer in het beroeps- of handelsregister is opgenomen dat twee of meer personen slechts gezamenlijk vertegenwoordigingsbevoegd zijn, dan moeten de documenten ook door die twee of meer personen ondertekend worden. Wanneer er bij de bevoegdheid tot het vertegenwoordigen van de onderneming beperkingen zijn opgenomen, moet daar rekening mee gehouden worden.

Gegadigde wordt verzocht het uittreksel van de Kamer van Koophandel en/of een volmacht direct mee te sturen met zijn verzoek tot deelneming. Controleer vooraf goed of de handtekeningen die gezet zijn op de verschillende documenten overeenkomen met de bevoegde personen vermeld in het uittreksel. Het uittreksel van de Kamer van Koophandel mag bij het verzoek tot deelneming, niet ouder zijn dan zes (6) maanden gerekend vanaf de sluitingsdatum van het verzoek tot deelneming (zie paragraaf 3.2).

3.13 Nederlandse taal

Alle aanbestedingsstukken zijn in de Nederlandse taal gesteld. De voertaal tijdens de aanbestedingsprocedure en bij de uitvoering van de overeenkomst is de Nederlandse taal. Door gegadigden in te dienen stukken moeten in de Nederlandse taal gesteld zijn. Indien de gevraagde informatie een officieel document betreft dat niet in het Nederlands beschikbaar is, dient naast het originele document een Nederlandse vertaling daarvan te worden bijgevoegd.

3.14 Voorbehouden van de Aanbestedende dienst

De Aanbestedende dienst behoudt zich te allen tijde het recht voor om de aanbestedingsprocedure op te schorten dan wel niet tot selectie over te gaan en/of de aanbestedingsprocedure tussentijds eenzijdig te beëindigen. Gegadigden ontvangen in voorkomend geval schriftelijk bericht van de Aanbestedende dienst.

Indien de Aanbestedende dienst in een laat stadium overgaat tot het afbreken van deze aanbestedingsprocedure, dan zal de Aanbestedende dienst – afhankelijk van de omstandigheden (waaronder het stadium waarin de aanbesteding zich bevindt en de tot dan toe door inschrijvers redelijkerwijs gepleegde inspanningen) – een door Aanbestedende dienst naar vrije bepaling vast te stellen vergoeding betalen voor de door de inschrijvers gemaakte kosten.

3.15 Kostenvergoeding

Aan inschrijvers die in de volgende fase van de aanbesteding (de gunningsfase) een geldige inschrijving hebben ingediend én de raamovereenkomst niet gegund krijgen, zal na afloop van deze aanbestedingsprocedure een vergoeding van € 2.500,- (inclusief btw) worden toegekend.

3.16 Intellectueel eigendom

Het intellectueel eigendom van de selectieleidraad berust bij de Aanbestedende dienst. Behoudens uitzonderingen door de wet gesteld, mag zonder schriftelijke toestemming van de Aanbestedende dienst niets uit de selectieleidraad worden verveelvoudigd anders dan voor het doel van deze aanbestedingsprocedure.

3.17 Staking van bedrijfsactiviteiten of overname

Als tijdens de aanbestedingsprocedure een gegadigde de voor deze aanbesteding relevante bedrijfsactiviteit(en) moet staken of het bedrijf wordt overgenomen, dan moet gegadigde de Aanbestedende dienst direct informeren. In dat geval behoudt de Aanbestedende dienst zich het recht voor deze gegadigde uit te sluiten van deelname aan de procedure.

3.18 Onjuistheden in de selectieleidraad

De selectieleidraad is met zorg samengesteld. De gegadigde moet de Aanbestedende dienst zo spoedig mogelijk, doch uiterlijk twaalf (12) kalenderdagen vóór de sluitingsdatum voor het indienen van het verzoek tot deelneming melden als er toch onvolkomenheden, procedurefouten en/of tegenstrijdigheden voorkomen. Voor het doen van een melding kan uitsluitend de berichtenmodule van TenderNed gebruikt worden. Berichten die op een andere manier worden ingediend dan via TenderNed worden niet beantwoord. Na de hierboven vermelde termijn opgemerkte onvolkomenheden, procedurefouten en/of tegenstrijdigheden die niet eerder door gegadigde zijn waargenomen, zijn voor risico en rekening van gegadigde. In dat geval heeft de gegadigde ter zake zijn rechten verwerkt.

3.19 Nederlands recht en geschillen

Op deze aanbesteding is Nederlands recht van toepassing. Voor alle geschillen die verband houden met deze aanbesteding en de overeenkomst die op grond van de aanbesteding wordt gesloten, is de rechtbank Den Haag de bevoegde rechtelijke instantie.

4 BEOORDELING FORMELE EISEN, UITSLUITINGSGRONDEN EN GESCHIKTHEID

In dit hoofdstuk wordt de beoordeling van de formele eisen uiteengezet en worden de uitsluitingsgronden en geschiktheidseisen beschreven die aan gegadigde worden gesteld. Bij elke eis wordt aangegeven welke documenten moeten worden overlegd als onderdeel van het verzoek tot deelneming dan wel welke documenten pas later tijdens de verificatie als bedoeld in paragraaf 6.1 van de geselecteerde gegadigden wordt verlangd.

Indien een gegadigde niet voldoet aan de gestelde uitsluitingsgronden of geschiktheidseisen dan wordt zijn verzoek tot deelneming terzijde gelegd en niet verder beoordeeld.

4.1 Beoordeling formele eisen

Voordat het verzoek tot deelneming inhoudelijk wordt beoordeeld op de uitsluitingsgronden en geschiktheid, wordt eerst bekeken of het verzoek geldig is. Dat betekent dat er wordt getoetst aan de formele eisen zoals beschreven in deze paragraaf. Indien het verzoek tot deelneming op een of meerdere onderdelen niet voldoet, dan kan de Aanbestedende dienst het verzoek ongeldig verklaren en niet verder meenemen in de beoordeling.

Onverminderd de overige eisen die voortvloeien uit hoofdstuk 3, wordt speciale aandacht gevraagd voor de volgende eisen:

- Het verzoek tot deelneming moet tijdig ontvangen zijn conform paragraaf 3.4
- Het verzoek tot deelneming moet rechtsgeldig ondertekend zijn conform paragraaf 3.12
- Het verzoek tot deelneming moet opgesteld zijn in het Nederlands conform paragraaf 3.13
- Het verzoek tot deelneming moet volledig en volgens de voorschriften zijn opgesteld conform paragraaf 3.5.

Indien het verzoek tot deelneming ongeldig wordt verklaard op basis van de formele eisen zoals gesteld in hoofdstuk 3, dan informeert de Aanbestedende dienst gegadigde hierover zo spoedig mogelijk.

4.2 Uitsluitingsgronden

Gegadigde moet verklaren dat geen van de uitsluitingsgronden zoals beschreven in deel III A, B en C van het UEA op hem van toepassing is door bijlage 1 UEA volledig in te vullen en rechtsgeldig te ondertekenen. Als toelichting op de uitsluitingsgrond ‘ernstige beroepsfout’ zoals bedoeld in deel IIIC van het UEA wordt opgemerkt dat een boete opgelegd door de ACM als indicatie van een beroepsfout wordt gezien.

De Aanbestedende dienst zal de juistheid van het volledig ingevulde UEA van de geselecteerde gegadigden controleren door het opvragen van de bijbehorende bewijsmiddelen. Het gaat om de volgende documenten:

1. Een gedragsverklaring aanbesteden afgegeven door het ministerie van Justitie en Veiligheid. De gedragsverklaring aanbesteden mag niet ouder zijn dan twee (2) jaar, gerekend vanaf de sluitingsdatum van indiening van het verzoek tot deelneming.
2. Een verklaring van de Belastingdienst met betrekking tot betaling van sociale zekerheidspremies en belastingen. De verklaring mag niet ouder zijn dan zes (6) maanden, gerekend vanaf de sluitingsdatum van indiening van het verzoek tot deelneming.

4.3 Geschiktheidseisen

Geschiktheidseisen zijn bedoeld om vast te stellen of de onderneming van gegadigde geschikt is om de gevraagde opdracht zoals beschreven in de selectieleidraad uit te voeren. De gegadigde dient bij deel IV van het UEA te verklaren dat hij aan de gestelde geschiktheidseisen voldoet. De Aanbestedende dienst heeft voor deze aanbesteding de hieronder gestelde eisen geformuleerd.

4.3.1 Technische bekwaamheid en beroepsbekwaamheid

Gegadigde dient aan de hand van zijn referenties aan te tonen dat hij beschikt over de kerncompetenties die nodig zijn voor de uitvoering van deze opdracht. Dit doet gegadigde door gebruik te maken van de referentieformulieren (bijlage 3 en bijlage 4A en 4B)

Gegadigde dient voor kerncompetentie 1 vijf referentieopdrachten van vijf verschillende opdrachtgevers te overleggen. Voor kerncompetentie 2 moeten twee referentieopdrachten van twee verschillende opdrachtgevers worden overlegd. De Rijksoverheid mag voor beide kerncompetenties meerdere keren worden opgevoerd als opdrachtgever, mits het onafhankelijk van elkaar uitgevoerde opdrachten betreft voor verschillende organisatieonderdelen.

Voorts is het toegestaan om één referentieopdracht twee keer op te voeren mits deze voor verschillende kerncompetenties wordt gebruikt (ter verduidelijking, hiermee wordt bedoeld: één referentieopdracht mag één keer voor kerncompetentie 1 en één keer voor kerncompetentie 2 worden ingediend).

De uitvoering van de dienstverlening van de aangeleverde referenties mag niet langer dan drie (3) jaar geleden zijn, gerekend vanaf de sluitingsdatum indienen verzoek tot deelneming (zie paragraaf 3.4). Indien gebruik wordt gemaakt van een nog niet (geheel) afgeronde opdracht mag alleen het werkelijk behaalde resultaat van de opdracht worden opgegeven; een prognose van het te verwachten resultaat zal buiten beschouwing worden gelaten.

Aangezien de Aanbestedende dienst de referenties ook gebruikt om deze te scoren als onderdeel van de selectiecriteria zoals beschreven in hoofdstuk 5, wordt als extra eis gesteld dat gegadigde de referentieformulieren voor kerncompetentie 2 (bijlage 4A en 4B) laat ondertekenen door de referent. De Aanbestedende dienst vraagt deze extra inzet van gegadigde om de betrouwbaarheid van de inhoud van de referentie te vergroten en daarmee de gelijke behandeling van gegadigden bij beoordeling te garanderen.

Conform het gestelde in paragraaf 3.8 kan gegadigde zich beroepen op de technische bekwaamheid van een derde. Door indiening van een referentie geeft de gegadigde aan de Aanbestedende dienst toestemming om de referentie te verifiëren.

De gegadigde wordt gevraagd om op basis van zijn referentie(s) de volgende kerncompetenties aan te tonen:

<u>Kerncompetentie 1: Ervaring met implementatie, beheer en onderhoud van meerdere communities</u>
Gegadigde dient aan te tonen aan minimaal 5 online communities licenties te hebben verstrekt, waarbij gegadigde aanvullend verantwoordelijk was voor implementatie, beheer en onderhoud (niet-inhoudelijk) van deze 5 online communities.

De referenties die worden opgevoerd moet voldoen aan de volgende eisen:

1. Gegadigde heeft voor iedere referent een eigen licentie voor online community tooling beschikbaar gesteld, waarbij gegadigde aanvullend verantwoordelijk was voor implementatie, beheer en onderhoud (niet-inhoudelijk) van elk van deze vijf licenties;
2. De vijf licenties zijn op enig moment, binnen een periode van drie jaar, tegelijkertijd actief in gebruik genomen door de referent en gebruikers/leden van de online communities, waardoor gegadigde deze vijf communities tegelijk heeft voorzien van beheer en onderhoud.
3. Elk van deze vijf online communities is gedurende een onafgebroken periode van minimaal één jaar actief in gebruik geweest.

Voorts geldt voor minimaal twee van de vijf opgevoerde referenties het volgende:
4. De (minimaal) twee online communities bestonden op enig moment binnen de genoemde looptijd van één jaar (eis 3), uit minimaal 500 leden.

Gegadigde dient in het referentieformulier (bijlage 3) voor elk van de 5 referenties de volgende zaken te beschrijven:
- de opdrachtgever;
- doelstelling van de community;
- startdatum van de opdracht;
- startdatum (live-gang) van de community;
- einddatum van de community (indien de community nog actief is: 'NVT');
- aantal leden bij einde van de community (of als deze nog actief is, huidig aantal leden).

Kerncompetentie 2: Ervaring met coaching op het gebied van community management
Gegadigde dient aan te tonen ervaring te hebben met coaching van opdrachtgevers op het gebied van (succesvol) community management voor minimaal twee online communities.

De twee referenties moeten ieder voldoen aan de volgende eisen:
- Gegadigde heeft aan de referent een licentie voor online community tooling beschikbaar gesteld waarbij gegadigde aanvullend verantwoordelijk was voor implementatie, beheer en onderhoud (niet-inhoudelijk) van deze licentie;
- Gegadigde heeft de referent actief gecoacht op het gebied van succesvol en doeltreffend community management, zoals beschreven in paragraaf 2.1.1 (punt 2c Coaching Community management).

Gegadigde dient in de betreffende referentieformulieren (bijlage 4A en 4B) voor beide referenties de volgende zaken te beschrijven:
- de opdrachtgever;
- doelstelling van de community;
- startdatum van de opdracht;
- startdatum (live-gang) van de community;
- einddatum van de community (indien de community nog actief is, NVT);
- aantal leden bij einde van de community (of als deze nog actief is, huidig aantal leden);

Voorts dient gegadigde, ten behoeve van nadere selectie, voor deze twee referentieopdrachten een beschrijving te geven van de opdracht in diezelfde referentieformulieren. In paragraaf 5.1 staat beschreven waaraan deze opdrachtomschrijving moet voldoen en op welke wijze deze verder wordt beoordeeld.

4.3.2 Beroepsbevoegdheid

De gegadigde moet zijn ingeschreven zijn in het beroeps- of handelsregister of een buitenlandse variant daarvan volgens de geldende wetgeving in zijn land van vestiging. Hiertoe dient deel IIA van het UEA worden ingevuld. Om de rechtsgeldige ondertekening vast te stellen op basis van paragraaf 3.12 dient het uittreksel van de Kamer van Koophandel alvast onderdeel uit te maken van het verzoek tot deelneming.

5 SELECTIECRITERIA

In dit hoofdstuk staan de selectiecriteria beschreven ter bepaling van het maximaal aantal van vijf gegadigden die worden uitgenodigd voor de gunningsfase van de aanbesteding. Alleen gegadigden die voldoen aan de formele eisen in hoofdstuk 3 en de uitsluitingsgronden en geschiktheidseisen in hoofdstuk 4 komen voor een beoordeling van de selectiecriteria in aanmerking. Deze criteria zijn dus bedoeld om gegadigden te wegen en kunnen niet meer leiden tot het ongeldig verklaren van een verzoek tot deelneming.

Indien het aantal gegadigden wat voldoet aan de formele eisen, de uitsluitingsgronden en geschiktheidseisen lager of gelijk is aan het maximaal aantal gegadigden voor de gunningsfase, dan zal de Aanbestedende dienst de selectiecriteria niet meer toepassen en gelijk overgaan tot het nemen van de selectiebeslissing, mits het aantal gegadigden voldoende is om de mededinging te waarborgen.

5.1 Uitwerking selectiecriteria

Onverminderd alle eisen en voorwaarden zoals opgenomen in deze selectieleidraad zal selectie plaatsvinden op basis van kerncompetentie 2 *Ervaring met coaching op het gebied van community management* (zie ook paragraaf 4.3):

Gegadigde dient in de referentieformulieren bijlage 4A en 4B een omschrijving van de referentieopdrachten uit te werken.

In de opdrachtomschrijving dient gegadigde minimaal in te gaan op:

- De opdracht: (communicatie)doelstelling(en) van de community (doelstelling(en) kunnen vanzelfsprekend verder gaan dan het vergroten van het aantal (actieve) gebruikers), doelgroep, wensen en randvoorwaarden van de opdrachtgever en de concrete behoefte van opdrachtgever op het gebied van coaching.
- Aanpak: inclusief onderbouwing van gemaakte keuzes ten aanzien van de (inrichting van) de community en coaching van de opdrachtgever.
- Resultaat: Een beschrijving van het door gegadigde beoogde eindresultaat van de beschreven aanpak en de bijdrage die gegadigde heeft geleverd aan het behalen van de doelstelling van opdrachtgever.

LET OP!

- Voor de uitwerking van de opdrachtomschrijving van de referentieopdrachten dient gegadigde maximaal 1.500 woorden te gebruiken.
- Daarnaast mag, per referentie, maximaal één (1) pagina A4 illustraties aan de opdrachtomschrijving toevoegen.
- Woorden in illustraties die van inhoudelijke aard zijn (dat wil zeggen bijdragen aan de uitleg en onderbouwing van de opdrachtomschrijving) worden meegeteld in het maximaal aantal toegestane woorden.

Bij het beoordelen van deze kerncompetentie wordt voor elk van de twee ingediende referenties aan onderstaande aspecten een score gegeven:

R.1 Aanpak
De wijze waarop de door gegadigde ingezette coachingsvorm(en) aansluit bij de doelstelling(en) en randvoorwaarden van de community van de referent. En de mate waarin gegadigde de gekozen aanpak overtuigend heeft onderbouwd en getuigt van expertise op het gebied van community management.

R.2 Resultaat
De mate waarin de ingezette coaching aantoonbaar heeft bijgedragen aan het behalen van de doelstelling(en) van de opdrachtgever.

5.2 Beoordeling selectiecriteria

De Aanbestedende dienst heeft een beoordelingscommissie van vier leden samengesteld voor het beoordelen van de verzoeken tot deelneming op de selectiecriteria. De verzoeken tot deelneming worden door alle leden van de beoordelingscommissie onafhankelijk van elkaar beoordeeld en schrijft zijn beoordeling op zijn eigen beoordelingsformulier. Vervolgens vindt een plenaire beoordelingssessie plaats onder leiding van de projectleider van deze aanbesteding. Zodra consensus is bereikt, druk de beoordelingscommissie de beoordeling uit in een gezamenlijke puntenwaardering. De projectleider legt de score vast op het gezamenlijk beoordelingsformulier. Als beoordelaars geen consensus weten te bereiken, dan bepalen zij de score door meerderheid van stemmen.

De beoordelingscommissie geeft een score op basis van de kerncompetentie K2 De score wordt gegeven volgens onderstaande tabel:

Score	Waardering	Punten
A	Uitstekend - Alle gevraagde elementen en aspecten zijn volledig uitgewerkt. De inhoudelijke uitwerking is helder, logisch, sluit aan bij de (communicatie)doelstelling is en op alle relevante aspecten zeer overtuigend onderbouwd.	10
B	Goed – Alle gevraagde elementen en aspecten zijn volledig uitgewerkt. De inhoudelijke uitwerking is helder en overtuigend onderbouwd en sluit aan bij de (communicatie)doelstelling.	8
C	Voldoende - Alle gevraagde elementen en aspecten zijn volledig of bijna volledig uitgewerkt. De inhoudelijke uitwerking is voldoende helder. Ook is de uitwerking voldoende of in beperkte mate overtuigend onderbouwd en sluit voldoende aan bij de (communicatie)doelstelling.	6
D	Matig – De gevraagde elementen en aspecten zijn slechts ten dele of beperkt uitgewerkt. De inhoudelijke uitwerking is beknopt en slechts in beperkte mate overtuigend onderbouwd en sluit ten dele of beperkt aan bij de (communicatie)doelstelling.	4
E	Onvoldoende - De gevraagde elementen en aspecten zijn slechts ten dele of zeer beperkt uitgewerkt. De inhoudelijke uitwerking is zeer beknopt en niet overtuigend onderbouwd en sluit slechts ten dele of zeer beperkt aan bij de (communicatie)doelstelling.	2
F	Zeer slecht/ontbreekt – De gevraagde elementen en aspecten zijn zeer beperkt of in het geheel niet uitgewerkt. De inhoudelijke uitwerking is onsamenhangend en niet overtuigend onderbouwd. De uitwerking sluit dan ook niet aan bij de (communicatie)doelstelling.	0

Niet ieder aspect weegt even zwaar mee bij het bepalen van de eindscore. In onderstaande tabel staat aangegeven welke weging is toegekend aan de aspecten van de twee referenties van kerncompetentie 2.

		Punten maximaal	**Weging**	**Maximaal te behalen punten na weging**
Referentie A:	R.1A: Aanpak	10	3.5	*35*
	R.2A: Resultaat	10	1.5	*15*
Totaal Referentie A				**50**
Referentie B	R.1B: Aanpak	10	3.5	*35*
	R.2B: Resultaat	10	1.5	*15*
Totaal Referentie B				**50**
Maximaal te behalen punten na weging				**100**

5.3 Proces bij gelijke score

Indien twee (2) of meer gegadigden gelijk eindigen op de laatste plaats in de rangorde die nog toegang geeft tot de gunningsfase van de aanbesteding, dan komt de gegadigde met de hoogste totaal score voor R.1A en R.1B hoger in de rangorde. Indien ook op die kerncompetentie de score gelijk is, dan wordt door middel van loting bepaald welke gegadigde wordt toegelaten tot de gunningsfase.

6 VERIFICATIE EN SELECTIEBESLISSING

6.1 Verificatie

De Aanbestedende dienst zal bewijsvoering opvragen voor de informatie die de gegadigde in het kader van deze aanbestedingsprocedure gegeven heeft. Om de administratieve last te beperken zal de Aanbestedende dienst in eerste instantie aan gegadigden alleen het UEA vragen in plaats van alle bewijsstukken. De bewijsstukken die vallen onder het UEA met uitzondering van de referenties en het uittreksel van de Kamer van Koophandel, worden in principe alleen opgevraagd bij de gegadigden die op basis van de beoordeling in aanmerking komt om te worden geselecteerd voor de gunningsfase. De gevraagde bewijsvoering moet worden geleverd binnen de door de Aanbestedende dienst gestelde termijn. Het betreft de bewijsstukken genoemd in paragraaf 4.2. Als blijkt dat de gegadigde geen bewijsvoering kan leveren of onjuiste informatie heeft gegeven, kan dit alsnog leiden tot uitsluiting van de aanbestedingsprocedure.

6.2 Mededeling selectiebeslissing

De Aanbestedende dienst maakt de selectiebeslissing zo snel mogelijk schriftelijk bekend. Alle gegadigden worden door de Aanbestedende dienst gelijktijdig bericht over de selectiebeslissing. De afgewezen gegadigden ontvangen via de berichtenmodule van TenderNed een brief met de relevante redenen van deze beslissing en de namen van de geselecteerde gegadigden.

De Aanbestedende dienst neemt een standstill periode van twintig (20) kalenderdagen in acht, na de dag van verzending van de mededeling van de selectiebeslissing. Indien een gegadigde bezwaar heeft tegen de selectiebeslissing, dan dient gegadigde binnen deze termijn een kort geding aanhangig te hebben gemaakt, wat moet blijken uit toezending van een kopie van het exploot van dagvaarding. In dat geval zal de Aanbestedende dienst niet tot de gunningsfase overgaan voordat vonnis is gewezen. De termijn van twintig kalenderdagen geldt als een vervaltermijn. Indien niet binnen deze termijn een kort geding aanhangig is gemaakt, kunnen gegadigden geen bezwaar meer maken en hebben zij hun rechten ter zake verwerkt. De Aanbestedende dienst is in dat geval dan ook vrij om te starten met de gunningsfase van de aanbesteding.

BIJLAGE 1 UNIFORM EUROPEES AANBESTEDINGSDOCUMENT

Zie separaat PDF-bestand.

BIJLAGE 2 TERBESCHIKKINGSVERKLARING DERDE

□ Niet van toepassing.
□ Indien van toepassing, vul onderstaande verklaring volledig in.

Lees paragraaf 3.8 om te bepalen of deze verklaring moet worden ondertekend en bijgevoegd bij het verzoek tot deelneming.

VERKLARING DERDE	
Omschrijving van de technische/beroepsbekwaamheid van derde	[omschrijf welke eis het betreft]
Verklaring derde	Ondergetekende verklaart bij de uitvoering van de opdracht haar technische/beroepsbekwaamheid in te zetten ten behoeve van gegadigde.

Ondertekening derde	
Bedrijfsnaam en eventueel rechtsvorm	
Naam rechtsgeldige vertegenwoordiger	
Functie	
Handtekening rechtsgeldige vertegenwoordiger derde	
Plaats, datum	

LET OP: Lees paragraaf 3.12 ter voorkoming van ongeldige ondertekening

BIJLAGE 3 REFERENTIEFORMULIER KERNCOMPETENTIE 1

Toelichting	In deze bijlage dient u de gevraagde informatie van de referentieopdrachten voor kerncompetentie 1 (zoals beschreven in paragraaf 4.3) voor vijf referentieopdrachten (A tot en met E) in te vullen. De controlevragen in de tabel hieronder hebben betrekking op de geschiktheidseisen zoals opgesomd in paragraaf 4.3, lees deze goed.

Referentieopdrachten A tot en met E voor Kerncompetentie 1: Ervaring met implementatie, beheer en onderhoud van meerdere communities	
Controlevragen (indien nee wordt geantwoord, voldoen de referenties niet aan de gestelde eisen. Hiermee voldoet gegadigde niet aan de geschiktheidseisen.)	
Gegadigde heeft voor iedere referent een eigen licentie voor online community tooling beschikbaar gesteld waarbij gegadigde aanvullend verantwoordelijk was voor implementatie, beheer (niet-inhoudelijk) en onderhoud van elk van deze vijf licenties;	☐ Ja ☐ Nee
De vijf licenties zijn op enig moment binnen een periode van drie jaar, tegelijkertijd actief in gebruik genomen door de referent en gebruikers/leden van de online communities, waardoor gegadigde deze vijf communities tegelijk heeft voorzien van implementatie, beheer en onderhoud.	☐ Ja ☐ Nee
Elk van deze vijf online communities is gedurende een onafgebroken periode van minimaal één jaar actief in gebruik geweest.	☐ Ja ☐ Nee
(Minimaal) twee online communities bestonden op enig moment binnen de genoemde looptijd van één jaar (zie hierboven), uit minimaal 500 leden.	☐ Ja ☐ Nee

Referentieopdracht A	
Adres- en contactgegevens referentieopdracht A	
Opdrachtgever	
Adres	
Postcode en plaats	
Contactpersoon	
Functie	
Telefoonnummer	
E-mailadres	
Algemene informatie referentieopdracht A	
Startdatum opdracht (ná 2 september 2017)	
Einddatum opdracht	
Gewerkt in combinatie	☐ Ja ☐ Nee
Gewerkt met onderaannemers	☐ Ja ☐ Nee
Indien gewerkt in combinatie of met onderaannemers: welk gedeelte (of %) is door gegadigde uitgevoerd?	
Opdrachtwaarde	€
Doelstelling van de community	
Startdatum van de community (live-gang)	
Einddatum van de community (indien nog actief: "NVT")	
Aantal leden bij einde van de community (of als deze nog actief is, huidig aantal leden).	

Referentieopdracht B	
Adres- en contactgegevens referentieopdracht B	
Opdrachtgever	
Adres	
Postcode en plaats	
Contactpersoon	
Functie	
Telefoonnummer	
E-mailadres	
Algemene informatie referentieopdracht B	
Startdatum opdracht (ná 2 september 2017)	
Einddatum opdracht	
Gewerkt in combinatie	☐ Ja ☐ Nee
Gewerkt met onderaannemers	☐ Ja ☐ Nee
Indien gewerkt in combinatie of met onderaannemers: welk gedeelte (of %) is door gegadigde uitgevoerd?	
Opdrachtwaarde	€
Doelstelling van de community	
Startdatum van de community (live-gang)	
Einddatum van de community (indien nog actief: "NVT")	
Aantal leden bij einde van de community (of als deze nog actief is, huidig aantal leden).	

Referentieopdracht C	
Adres- en contactgegevens referentieopdracht C	
Opdrachtgever	
Adres	
Postcode en plaats	
Contactpersoon	
Functie	
Telefoonnummer	
E-mailadres	
Algemene informatie referentieopdracht C	
Startdatum opdracht (ná 2 september 2017)	
Einddatum opdracht	
Gewerkt in combinatie	☐ Ja ☐ Nee
Gewerkt met onderaannemers	☐ Ja ☐ Nee
Indien gewerkt in combinatie of met onderaannemers: welk gedeelte (of %) is door gegadigde uitgevoerd?	
Opdrachtwaarde	€
Doelstelling van de community	
Startdatum van de community (live-gang)	
Einddatum van de community (indien nog actief: "NVT")	
Aantal leden bij einde van de community (of als deze nog actief is, huidig aantal leden).	

Referentieopdracht D	
Adres- en contactgegevens referentieopdracht D	
Opdrachtgever	
Adres	
Postcode en plaats	
Contactpersoon	
Functie	
Telefoonnummer	
E-mailadres	
Algemene informatie referentieopdracht D	
Startdatum opdracht (ná 2 september 2017)	
Einddatum opdracht	
Gewerkt in combinatie	☐ Ja ☐ Nee
Gewerkt met onderaannemers	☐ Ja ☐ Nee
Indien gewerkt in combinatie of met onderaannemers: welk gedeelte (of %) is door gegadigde uitgevoerd?	
Opdrachtwaarde	€
Doelstelling van de community	
Startdatum van de community (live-gang)	
Einddatum van de community (indien nog actief: "NVT")	
Aantal leden bij einde van de community (of als deze nog actief is, huidig aantal leden).	

Referentieopdracht E	
Adres- en contactgegevens referentieopdracht E	
Opdrachtgever	
Adres	
Postcode en plaats	
Contactpersoon	
Functie	
Telefoonnummer	
E-mailadres	
Algemene informatie referentieopdracht E	
Startdatum opdracht (ná 2 september 2017)	
Einddatum opdracht	
Gewerkt in combinatie	☐ Ja ☐ Nee
Gewerkt met onderaannemers	☐ Ja ☐ Nee
Indien gewerkt in combinatie of met onderaannemers: welk gedeelte (of %) is door gegadigde uitgevoerd?	
Opdrachtwaarde	€
Doelstelling van de community	
Startdatum van de community (live-gang)	
Einddatum van de community (indien nog actief: "NVT")	
Aantal leden bij einde van de community (of als deze nog actief is, huidig aantal leden).	

BIJLAGE 4A REFERENTIEFORMULIER KERNCOMPETENTIE 2

Toelichting	In deze bijlage dient u de gevraagde informatie van de referentieopdracht(en) voor kerncompetentie 2 (zoals beschreven in paragraaf 4.3) in te vullen. Voor kerncompetentie 2 dient gegadigde één formulier in te vullen per referentieopdracht (bijlage 4A én bijlage 4B). In deze formulieren dient gegadigde tevens de selectiecriteria uit te werken (paragraaf 5.1). Gegadigde mag voor de uitwerking van de opdrachtomschrijving (per referentie) **maximaal 1.500 woorden** gebruiken. Daarnaast mag gegadigde **maximaal één (1) pagina A4 illustraties** aan de opdrachtomschrijving toevoegen. Woorden in illustraties die van inhoudelijke aard zijn (dat wil zeggen bijdragen aan de uitleg en onderbouwing van de opdrachtomschrijving) worden meegeteld in het maximaal aantal toegestane woorden. Gegadigde dient zich strikt aan dit omvangsvoorschrift te houden. Ingevulde referentieformulieren die niet voldoen aan het omvangvoorschrift kunnen terzijde worden gelegd en niet in de (verdere) beoordeling worden meegenomen. **Let op!:** De referent moet akkoord zijn met de opgegeven referentieopdracht door ondertekening van het referentieformulier in het daartoe bestemde vak.

Referentieopdracht A voor Kerncompetentie 2: Ervaring met coaching op het gebied van community management	
Controlevragen (indien nee wordt geantwoord, voldoen de referenties niet aan de gestelde eisen. Hiermee voldoet gegadigde niet aan de geschiktheidseisen.)	
Gegadigde heeft aan de referent een licentie voor online community tooling beschikbaar gesteld waarbij gegadigde aanvullend verantwoordelijk was voor implementatie, beheer en onderhoud van deze licentie;	☐ Ja ☐ Nee
Gegadigde heeft de referent actief gecoacht op het gebied van succesvol en doeltreffend community management, zoals beschreven in paragraaf 2.1.1 (punt 2c Coaching Community management).	☐ Ja ☐ Nee

Adres- en contactgegevens referentieopdracht A	
Opdrachtgever	
Adres	
Postcode en plaats	
Contactpersoon	
Functie	
Telefoonnummer	
E-mailadres	
Algemene informatie referentieopdracht A	
Startdatum opdracht (ná 2 september 2017)	
Einddatum opdracht	
Gewerkt in combinatie	☐ Ja ☐ Nee
Gewerkt met onderaannemers	☐ Ja ☐ Nee
Indien gewerkt in combinatie of met onderaannemers: welk gedeelte (of %) is door gegadigde uitgevoerd?	
Opdrachtwaarde	€
Doelstelling van de community	
Startdatum van de community (live-gang)	
Einddatum van de community (indien nog actief: "NVT")	
Aantal leden bij einde van de community (of als deze nog actief is, huidig aantal leden).	

Opdrachtomschrijving referentieopdracht A **Let op: zorg ervoor dat u alle genoemde punten (opdracht, aanpak en resultaat, zie paragraaf 5.1) aan bod laat komen.**	
Opdrachtomschrijving	[In dit veld geeft u een beschrijving van de referentieopdracht, waaruit moet blijken dat wordt voldaan aan de gestelde eisen uit de kerncompetentie en op basis waarvan de referentieopdracht wordt beoordeeld op de genoemde aspecten in paragraaf 5.1]

Ondertekening referent	
Bedrijfsnaam	
Naam / Functie vertegenwoordiger	
Handtekening vertegenwoordiger	
Plaats, datum	

BIJLAGE 4B REFERENTIEFORMULIER KERNCOMPETENTIE 2

Toelichting	In deze bijlage dient u de gevraagde informatie van de referentieopdracht(en) voor kerncompetentie 2 (zoals beschreven in paragraaf 4.3) in te vullen. Voor kerncompetentie 2 dient gegadigde één formulier in te vullen per referentieopdracht (bijlage 4A én bijlage 4B). In deze formulieren dient gegadigde tevens de selectiecriteria uit te werken (paragraaf 5.1). Gegadigde mag voor de uitwerking van de opdrachtomschrijving (per referentie) **maximaal 1.500 woorden** gebruiken. Daarnaast mag gegadigde **maximaal één (1) pagina A4 illustraties** aan de opdrachtomschrijving toevoegen. Woorden in illustraties die van inhoudelijke aard zijn (dat wil zeggen bijdragen aan de uitleg en onderbouwing van de opdrachtomschrijving) worden meegeteld in het maximaal aantal toegestane woorden. Gegadigde dient zich strikt aan dit omvangsvoorschrift te houden. Ingevulde referentieformulieren die niet voldoen aan het omvangvoorschrift kunnen terzijde worden gelegd en niet in de (verdere) beoordeling worden meegenomen. **Let op!:** De referent moet akkoord zijn met de opgegeven referentieopdracht door ondertekening van het referentieformulier in het daartoe bestemde vak.

Referentieopdracht B voor Kerncompetentie 2: Ervaring met coaching op het gebied van community management	
Controlevragen (indien nee wordt geantwoord, voldoen de referenties niet aan de gestelde eisen. Hiermee voldoet gegadigde niet aan de geschiktheidseisen.)	
Gegadigde heeft aan de referent een licentie voor online community tooling beschikbaar gesteld waarbij gegadigde aanvullend verantwoordelijk was voor implementatie, beheer en onderhoud van deze licentie;	☐ Ja ☐ Nee
Gegadigde heeft de referent actief gecoacht op het gebied van succesvol en doeltreffend community management, zoals beschreven in paragraaf 2.1.1 (punt 2c Coaching Community management).	☐ Ja ☐ Nee

Adres- en contactgegevens referentieopdracht B	
Opdrachtgever	
Adres	
Postcode en plaats	
Contactpersoon	
Functie	
Telefoonnummer	
E-mailadres	
Algemene informatie referentieopdracht B	
Startdatum opdracht (ná 2 september 2017)	
Einddatum opdracht	
Gewerkt in combinatie	☐ Ja ☐ Nee
Gewerkt met onderaannemers	☐ Ja ☐ Nee
Indien gewerkt in combinatie of met onderaannemers: welk gedeelte (of %) is door gegadigde uitgevoerd?	
Opdrachtwaarde	€
Doelstelling van de community	
Startdatum van de community (live-gang)	
Einddatum van de community (indien nog actief: "NVT")	
Aantal leden bij einde van de community (of als deze nog actief is, huidig aantal leden).	

Opdrachtomschrijving referentieopdracht B **Let op: zorg ervoor dat u alle genoemde punten (opdracht, aanpak en resultaat, zie paragraaf 5.1) aan bod laat komen.**	
Opdrachtomschrijving	[In dit veld geeft u een beschrijving van de referentieopdracht, waaruit moet blijken dat wordt voldaan aan de gestelde eisen uit de kerncompetentie en op basis waarvan de referentieopdracht wordt beoordeeld op de genoemde aspecten in paragraaf 5.1]

Ondertekening referent	
Bedrijfsnaam	
Naam / Functie vertegenwoordiger	
Handtekening vertegenwoordiger	
Plaats, datum	

BIJLAGE 5 (CONCEPT-)PROGRAMMA VAN EISEN
Begripsbepalingen

In dit concept-programma van eisen wordt een aantal begrippen met een hoofdletter geschreven. Deze begrippen kennen uitsluitend de betekenis zoals hieronder gedefinieerd:

- **Opdrachtgever:** de Staat der Nederlanden vertegenwoordigd door Dienst Publiek en Communicatie (DPC)
- **Opdrachtnemer:** de wederpartij van Opdrachtgever
- **Community:** een online community is een groep mensen met een gezamenlijk doel, belang of interesse waarvan de leden elkaar primair online treffen op een speciaal daarvoor bedoeld (afgeschermd) platform. Een online community kan los van organisatiegrenzen functioneren. De leden van de community communiceren of werken met elkaar om samen meer te weten of te kunnen dan ieder afzonderlijk.
- **Groepen:** binnen een community zijn er groepen, die beschouwd kunnen worden als subcommunities. Deze groepen kunnen open of besloten zijn.
- **Open groepen:** Leden van Communities kunnen lid worden van open groepen om daar vervolgens interactie aan te gaan. De inhoud van open groepen is, afhankelijk van de inrichting, zichtbaar voor Bezoekers en/of Leden van de Community.
- **Besloten groepen:** Lidmaatschap voor besloten groepen kan enkel op uitnodiging of via het aanvragen van lidmaatschap bij de Groepsbeheerder. De inhoud van besloten groepen is alleen zichtbaar voor Leden van de besloten groep.
- **Bezoeker:** bezoeker van de Community, maar heeft geen account. Kan alleen bij openbare informatie en, afhankelijk van de inrichting, Open groepen, maar kan geen content delen.
- **Leden**: deelnemer aan de community en medewerker van de Rijksoverheid (met een e-mail adres van de Rijksoverheid). Dat wil zeggen dat hij/zij een account heeft, waarmee hij/zij rechten heeft om actief bij te dragen aan de community.
- **Externe Leden**: deelnemer aan de community van buiten de Rijksoverheid (zonder een e-mail adres van de Rijksoverheid). Dat wil zeggen dat hij/zij een account heeft, waarmee hij/zij rechten heeft om actief bij te dragen aan de community.
- **Groepsbeheerder:** iedere ambtenaar kan groepsbeheerder worden, mits de Groep is goedgekeurd door de Community manager. De groepsbeheerder staat hiërarchisch boven Leden, wat betekent dat alles wat Leden kunnen de groepsbeheerder ook kan.
- **Community manager:** de community manager heeft rechten over alle groepen heen. De community manager monitort de gehele Community. De community manager staat hiërarchisch boven de Groepsbeheerder, wat betekent dat alles wat Leden en de Groepsbeheerder kunnen, de community manager ook kan.

Functionele en technische eisen
In deze paragraaf worden functionaliteiten en enkele technische eisen beschreven waaraan de SAAS Community Tool minimaal moet voldoen bij start dienstverlening. In aanvulling op onderstaande kan het voorkomen dat, gedurende de looptijd van de raamovereenkomst aanvullende functionaliteiten gewenst zijn. In deze gevallen zal Opdrachtgever hierover aanvullende afspraken maken met Opdrachtnemer.

Algemene en Technische Functionaliteiten

1. **Rollen en rechten (Access Control List)**
   Opdrachtnemer richt de Community in met minimaal de rollen: Leden, Groepsbeheerder en Community manager. De rechten die een bepaalde rol heeft hangen samen met wat voor functionaliteiten en content er voor deze rol zichtbaar zijn. Ter illustratie: lidmaatschap van een Besloten groep heeft logischerwijs invloed op de zichtbaarheid van content en Leden; zo

kunnen bijvoorbeeld bijdragen van Leden van een Besloten groep niet worden ingezien door niet-Leden van deze Groep. Wanneer Leden besluiten al hun bijdragen zichtbaar te maken op hun profielpagina, dan nog steeds geldt dat bijdragen uit de Besloten groep alleen getoond worden aan Leden van diezelfde Besloten groep.

Opdrachtnemer maakt dus per rol alleen zichtbaar wat zichtbaar mag zijn.

2. Extra rollen definiëren

Per Community moeten extra rollen (met andere rechten) toegevoegd kunnen worden. Dit kan noodzakelijk zijn voor het behalen van de doelstelling(en) van de betreffende Community. Opdrachtnemer adviseert opdrachtgevers in de keuzemogelijkheden.

3. Toegankelijkheidseisen

De community tool voldoet aan de geldende eisen voor rijkswebsites (www.eisenrijkswebsites.nl). Opdrachtnemer zorgt ervoor dat hij op de hoogte blijft van eventuele wijzigingen/updates ten aanzien van de geldende eisen en dat deze binnen een redelijke termijn worden doorgevoerd voor de community tool.

4. Mobiele app

Opdrachtnemer stelt aan alle Leden van de Community een mobiele app beschikbaar, minimaal geschikt voor gebruik op Android en iOS devices. De Community is daarmee voor Leden dus ook benaderbaar via een mobiele app. Deze mobiele app voldoet minimaal aan de eisen die gelden voor Digitale Toegankelijkheid (waaronder Responsive Web Design). De app ondersteunt minimaal het ontvangen van notificaties/pushberichten, waarmee Leden op de hoogte blijven van nieuwe content (zelfde mogelijkheden als genoemd in punt 15 van Functionaliteiten Leden) en het posten van berichten.

5. Aansluitvoorwaarden Single Sign On (SSOn)

Opdrachtnemer voldoet aan de volgende aansluitvoorwaarden applicaties SAML2.0:

- aansluiting na goedkeuring systeemeigenaar en technisch eigenaar;
- applicatie is een webservice;
- inlogfunctionaliteit; geldig inlogaccount op de te ontsluiten applicaties via Single Sign On;
- handmatig inloggen met username/wachtwoord als authenticatiemiddel blijft mogelijk naast Single Sign On functionaliteit;
- applicatie levert SAML 2.0 koppelvlak en wordt ontsloten via Rijksweb VPN;
- het SAML2.0 koppelvlak wordt via een trust gekoppeld aan het SSOn Rijk-koppelvlak (ondersteunde profiles, identifier + attributen);
- autorisatie wordt afgehandeld door applicatie. De applicatie neemt wel de juiste autorisatiebeslissing om op basis van de claim (en attributen) van de federatieve gebruiker het toegangsniveau te bepalen als deze een applicatie of service benadert
- primair E-mailadres wordt gebruikt als identifier;
- de Single Sign On-functionaliteit met een mobile-app kan alleen via een beveiligde MDM-voorziening (zoals GOOD) op de smartphone/tablet worden gefaciliteerd.

Bovenstaande voorwaarden zijn afkomstig van SSC ICT, het rijksbrede Shared Service Center ICT waar opdrachtgevers op aangesloten moeten worden bij implementatie van SSOn.

6. Laagdrempelige toegang via Rijksportaal

- De applicatie is voorzien van RESTful API's ingericht conform de standaarden (REST API DesignRules – Forum Standaardisatie) en voorziet in mogelijkheden om communityberichten en persoonlijke berichten op te halen.

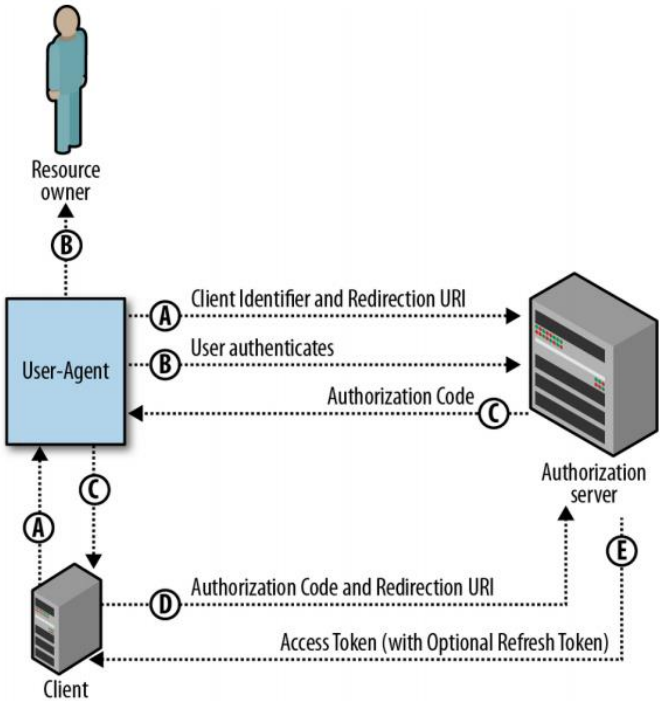
Opdrachtnemer implementeert een REST server interface met GET requests en JSON responses naar onderstaand voorbeeld (of komt met een eigen oplossing afgestemd met SSC ICT). Toegang tot persoonsgebonden berichten is beveiligd met OAuth2 via server-side web application flow.

GET Request:
GET persoonlijkeberichten

JSON response:
Response op 'persoonlijkeberichten' request is een JSON array met objecten waarin de berichten zitten. Een bericht bestaat uit een header, een body en een url.

```
[
        {
                head: "koptekst 1",
                body: "bodytekst 1",
                url: https://verwijzingnaardeeerstebron.nl
        },
        {
                head: "koptekst 2",
                body: "bodytekst 2",
                url: https://verwijzingnaardetweedebron.nl
        }
]
```

OAUth2 Server-side Web Application flow:



7. Zoeken en vinden

Opdrachtnemer levert een zoekmachine binnen de Community waarmee Leden invloed kunnen uitoefenen op de presentatievolgorde van de zoekresultaten (ondersteund wordt als twee aparte mogelijkheden het sorteren op relevantie en het sorteren op datum). Het zoeken op booleaanse operatoren (EN/OF) wordt eveneens ondersteund. Opdrachtnemer indexeert elke Community full-tekst en toont alleen die resultaten waartoe Leden gerechtigd zijn.

8. Domein

Opdrachtnemer communiceert geen eigen URL's naar externen. Leveranciersbranding is niet toegestaan. De verschillende Communities worden onder eigen domeinnamen van opdrachtgevers gehost.

Functionaliteiten voor Leden

1. Toegang tot de community

Bezoekers met een e-mail adres van de Rijksoverheid kunnen via de Community website toegang tot de Community aanvragen (lid worden). Bezoekers zonder e-mail adres van de Rijksoverheid kunnen alleen lid (Externe Leden) worden van een community op uitnodiging van een Community Manager.

Bezoekers krijgen een goedkeuring of afwijzing via het opgegeven mailadres. De gebruikersnaam bij aanmelding moet gebaseerd zijn op de echte naam van de gebruiker. (Externe) Leden kunnen zelf een (vergeten) wachtwoord instellen.

2. Toegang tot een Groep voor Leden

Opdrachtnemer ondersteunt een inrichting van een Community met Open en Besloten Groepen. Opdrachtnemer zorgt ervoor dat alle Groepen minimaal een titel en korte omschrijving bevatten, dat de Groepsbeheerder bekend is en dat er contact opgenomen kan worden met de Groepsbeheerder(s). Deze functionaliteit is zichtbaar voor alle Leden.

a. Open groepen

De inhoud van Open groepen is zichtbaar voor Leden. Om interactie aan te kunnen gaan binnen een Open groep, moeten Leden wel lid worden van die Open groep.

b. Besloten groepen

Om de inhoud te zien van Besloten groepen is toegang van de Groepsbeheerder noodzakelijk. Na goedkeuring door de Groepsbeheerder kunnen Leden naast het zien van de inhoud ook direct interactie aangaan (zelf content delen of reageren). Zie verder punt 1 en 2 bij Functionaliteiten voor Groepsbeheerders.

3. Toegang tot een Groep voor Externe Leden

Externe Leden kunnen enkel op uitnodiging van een Groepsbeheerder lid worden van een Groep en kunnen geen andere Open en Besloten Groepen binnen die Community zien tenzij hiervoor rechten zijn toegekend door Groepsbeheerder of Community Manager.

4. Profielpagina Leden

Alle Leden en Externe Leden (hierna: Leden, tenzij expliciet anders aangegeven) krijgen een eigen profielpagina die bestaat uit een standaardset aan basisgegevens (verplicht) en aanvullende gegevens (optioneel). Een profielpagina bestaat minimaal uit '(gebruikers)naam' en een overzicht van de persoonlijke bijdragen die via de Community/Groep zijn gepubliceerd. Bijdragen uit besloten Groepen zijn uiteraard alleen zichtbaar als de persoon lid is van deze besloten Groep.

De aanvullende (optionele) gegevens kunnen per Community verschillen. Opdrachtnemer bespreekt en adviseert opdrachtgevers over de mogelijkheden bij de inrichting van de Community.

5. Bijdragen en reacties

Bijdragen in de vorm van tekst, audio, beeld en bestanden kunnen worden:

- Aangemaakt/geüpload
- Gepubliceerd
- Gewijzigd
- Verwijderd

6. Informatie bij bijdragen en reacties

Opdrachtnemer zorgt ervoor dat bijdragen en de reacties op bijdragen minimaal basisinformatie zoals publicatiedatum, -tijdstip en gebruikersnaam van de Leden bevatten.

7. Content aanmaken en publiceren

Leden kunnen, afhankelijk van de toebedeelde rechten, content (tekst, plaatjes, audio, (embedded) video, documenten) aanmaken, opmaken, publiceren en wijzigen.

Minimaal ondersteund zijn de bestandstypen:

- PDF;
- Excel;
- Word;
- Powerpoint;
- OpenDocument;
- JPG;
- PNG;
- GIF;
- mp4;
- wmv.

Bij de inrichting wordt per Community door de Community Manager bepaald welke van de bovengenoemde bestandstypen zijn toegestaan.

8. Content verwijderen

Leden kunnen hun eigen bijdrage zonder tussenkomst van anderen verwijderen, wanneer zij dit wensen. Opdrachtnemer zorgt voor een extra attentie die Leden bevestigend moeten beantwoorden, alvorens content wordt verwijderd.

9. Publicatiemechanisme

Leden kunnen bijdragen uitgesteld publiceren en depubliceren zonder te verwijderen.

10. Interactie op content

Leden kunnen op gedeelde content reageren en andere Leden en onderwerpen in de reactie *taggen* (middels gebruikersnaam). Het reageren op gedeelde content kan door de Community manager of Groepsbeheerder worden uitgeschakeld (zie ook rechten Groepsbeheerder).

11. Mijn Account

Via "mijn account" kunnen Leden de volgende zaken zelf instellen:

a. Wachtwoord wijzigen
b. Notificaties aan-/uitzetten (zie functionaliteiten Leden punt 15)
c. Contactgegevens wijzigen

12. Wachtwoord vergeten

De Opdrachtnemer biedt via de Community een inlogscherm aan waar Leden een wachtwoord wijziging aan kunnen vragen. Opdrachtnemer gebruikt voor een wachtwoordwijziging het mailadres waarmee destijds de aanmelding is gedaan. Leden ontvangen (geautomatiseerd) een mail met een link om een nieuw wachtwoord aan te maken.

13. Agenda-items aanmaken en delen

Leden kunnen zich aan- en afmelden voor evenementen op de volgende wijze: na aanmelding ontvangen Leden een mail met een ICS (of vergelijkbaar) waarmee het evenement direct in de eigen agenda (bijvoorbeeld Microsoft Outlook) kan worden opgenomen. Wanneer een evenement het maximaal aantal deelnemers heeft bereikt, worden overige aanmeldingen op de Reservelijst geplaatst en worden de betreffende Leden daarvan op de hoogte gebracht via de mail. Afmelden kan via de evenementenpagina of via de mail.

Leden kunnen ook zelf agenda-items aanmaken (met een maximaal aantal deelnemers en een reservelijst), ook voor events die niet door hem/haar zelf zijn georganiseerd (tippen). Ook deze agenda-items kunnen in de eigen externe agenda's (ICS of vergelijkbaar) worden opgenomen.

14. Groepen aanmaken

Afhankelijk van de inrichting per Community is het mogelijk voor Leden (let op: maar dit geldt nooit voor Externe Leden) om zelf Groepen aan te maken binnen de Community. Degene die een groep aanmaakt is daarmee ook automatisch Groepsbeheerder van die Groep. Opdrachtnemer kijkt samen met opdrachtgevers per Community of deze inrichting gewenst is.

15. Notificaties, op de hoogte blijven

Leden kunnen zich abonneren op notificaties) per Groep, persoon, onderwerp, pagina en eigen persoonlijke naamtag. Notificaties worden minimaal via mail en notificaties vanuit de mobiele app verstuurd.

Daarnaast kunnen Leden ervoor kiezen om alleen van die onderdelen op de hoogte te worden gehouden waarin zij zelf geparticipeerd hebben. Alle type notificaties kunnen per onderdeel door Leden zelf aan of uit worden gezet. Bij het aanzetten hebben Leden de keuze voor opt-in voor real-time, dagelijks of wekelijkse samenvattingen. Bij het uitzetten is het ook mogelijk om te kiezen voor een volledige opt-out. Na inlog in de Community is zichtbaar dat er nieuwe notificaties zijn.

16. Digitale export

Opdrachtnemer biedt huidige Leden de mogelijkheid om alle data die zij ooit in de Community hebben toegevoegd te exporteren naar een veelgebruikt format (digitaal bestand).

17. Lidmaatschap opzeggen

Binnen de Community hebben Leden de mogelijkheid om zich uit te schrijven. Dat wil zeggen dat het lidmaatschap van een Groep en/of van de totale Community is op te zeggen. Definitief uitschrijven moet bevestigd worden via de mail.

Functionaliteiten voor Groepsbeheerders
De Groepsbeheerder moet beschikken over alle functionaliteiten en mogelijkheden waarover Leden kunnen beschikken. Aanvullende functionaliteiten staan hieronder opgesomd:

1. **Toegang tot een Open groep en Besloten groep zonder uitnodiging**
   Groepsbeheerders van Open groepen en Besloten groepen zonder uitnodiging ontvangen een notificatie (minimaal via mail en app) wanneer een lidmaatschap wordt aangevraagd. De Groepsbeheerder kan deze aanvragen goedkeuren, maar ook afwijzen. Goedkeuring kan ook automatisch verlopen aan de hand van een lijst met domeinen of specifieke mailadressen.

2. **Besloten Groep op uitnodiging**
   Van sommige Besloten groepen kunnen Leden alleen lid worden op uitnodiging (minimaal via de mail). Leden krijgen bij deze Besloten groepen dan geen aanmeldknop of vergelijkbaar te zien (zie punt 2b Functionaliteiten voor Leden). In plaats daarvan zorgt Opdrachtnemer voor een alternatieve aanmeldmogelijkheden voor Besloten groepen. De Groepsbeheerder bepaalt of gebruik wordt gemaakt van deze mogelijkheid.

3. **Monitoren bezoek van Groepen**
   Opdrachtgevers maken intensief gebruik van webstatistieken (momenteel wordt gebruik gemaakt van Piwik). Groepsbeheerders moeten middels deze webstatistieken het bezoek kunnen analyseren. Opdrachtnemer moet een door Opdrachtgever aangeboden (Piwik) code implementeren en beschikbaar stellen in de Community.

4. **Monitoren engagement op Groepen**
   Opdrachtnemer levert statistieken voor engagement (minimaal het aantal likes en aantal reacties per bericht en per Groep).

5. **Berichten van de Groepsbeheerder**
   Groepsbeheerders kunnen berichten versturen (minimaal via mail en notificaties van de mobiele app) naar alle Leden binnen de Groep tegelijkertijd.

6. **Poll**
   De community biedt de optie om een poll toe te voegen aan een Groep. Middels deze poll kan de Groepsbeheerder naar de mening van zijn/haar Leden vragen. De poll bestaat uit meerdere vooraf gedefinieerde antwoorden, er kan slechts één antwoord worden gekozen en kan maar één keer (per poll) per account worden ingevuld.

   De resultaten van de poll kunnen minimaal na afloop van de poll door de Groepsbeheerder worden gedeeld.

7. **Organiseren van evenementen en vergaderingen**
   Opdrachtnemer zorgt ervoor dat Groepsbeheerders evenementen kunnen aanmaken, daarvoor Leden kunnen uitnodigen en registraties van aanmeldingen voor een evenement beheren en wijzigen. Hiertoe dient de Groepsbeheerder minimaal een deelnemerslijst en reservelijst te kunnen genereren (CSV-bestand).

8. Reservelijst evenementen en vergaderingen

Leverancier biedt de mogelijkheid om een reservelijst met auto-aanmelding in te zetten voor evenementen en vergaderingen. Dat wil zeggen: bij afmelding, dan is de eerstvolgende aanmelding (op basis van aanmeldvolgorde) aan de beurt. Vervolgens wordt hij/zij automatisch aangemeld voor het evenement en krijgt daarvan een automatisch aangemaakte notificatie (zie punt 10 Leden).

9. Voorpagina van een Groep

Groepsbeheerders kunnen de landingspagina van een Groep naar eigen inzicht inrichten. Het gaat dan om inrichting van functionele mogelijkheden, hiermee wordt minimaal bedoeld:

- het kunnen toevoegen van blokken tekst (inclusief links);
- toevoegen van afbeeldingen;
- overzicht van de Leden;
- (selectie van) berichten (chronologisch, op basis van trefwoorden) uit de tijdlijn en agenda.

10. Content onzichtbaar maken

De Groepsbeheerder kan content (berichten, reacties, evenementen) op onzichtbaar zetten. Op de plek waar content onzichtbaar is gemaakt kan in plaats daarvan een melding worden getoond waarom deze content niet meer zichtbaar is.

11. Interactie vergrendelen

De Groepsbeheerder kan de mogelijkheid om te reageren op content vergrendelen. Hiermee wordt het mogelijk om een bericht te publiceren waar door Leden niet op gereageerd kan worden. Ook kan hiermee bijvoorbeeld de discussie die gaande is op een bepaald bericht worden gesloten.

12. Meerdere Groepsbeheerders per Groep

Een Groep kan meerdere Groepsbeheerders hebben.

13. Formulieren editor

De Groepsbeheerder kan vragen stellen aan Leden middels een formulier. Dit formulier moet door de Groepsbeheerder zelf worden samengesteld. Opdrachtnemer zorgt ervoor dat Groepsbeheerders minimaal de volgende types invulvelden kunnen gebruiken:

- tekstveld - veld voor 1 regel tekst;
- tekstvak - veld voor langere tekst,
- datumveld (dd/mm/jjjj)
- uploadveld - invuller kan bestand meesturen (alleen toegestane bestandstypen gedefinieerd tijdens de inrichting).

Per veld kan de Groepsbeheerder aangeven of dit een verplicht veld is. Output moet beschikbaar worden gesteld aan de Groepsbeheerder in CSV-format (of vergelijkbaar).

Functionaliteiten voor Community Managers

De Community manager moet beschikken over alle functionaliteiten en mogelijkheden waarover de Groepsbeheerder kan beschikken. Aanvullende functionaliteiten staan hieronder opgesomd:

1. **Toegang tot de community**

   De Community tooling dient de volgende toegangsmogelijkheden te ondersteunen:

   - Bezoekers zijn na aanvraag automatisch lid; en/of
   - De Community manager kan automatisch aan de hand van een domeinenlijst (bijvoorbeeld @az.nl) of een lijst met daarin specifieke e-mailadressen opgenomen Bezoekers uitnodigen voor de Community; en/of
   - Elk aangevraagd lidmaatschap kan handmatig door de Community manager worden geaccordeerd.

   Community managers kunnen de gewenste wijze van autorisatie zoveel mogelijk zelf, zonder tussenkomst van de leverancier, inrichten.

2. **Toekennen van rollen en rechten Groepsbeheerder**

   De Community manager moet naar eigen inzicht Groepsbeheerder(s) kunnen toevoegen of verwijderen en per Groepsbeheerder rollen en rechten kunnen toekennen.

3. **Vormgeving Community**

   De Community manager heeft zelf invloed op de vormgeving voor zijn/haar Community. Community managers kunnen kiezen uit elk van de beschikbare mogelijkheden qua stijlen die zijn samengesteld op basis van de Rijkshuisstijl.

4. **Bestaande groepsinrichting hergebruiken**

   De Community tooling ondersteunt dat Community managers een bestaande inrichting (van een Groep) kunnen kopiëren voor hergebruik in een nieuwe Groep.

5. **Berichten van de Community manager**

   De Community tool ondersteunt dat de Community manager middels het versturen van berichten met alle Leden van de Community (tegelijkertijd) kan communiceren.

6. **Structuur in Groepen**

   De Community tool ondersteunt de mogelijkheid om verbanden tussen en hiërarchie ten opzichte van verschillende Groepen (binnen een Community) door de Community manager zichtbaar te maken.

7. **Pagina's los van een Groep**

   Opdrachtnemer zorgt ervoor dat de Community manager content kan publiceren los van een Groep voor bijvoorbeeld, maar niet uitsluitend, 'vraag & antwoord'-pagina's of 'help'-pagina's.

8. **Leden op inactief zetten**

   Opdrachtnemer zorgt ervoor dat Community managers de optie hebben om Leden op inactief te zetten (toegangsrechten in te trekken). Leden dienen na een (nader in te stellen) periode automatisch op inactief te worden gezet, waardoor ze geen toegang meer tot de Community hebben. Ze worden echter niet verwijderd uit het systeem.

9. Content na beëindiging lidmaatschap

Opdrachtnemer biedt drie mogelijkheden voor het verwijderen/aanpassen van content van voormalige Leden. Dit zijn:

a. alle berichten van deze persoon blijven gehandhaafd binnen de Community zoals tijdens lidmaatschap; of

b. alles wordt geanonimiseerd (niet herleidbaar naar het individu) en blijft staan; of

c. alle berichten worden verwijderd.

Opdrachtnemer zorgt ervoor dat alle bovengenoemde opties geautomatiseerd kunnen worden doorgevoerd in betreffende Groepen/Communities.

Opdrachtnemer zorgt ervoor dat de Community manager ook na een beëindigd lidmaatschap een digitale export kan leveren van de content van voormalige Leden.

BIJLAGE 6 LIJST DEELNEMENDE ORGANISATIES

Ministerie van Algemene Zaken:
- Kerndepartement
- Dienst Publiek en Communicaite (DPC)
- Bureau voor de Wetenschappelijke Raad voor het Regeringsbeleid (WRR)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties:
- Kerndepartement
- SSC-ICT
- Rijksdienst voor Identiteitsgegevens (RvIG) (voorheen BPR)
- Logius
- Uitvoeringsorganisatie Bedrijfsvoering Rijk UBR (voorheen DWM)
- Rijksvastgoedbedrijf (RVB)
- Dienst Huurcommissie
- P-Direkt
- Doc Direkt
- FM Haaglanden

Ministerie van Buitenlandse Zaken:
- Europese Samenwerking
- Internationale Samenwerking
- Politieke Zaken
- Buitenlandse Economische Betrekkingen
- de PSG kolom

Ministerie van Economische Zaken en Klimaat:
- Bestuursdepartement (inclusief Adviescollege Toetsing Regeldruk (ATR) maar **exclusief** de Nationaal Coördinator Groningen (NCG))
- Rijksdienst voor Ondernemend Nederland (RVONL) (inclusief PIANOo Expertisecentrum Aanbesteden)
- Autoriteit Consument en Markt (ACM)
- Dienst ICT Uitvoeringsorganisatie (DICTU)
- Agentschap Telecom (AT)
- Staatstoezicht op de Mijnen (SodM)

Ministerie van Financiën:
- Kerndepartement
- Domeinen Roerende Zaken (DRZ)

Ministerie van Infrastructuur en Waterstaat:
- Bestuurskern
- Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)
- Inspectie Leefomgeving en Transport (ILT)
- Rijkswaterstaat (RWS)
- KNMI

Ministerie van Justitie en Veiligheid:

- Bestuursdepartement (inclusief Dienst Justis en Dienst Terugkeer en Vertrek (DT&V))
- Openbaar Ministerie (OM)
- Centraal Justitieel Incassobureau (CJIB)
- Wetenschappelijk Onderzoek en Documentatiecentrum (WODC)

Ministerie van Landbouw, Natuur en Voedselkwaliteit:

- Bestuursdepartement

Ministerie van Onderwijs, Cultuur en Wetenschap:

- Bestuursdepartement
- Dienst Uitvoering Onderwijs (DUO)
- Rijksdienst voor het Cultureel Erfgoed (RCE)
- Nationaal Archief (NA)
- Inspectie van het Onderwijs (IvhO)
- Erfgoedinspectie (EGI)
- Onderwijsraad (OR)
- Adviesraad voor het Wetenschaps- en Technologiebeleid (AWT)
- College voor Toetsen en Examens (CvTE)
- Raad voor Cultuur (RvC)

Ministerie van Volksgezondheid, Welzijn en Sport

- Bestuursdepartement
- Gezondheidsraad (GR)
- Rijksinstituut voor de Volksgezondheid en Milieu (RIVM)
- Sociaal en Cultureel Planbureau (SCP)
- Centraal Informatiepunt Beroepen Gezondheidszorg (CiBG)
- College ter Beoordeling van Geneesmiddelen (inclusief agentschap en commissie)
- Dienst Uitvoering Subsidies aan Instellingen (DUS-I)
- Nederlandse Zorgautoriteit (NzA)

BIJLAGE 7 DPC CLOUD-BELEID

Dienst Publiek en Communicatie
Ministerie van Algemene Zaken

Cloudbeleid

Het gebruik van de Public Cloud uit oogpunt van informatiebeveiliging

Versie 1.0

Datum 28 maart 2019
Status Definitief

Colofon

Locatie # 4060469
Contactpersoon CISO Office: CISOoffice@minaz.nl

Auteurs Frederik van der Burg
Martin Dahlhaus

Inhoud

Inleiding en vaststelling

Publieke clouddiensten zijn al geruime tijd aanwezig in het digitale landschap. Leveranciers leveren steeds meer functionaliteit die ‘Cloud first’ of ‘Cloud only’ is. Als privé persoon maakt bijna iedere medewerker van AZ gebruik van een of meerdere diensten die worden geleverd uit en door de Cloud. De druk neemt zowel intern als extern toe om ook zakelijk gebruik te maken van clouddiensten. Medewerkers willen graag gebruik maken van de Cloud zodat contact en het uitwisselen van informatie met externen op een flexibele en gemakkelijke wijze mogelijk wordt. Ook worden via de Cloud eenvoudig toegankelijke en kwalitatief goede diensten geleverd, zoals kant en klare software of voor geconfigureerde hosting platforms. Deze diensten zijn vaak ook nog goedkoop en vragen geen of minimaal beheer van de eigen ICT organisatie.
De voordelen van Clouddiensten zijn duidelijk. Maar er zijn ook nadelen, die vooral met veiligheid te maken hebben.

Er is op dit moment geen eenduidig en sluitend Rijksbeleid hoe om te gaan met de Cloud. Wanneer mag je het wel gebruiken en wanneer niet? Dit beleid geeft antwoord op deze vraag.

1 Doel en scope

1.1 Doel

Doel van het beleid is duidelijk te maken onder welke voorwaarden gebruik kan worden gemaakt van public Cloud dienstverlening door en voor medewerkers van AZ. Daarmee wordt tevens aangegeven in welke gevallen Cloud dienstverlening geen optie is.

1.2 Scope

Het beleid is van toepassing op alle diensten die worden aangeboden door externe Cloud leveranciers, zowel commercieel als binnen het Rijk, en afgenomen worden door (medewerkers van) AZ.

2 Cloud definitie

Er bestaan veel misverstanden en meningsverschillen over wat 'Cloud' precies is. AZ maakt gebruik van de definitie zoals het National Institute of Standards and Technology (NIST)[1] deze hanteert in Special Publication 800-145[2]:

"Cloud computing is een model voor het leveren van gemakkelijke, on-demand toegang tot een gedeelde pool van computerresources (bijv. netwerken, servers, opslag, applicaties en diensten) die snel kunnen worden ingericht en vrijgegeven met minimale inspanning of interactie tussen de dienstverlener en aanvrager. Het Cloud model bestaat uit vijf essentiële kenmerken, drie servicemodellen en vier implementatiemodellen."

2.1 Essentiele kenmerken

2.1.1 On-demand self-service.
Een gebruiker van een clouddienst kan eenzijdig computercapaciteiten, zoals servertijd en netwerkopslag, automatisch toewijzen zonder dat er menselijke interactie met de dienstverlener nodig is.

2.1.2 Toegankelijk via het Internet
Hoewel niet altijd het geval zoals bij gesloten (rijks) overheid cloud omgevingen is het overgrote deel van de Cloud capaciteiten beschikbaar via het Internet en toegankelijk via standaardmechanismen die het gebruik door heterogene client platforms bevorderen (bijv. mobiele telefoons, tablets, laptops en werkstations). Dit geld niet altijd, denk bijvoorbeeld aan gesloten interne clouds.

2.1.3 Resource pooling
De computercapaciteit van de provider wordt samengevoegd om meerdere consumenten te bedienen met behulp van een multi-tenant model, waarbij verschillende fysieke en virtuele resources dynamisch worden ingezet op basis van de vraag. Er is sprake van een vorm van locatieonafhankelijkheid waarbij de klant over het algemeen geen controle of kennis heeft over de exacte locatie van de geleverde computercapaciteiten, maar waar mogelijk wel een locatie op een hoger niveau van abstractie (bijvoorbeeld land, staat of datacenter) kan specificeren.

2.1.4 Snelle expansie en beperking van computercapaciteit
Computercapaciteiten kunnen elastisch worden opgeschaald en vrijgegeven, in sommige gevallen automatisch. Voor de consument lijken de beschikbare mogelijkheden vaak onbeperkt en kunnen ze op elk gewenst moment in elke hoeveelheid worden toegewezen.

2.1.5 Service op basis van monitoring
Cloudsystemen regelen en optimaliseren automatisch het gebruik van bronnen door gebruik te maken van een meetfunctie op een abstractieniveau dat geschikt is voor het type service (bijvoorbeeld hoeveelheid opslag, aantallen verwerkingen, hoeveelheid bandbreedte en/of aantallen actieve gebruikersaccounts). Het gebruik van hulpbronnen kan worden gemonitord, gecontroleerd en gerapporteerd, wat transparantie biedt voor zowel de aanbieder als de consument van de gebruikte service.

2.2 Servicemodellen

Enkele voorbeelden van veel voorkomende Cloud service modellen zijn:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

2.2.1 Software as a Service (SaaS)
Een dienst geleverd aan een bedrijf of consument waarbij men gebruik maakt van applicaties aangeboden op het platform van de applicatieprovider. De applicaties zijn toegankelijk vanaf verschillende typen apparatuur door ofwel een interface zoals een

1 Het NIST is een Amerikaanse wetenschappelijke instelling die zich inzet voor standaardisatie
2 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

webbrowser (bijv. web-based e-mail) of een programma-interface (een app). De afnemer beheert de onderliggende Cloud en applicatie infrastructuur niet, met de uitzondering van gebruiker specifieke configuratie-instellingen.

2.2.2 Platform as a Service (PaaS)
Een dienst geleverd aan een bedrijf of consument waarbij men in staat is om zelf applicaties en diensten te implementeren op een Cloud infrastructuur. Deze Cloud infrastructuur bestaat uit een fysieke laag en een abstractie laag. De fysieke laag bestaat uit de hardware bronnen die nodig zijn om de geleverde Cloud services te ondersteunen, en omvat doorgaans server-, opslag- en netwerkcomponenten. De abstractie laag bestaat uit de software die wordt ingezet over de fysieke laag, die de essentiële Cloud kenmerken vertoont zoals virtualisatie. Daar valt dus ook het besturingssysteem en eventuele databasesoftware onder.

De afnemer beheert de onderliggende Cloud infrastructuur niet maar heeft controle over de geïmplementeerde applicaties en mogelijk configuratie-instellingen voor de applicatie-hosting omgeving.

2.2.3 Infrastructure as a Service (IaaS)
Een dienst geleverd aan een bedrijf of consument die voorziet in verwerking, opslag, netwerken en andere fundamentele computerbronnen waar de afnemer in staat is om willekeurige software te implementeren en uit te voeren, waaronder besturingssystemen en applicaties. De afnemer heeft directe controle over besturingssystemen, opslag en geïmplementeerde applicaties en mogelijk beperkte controle over geselecteerde netwerkcomponenten (bijvoorbeeld host-firewalls).

2.3 Implementatie modellen

2.3.1 Private Cloud
Een Cloud infrastructuur die bestemd is voor exclusief gebruik door een enkele organisatie met eventueel meerdere interne afnemers. De Cloud omgeving is veelal eigendom van en wordt beheerd door de eigen organisatie. Het is mogelijk dat een derde partij het eigendom heeft of beheer uitvoert uit naam van de eigen organisatie. De eigen organisatie heeft echter te allen tijde directe controle over alle Cloud resources.
Voorbeeld: Een AZ Cloud.

2.3.2 Community Cloud
Een Cloud infrastructuur die is bestemd voor exclusief gebruik door een specifieke community van organisaties die gedeelde zorgen hebben (bijvoorbeeld over missies, beveiligingsvereisten, beleid en nalevingsaspecten). Het kan eigendom zijn van en beheerd worden door een of meer van de organisaties in de gemeenschap, een derde partij of een combinatie daarvan.

Voorbeeld: De RijksCloud.

2.3.3 Public Cloud
Een Cloud infrastructuur die is bestemd voor publiek gebruik. Het kan eigendom zijn van en beheerd worden door een bedrijf, academische of overheidsorganisatie, of een combinatie daarvan.

Voorbeeld: De Amazon Cloud (EMC), Google Cloud, Microsoft Azure.

2.3.4 Hybrid Cloud
Een Cloud infrastructuur die een samenstelling is van twee of meer afzonderlijke Cloud infrastructuren (private, community of public) die unieke entiteiten blijven, maar zijn verbonden door gestandaardiseerde of eigen technologie die gegevens- en datatransport, delen van applicaties en verwerkingsportabiliteit mogelijk maakt.

Voorbeeld: Microsoft Office 365 Hybrid Cloud implementaties.

3 Beleid

3.1 Algemeen

Het is onder voorwaarden toegestaan om gebruik te maken van cloudoplossingen voor de creatie, verwerking en opslag van AZ informatie en data. Alle initiatieven voor het gebruik van de Cloud moeten worden voorgelegd aan het CISO Office van AZ die een oordeel velt over de wenselijkheid vanuit een informatiebeveiligingsstandpunt. Medewerkers van AZ moeten zich bij het gebruikmaken van Clouddiensten conformeren aan het AZ beleid.

3.2 Kaders

3.2.1 Wettelijke kaders

Alle wettelijke kaders zoals de VIR, VIRBI en de AVG die voor AZ gelden zijn ook van toepassing op het gebruik van de Cloud.

3.2.2 Normenkaders

Elke dienstverlener van AZ dient te voldoen aan het BIR2017 normenkader. Dit normenkader is het minimum beveiligingsniveau van het Rijk. Als uit praktische overwegingen het niet mogelijk is de BIR2017 aan een leverancier op te leggen, dan kan een voor de dienstverlenging relevante ISO27001 certificering van de dienstverlener worden geaccepteerd. Of dit voldoende is, is ter beoordeling van het CISO Office. Deze certificering dient opgevraagd te kunnen worden bij de Cloud dienstverlener of is gepubliceerd op haar website.

3.3 Risicobeleid

Voordat een Clouddienst in gebruik wordt genomen, wordt door de informatie eigenaar een expliciete (IB) risicoafweging gemaakt i.s.m. het CISO Office. Deze wordt formeel door de informatie eigenaar geaccordeerd.

Daarnaast is net als bij ander informatiesystemen ten minste sprake van:

1. Een Quickscan BIR.
2. Een Fit/gap analyse op de BIR.
3. Een PIA indien dit noodzakelijk is.

3.4 Data en informatiehuishouding

Voor elke Clouddienst die afgenomen wordt moet beschreven staan hoe informatie en data die eigendom is van AZ in een goede, geordende en toegankelijke staat uit de Cloud kan worden gehaald. Dit is nodig als de dienstverlening wordt stopgezet of als dit noodzakelijk is t.b.v. archivering volgens de Archiefwet3. Dit wordt vastgelegd in een zogenaamde ‘exit strategie’. De CIO en CISO van AZ geven een kwaliteitsoordeel op de exit strategie waarna deze bij een positief oordeel formeel door de informatie eigenaar wordt vastgesteld.

Bij het opstellen van een exit strategie gelden tenminste de volgende aandachtspunten:

- **Houd zeggenschap over de eigen gegevens**
  Het is wenselijk om contractueel vast te leggen dat data van AZ bij beëindiging van de dienstverlening direct tot beschikking komt van AZ en ook hoe dit gebeurt. Immers, om de gegevens over te kunnen zetten naar een nieuwe Cloud omgeving of een ander systeem dienen de gegevens aangeboden te worden in een open formaat dat leesbaar en bruikbaar is voor AZ.
- **Breng de risico’s van het opheffen van de dienstverlening in kaart.**
  Definieer de herkenbare risico’s die voor jouw unit of AZ van toepassing zijn. Maakt hiervoor gebruik van een heat map en verdeel de risico’s dan naar ‘kans’ en ‘impact’. Per risico moet worden afgewogen of het risico geaccepteerd kan worden of dat er een mitigerende maatregel voor moet komen.
- Zorg voor een volledige overdracht

3 Archiefwaardige stukken dienen opgeslagen te worden in het DMS van AZ ongeacht de archiefvoorzieningen van de Cloud provider.

- Er mogen aantoonbaar geen gegevens achterblijven in de Cloud nadat de dienstverlening is stopgezet. Hiervan dient adequaat bewijs geleverd te worden aan AZ als opdracht gevende organisatie. Het is ook hier wenselijk dat dit bij de start van de dienstverlening contractueel wordt vastgelegd.
- **Ontwikkel fall-back scenario's**
  Na het beëindigen van het contract met een Cloud leverancier kan het zijn dat de dienstverlening niet meer noodzakelijk is. Echter in vele gevallen moet de ICT organisatie van AZ de afgenomen ICT-diensten zelf leveren of er moet een andere cloud leverancier worden gevonden. Door voorbereid te zijn op een eventuele 'exit' kan AZ de consequenties makkelijker opvangen.

3.5 AVG

De af te nemen clouddienst dient wanneer van toepassing te voldoen aan de eisen van de AVG. Wanneer de afgenomen dienst persoonsgegevens verwerkt is er tenminste sprake van:

- Een uitgevoerde PIA
- Een verwerkersovereenkomst
- Een melding in het meldingenregister

3.6 Monitoring van de dienstverlening

De dienstverlener rapporteert waar mogelijk regelmatig over relevante aspecten van zijn dienstverlening, zoals verbruikscijfers, beveiligingsincidenten of meer dienst specifieke informatie. Hierover kunnen afspraken worden gemaakt met de dienstverlener in een SLA.

3.7 Audits

Aan alle Clouddienstverleners wordt het 'right to audit' gevraagd. Wanneer dit niet mogelijk is dient de clouddienstverlener een duidelijke webpagina of proces te hebben voor het opvragen van audits uitgevoerd door erkende externe auditors.

3.8 Selectie op basis van de classificatie van de informatie of data

Voor de selectie van Clouddienstverlening wordt gebruik gemaakt van de classificatie van de informatie of data die wordt gecreëerd, verwerkt en opslagen door en bij de Clouddienstverlener. Bij het opslaan van informatie in de cloud worden de aanbeveling in de nota 'Dataopslag Handreiking dataopslag' (DGOO) zoals vastgesteld in het CTO-Beraad dd. 19 mei 2016, geborgd.

Classificatie informatie/data	Selectie
Openbare data.	Er mag gebruik worden gemaakt van alle clouddienstverleners zolang deze voldoen aan de gestelde normenkaders en ze niet in strijd zijn met wet en regelgeving.
Niet gerubriceerde overheidsdata en/of **informatie waarin persoonsgegevens zijn verwerkt.** Gegevens mogen alleen toegankelijk zijn voor een bepaalde groep. Openbaarmaking kan leiden tot beperkte (imago) schade van AZ.	Deze mag alleen worden opgeslagen bij: **A.** Cloudleverancier opereert strikt binnen de Europese Economische Ruimte (EER), *óf* **B.** Cloudleverancier voldoet aan de ISO27017 en ISO27018 normen.
Departementaal Vertrouwelijke Informatie en **informatie waarin meerdere typen persoonsgegevens en/of bijzondere persoonsgegevens zijn verwerkt.**	Deze informatie mag alleen worden opgeslagen bij Cloudleverancier binnen de EER waarbij gebruik wordt gemaakt van encryptie waarvan het sleutelbeheer binnen de invloedsfeer van AZ plaats vindt. (Bij AZ of bij onze contractant, mits deze partij niet de cloudleverancier is én niet onder de CLOUD-act valt.) Clouddiensten voldoen aan de ISO27017 en ISO27018 normen.
Staatsgeheime informatie of verzamelingen van meerdere typen bijzondere persoonsgegevens.	Er mag onder **geen enkele voorwaarde** gebruik worden gemaakt van een publieke Cloud dienstverlener.

Daarbij gelden de volgende definities:

Type informatie/data	Definitie
Openbare data.	Informatie die doelbewust openbaar wordt gemaakt.
Niet gerubriceerde overheidsdata.	Interne informatie die je gebruikt bij de uitvoering van je taak en die niet-gerubriceerd is. Openbaarmaking kan leiden tot beperkte (imago) schade van AZ.
Departementaal Vertrouwelijke Informatie.	Informatie waarbij kennisname door niet-geautoriseerde schade kan toebrengen aan de belangen van AZ en/of andere ministeries (=definitie VIR-BI). Deze classificatie wordt formeel bepaald aan de hand van het rubriceringsbesluit.
Staatsgeheime informatie.	Informatie waarbij kennisname door niet-geautoriseerde schade kan toebrengen aan de belangen van de staat en/of haar bondgenoten. Deze classificatie wordt formeel bepaald aan de hand van het rubriceringsbesluit.

4 Verantwoordelijkheden

Handhaving van het beleid is een verantwoordelijkheid van meerdere actoren.

Actor	Verantwoordelijkheid
CISO Office	• Opstellen en zo nodig bijstellen van dit beleid. • Het beleid bekendmaken binnen de organisatie. • Adviseren in specifieke situaties. • Corrigerend dan wel escalerend optreden in geval van overtreding van het beleid. • Adviseren in geval van incidenten. • Inzicht bieden in naleving van het beleid.
Diensthoofden / afdelingshoofden	• Toepassen en handhaven van het beleid. • Het beleid bekendmaken bij eigen medewerkers en externen. • Het goede voorbeeld geven.
Team Inkoop	• Signalerende functie bij inkoop van dienstverlening. Indien het vermoeden bestaat dat dit beleid van toepassing is worden zowel de aanvrager als het CISO Office op de hoogte gebracht.
ICT Servicedesk	• Signalerende functie, zowel richting de gebruiker, diensthoofden als richting het CISO Office. • Verwijzen iedere aanvraag van gebruikers waarbij de wens bestaat gebruik te maken van Cloud dienstverlening door naar het CISO Office.
AZ medewerkers	• Dienen op de hoogte te zijn van het beleid. • Gebruiken alleen Cloud dienstverlening in overeenstemming met dit beleid en na expliciete goedkeuring van hun leidinggevende.
Systeem/informatie eigenaar	• Stelt criteria op voor de behandeling van de informatie, en is verantwoordelijk voor het uitvoeren van een PIA.

5 Kritieke Prestatie Indicatoren (KPI's)

Om inzicht te bieden in de naleving van het beleid zijn de volgende KPI's opgesteld.

KPI	Operationalisering	Door
Niet geautoriseerd en niet aangemeld gebruik van de Cloud binnen de AZ netwerken.	• Rapportages uit de diverse firewall omgevingen van AZ.	CISO Office
Geautoriseerd en aangemeld gebruik van de Cloud.	• Registratie van in gebruik zijnde Cloud dienstverlening in Topdesk. • Registratie van aanvragen voor het gebruik van Cloud dienstverlening in Topdesk. • Meldingen vanuit Teaminkoop van aanvragen voor aanschaf van Cloud dienstverlening. • Rapportages uit de diverse firewall omgevingen van Algemene Zaken.	Servicedesk, Teaminkoop, Functioneel Beheer, Backoffice
Het aantal gebruikers van clouddienstverlening.	• Monitoring aangeboden vanuit de clouddienstverlener. • Rapportages uit de diverse firewall omgevingen van Algemene Zaken.	Clouddienstverlener, Backoffice
Het verbruik van clouddienstverlening.	• Monitoring aangeboden vanuit de clouddienstverlener. • Rapportages uit de diverse firewall omgevingen van Algemene Zaken.	Clouddienstverlener, Backoffice
Overtredingen van het beleid op basis van de classificatie van de informatie of data.	• Interne audits • Monitoring aangeboden vanuit de clouddienstverlener. • Rapportages uit de diverse firewall omgevingen van Algemene Zaken.	CISO Office
Het aantal gebruikte clouddiensten zonder een exit strategie.	• Interne audits. Deze data is vastgelegd in de BIR Systeemlijst.	CISO Office
Het aantal gebruikte clouddiensten zonder een expliciete risicoafweging.	• Interne audits. Dit wordt vastgelegd in kwartaalrapportages.	CISO Office

BIJLAGE 8 FIT/GAP ANALYSE

Het vastgestelde **Basis Beveiligings Niveau:**	**BBN2**, voor het aspect Beschikbaarheid geldt dat de BIO normen op BBN1 niveau mogen worden toegepast, tenzij de leverancier gebruikt maakt van clouddiensten (waar wij, in dit geval, van uit gaan).			
Is opdrachtnemer Verwerkingsverantwoordelijke of Verwerker:	Verwerkingsverantwoordelijke: Ja/Nee	Ja: type 'X' →	X	**Lev. ❶** na aanpassing in cel H20 'X' selecteren
	Verwerker: Ja/Nee	Ja: type 'X' →	X	
Is er sprake van cloudgebruik en/of -dienstverlening	Worden er vertrouwelijke gegevens opgeslagen: Ja/Nee	Ja: type 'X' →	X	
	Worden er persoonsgegevens opgeslagen: Ja/Nee	Ja: type 'X' →	X	
BIO 1.04 fit/gap analyse	<naam systeem/dienstverlening>			**Lev. ❷**
Opgesteld door:	<naam IB verantwoordelijke & bedrijf>			
Datum laatst vastgesteld:	<datum invulling>			

Lees het onderstaande vóór het invullen van de rode velden in deze spreadsheet:

Een leverancier dient aan de IB-eisen te voldoen voor de systemen en processen die wij van hen afnemen. Zijn organisatie dient aan de IB-eisen te voldoen waar dat relevant is voor de af te nemen systemen en processen, en het beheer daarvan.

Kolom F:
Ja = Voldoen. Bondig beschreven en onderbouwd, zowel implementatie (vaststelling) als documentatie (vastlegging) moet aanwezig zijn (mét een verwijzing naar de specifieke passage in een document) in **kolom E.**
Nee = Er wordt niet aan voldaan. **Kolommen F en G** dienen te worden ingevuld.

Alle normen zijn van toepassing!
Voorbeeld: Er zijn normen die over 'verwijderbare media' gaan. Als u die niet gebruikt is de norm tóch van toepassing. Neem bij deze norm een verwijzing op naar beleid waarin vastgesteld wordt dat er geen verwijderbare media worden gebruikt.
Erkende uitzonderingen: Alleen de normen 14.2.5 t/m 14.2.9 vormen hierop een uitzondering. Deze zijn van een nadere duiding voorzien in rood.

Documentatie:
We hebben de meeste normen voorzien van concept-documentatie (mouse-over/rood hoekje). Deze tekst is slechts een suggestie, maar niet uitputtend en wellicht niet op uw situatie van toepassing.

Certificering ISO 27001
Wanneer u (aantoonbaar) in bezit bent van een ISO 27001 certificaat, lever ons dan het certificaat (inclusief Auditscope en Verklaring van Toepasselijkheid). U hoeft dan de blauwe normen niet in te vullen.

Certificering ISO 27017
Alleen indien de clouddienst AANTOONBAAR volledige ISO 27017 certificering heeft, voldoet u automatisch aan deze normen. Plaats dan een **V** in de **cel F4**, en lever ons de certificaten (inclusief Auditscope en Verklaring van Toepasselijkheid).

Certificering ISO 27018
Alleen indien de clouddienst AANTOONBAAR volledige ISO 27017 én ISO 27018 certificering heeft, voldoet u automatisch aan deze normen. Plaats dan een **V** in de cel **F5**, en lever ons de certificaten (inclusief Auditscope en Verklaring van Toepasselijkheid).

Certificering ISO/IEC 27701:2019
Alleen indien de leverancier AANTOONBAAR volledige ISO/IEC 27701:2019 certificering heeft (dus inclusief Annex A en Annex B, voldoet u automatisch aan deze normen. Plaats dan een **V** in de cellen **F2** en **F3**, en lever ons de certificaten (inclusief Auditscope en Verklaring van Toepasselijkheid).

Lev. ❸

Inhoudelijke verklaring Leverancier:

Aantal van toepassing zijnde normen: 197

Hoofdbeveiligings-categorie		Control	Voldoet ja/nee?	Hoe is de norm ingericht?	Welke maatregel is nodig om wel te voldoen?	Wanneer opgelost?	BBN2 (bij Cloud geen Varia)
5 Informatiebeveiligingsbeleid 5.1 Aansturing door de directie van de informatiebeveiliging	5.1.1	Beleidsregels voor informatiebeveiliging: Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.					x
5. Informatiebeveiligingsbeleid 5.1 Aansturing door de directie van de informatiebeveiliging	5.1.2	Beoordeling van het informatiebeveiligingsbeleid: Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.					x

6 Organiseren van informatiebeveiliging 6.1 Interne organisatie	6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging: Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.					x
6 Organiseren van informatiebeveiliging 6.1 Interne organisatie	6.1.2	Scheiding van taken: Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.					x
6 Organiseren van informatiebeveiliging 6.1 Interne organisatie	6.1.3	Contact met overheidsinstanties: Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.					x
6 Organiseren van informatiebeveiliging 6.1 Interne organisatie	6.1.5	Informatiebeveiliging in projectbeheer: Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.					x
6 Organiseren van informatiebeveiliging 6.2 Mobiele apparatuur en telewerken	6.2.1	Beleid voor mobiele apparatuur: Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.					x
6 Organiseren van informatiebeveiliging 6.2 Mobiele apparatuur en telewerken	6.2.2	Telewerken: Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.					x
7 Veilig personeel 7.1 Voorafgaand aan het dienstverband	7.1.1	Screening: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.					x
7 Veilig personeel 7.1 Voorafgaand aan het dienstverband	7.1.2	Arbeidsvoorwaarden: De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.					x
7 Veilig personeel 7.2 Tijdens het dienstverband	7.2.1	Directieverantwoordelijkheden: De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.					x
7 Veilig personeel 7.2 Tijdens het dienstverband	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.					x
7 Veilig personeel 7.2 Tijdens het dienstverband	7.2.3	Disciplinaire procedure: Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.					x

7 Veilig personeel 7.3 Beëindiging en wijziging van dienstverband	7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband: Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.					x
8 Beheer van bedrijfsmiddelen 8.1 Verantwoordelijkheid voor bedrijfsmiddelen	8.1.1	Inventariseren van bedrijfsmiddelen: Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.					x
8 Beheer van bedrijfsmiddelen 8.1 Verantwoordelijkheid voor bedrijfsmiddelen	8.1.2	Eigendom van bedrijfsmiddelen: Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.					x
8 Beheer van bedrijfsmiddelen 8.1 Verantwoordelijkheid voor bedrijfsmiddelen	8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen: Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.					x
8 Beheer van bedrijfsmiddelen 8.1 Verantwoordelijkheid voor bedrijfsmiddelen	8.1.4	Teruggeven van bedrijfsmiddelen: Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven					x
8 Beheer van bedrijfsmiddelen 8.2 Informatieclassificatie	8.2.1	Classificatie van informatie: Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.					x
8 Beheer van bedrijfsmiddelen 8.2 Informatieclassificatie	8.2.2	Informatie labelen: Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie					x
8 Beheer van bedrijfsmiddelen 8.2 Informatieclassificatie	8.2.3	Behandelen van bedrijfsmiddelen: Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.					x
8 Beheer van bedrijfsmiddelen 8.3 Behandelen van media	8.3.1	Beheer van verwijderbare media: Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.					x
8 Beheer van bedrijfsmiddelen 8.3 Behandelen van media	8.3.2	Verwijderen van media: Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures					x

8 Beheer van bedrijfsmiddelen 8.3 Behandelen van media	8.3.3	Media fysiek overdragen: Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.					x
9 Toegangsbeveiliging 9.1 Bedrijfseisen voor toegangsbeveiliging	9.1.1	Beleid voor toegangsbeveiliging: Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.					x
9 Toegangsbeveiliging 9.1 Bedrijfseisen voor toegangsbeveiliging	9.1.2	Toegang tot netwerken en netwerkdiensten: Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.					x
9 Toegangsbeveiliging 9.2 Beheer van toegangsrechten van gebruikers	9.2.1	Registratie en afmelden van gebruikers: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.					x
9 Toegangsbeveiliging 9.2 Beheer van toegangsrechten van gebruikers	9.2.2	Gebruikers toegang verlenen: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.					x
9 Toegangsbeveiliging 9.2 Beheer van toegangsrechten van gebruikers	9.2.3	Beheren van speciale toegangsrechten: Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.					x
9 Toegangsbeveiliging 9.2 Beheer van toegangsrechten van gebruikers	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers: Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.					x
9 Toegangsbeveiliging 9.2 Beheer van toegangsrechten van gebruikers	9.2.5	Beoordeling van toegangsrechten van gebruikers: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.					x
9 Toegangsbeveiliging 9.2 Beheer van toegangsrechten van gebruikers	9.2.6	Toegangsrechten intrekken of aanpassen: De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.					x
9 Toegangsbeveiliging 9.3 Verantwoordelijkheden van gebruikers	9.3.1	Geheime authenticatie-informatie gebruiken: Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.					x
9 Toegangsbeveiliging 9.4 Toegangsbeveiliging van systeem en toepassing	9.4.1	Beperking toegang tot informatie: Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.					x
9 Toegangsbeveiliging 9.4 Toegangsbeveiliging van systeem en toepassing	9.4.2	Beveiligde inlogprocedures: Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.					x
9 Toegangsbeveiliging 9.4 Toegangsbeveiliging van systeem en toepassing	9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.					x

9 Toegangsbeveiliging 9.4 Toegangsbeveiliging van systeem en toepassing	9.4.4	Speciale systeemhulpmiddelen gebruiken: Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.					x
9 Toegangsbeveiliging 9.4 Toegangsbeveiliging van systeem en toepassing	9.4.5	Toegangsbeveiliging op programmabroncode: Toegang tot de programmabroncode behoort te worden beperkt.					x
10 Cryptografie 10.1 Cryptografische beheersmaatregelen	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen: Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.					x
10 Cryptografie 10.1 Cryptografische beheersmaatregelen	10.1.2	Sleutelbeheer: Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.1 Beveiligde gebieden	11.1.1	Fysieke beveiligingszone: Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.1 Beveiligde gebieden	11.1.2	Fysieke toegangsbeveiliging: Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.1 Beveiligde gebieden	11.1.3	Kantoren, ruimten en faciliteiten beveiligen: Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.1 Beveiligde gebieden	11.1.4	Beschermen tegen bedreigingen van buitenaf: Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.1 Beveiligde gebieden	11.1.5	Werken in beveiligde gebieden: Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.1 Beveiligde gebieden	11.1.6	Laad- en loslocatie: Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.2 Apparatuur	11.2.1	Plaatsing en bescherming van apparatuur: Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.2 Apparatuur	11.2.2	Nutsvoorzieningen: Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.					x

11 Fysieke beveiliging en beveiliging van de omgeving 11.2 Apparatuur	11.2.3	Beveiliging van bekabeling: Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.2 Apparatuur	11.2.4	Onderhoud van apparatuur: Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.2 Apparatuur	11.2.5	Verwijdering van bedrijfsmiddelen: Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.2 Apparatuur	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein: Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.2 Apparatuur	11.2.7	Veilig verwijderen of hergebruiken van apparatuur: Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.2 Apparatuur	11.2.8	Onbeheerde gebruikersapparatuur: Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.					x
11 Fysieke beveiliging en beveiliging van de omgeving 11.2 Apparatuur	11.2.9	'Clear desk'- en 'clear screen'-beleid: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.					x
12 Beveiliging bedrijfsvoering 12.1 Bedieningsprocedures en verantwoordelijkheden	12.1.1	Gedocumenteerde bedieningsprocedures: Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.					x
12 Beveiliging bedrijfsvoering 12.1 Bedieningsprocedures en verantwoordelijkheden	12.1.2	Wijzigingsbeheer: Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.					x
12 Beveiliging bedrijfsvoering 12.1 Bedieningsprocedures en verantwoordelijkheden	12.1.3	Capaciteitsbeheer: Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.					x
12 Beveiliging bedrijfsvoering 12.1 Bedieningsprocedures en verantwoordelijkheden	12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen: Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.					x

12 Beveiliging bedrijfsvoering 12.2 Bescherming tegen malware	12.2.1	Beheersmaatregelen tegen malware: Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.					x
12 Beveiliging bedrijfsvoering 12.3 Back-up	12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.					x
12 Beveiliging bedrijfsvoering 12.4 Verslaglegging en monitoren	12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.					x
12 Beveiliging bedrijfsvoering 12.4 Verslaglegging en monitoren	12.4.2	Beschermen van informatie in logbestanden: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.					x
12 Beveiliging bedrijfsvoering 12.4 Verslaglegging en monitoren	12.4.3	Logbestanden van beheerders en operators: Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.					x
12 Beveiliging bedrijfsvoering 12.4 Verslaglegging en monitoren	12.4.4	Kloksynchronisatie: De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.					x
12 Beveiliging bedrijfsvoering 12.5 Beheersing van operationele software	12.5.1	Software installeren op operationele systemen: Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.					x
12 Beveiliging bedrijfsvoering 12.6 Beheer van technische kwetsbaarheden	12.6.1	Beheer van technische kwetsbaarheden: Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.					x
12 Beveiliging bedrijfsvoering 12.6 Beheer van technische kwetsbaarheden	12.6.2	Beperkingen voor het installeren van software: Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.					x
12 Beveiliging bedrijfsvoering 12.7 Overwegingen betreffende audits van informatiesystemen	12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen: Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.					x
13 Communicatiebeveiliging 13.1 Beheer van netwerkbeveiliging	13.1.1	Beheersmaatregelen voor netwerken: Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.					x

13 Communicatiebeveiliging 13.1 Beheer van netwerkbeveiliging	13.1.2	Beveiliging van netwerkdiensten: Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.					x
13 Communicatiebeveiliging 13.1 Beheer van netwerkbeveiliging	13.1.3	Scheiding in netwerken: Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.					x
13 Communicatiebeveiliging 13.2 Informatietransport	13.2.1	Beleid en procedures voor informatietransport: Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.					x
13 Communicatiebeveiliging 13.2 Informatietransport	13.2.2	Overeenkomsten over informatietransport: Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.					x
13 Communicatiebeveiliging 13.2 Informatietransport	13.2.3	Elektronische berichten: Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.					x
13 Communicatiebeveiliging 13.2 Informatietransport	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst: Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.1 Beveiligingseisen voor informatiesystemen	14.1.1	Analyse en specificatie van informatiebeveiligingseisen: De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.1 Beveiligingseisen voor informatiesystemen	14.1.2	Toepassingen op openbare netwerken beveiligen: Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.1 Beveiligingseisen voor informatiesystemen	14.1.3	Transacties van toepassingen beschermen: Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.2 Beveiliging in ontwikkelings- en ondersteunende processen	14.2.1	Beleid voor beveiligd ontwikkelen: Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.					x

14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.2 Beveiliging in ontwikkelings- en ondersteunende processen	14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen: Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.2 Beveiliging in ontwikkelings- en ondersteunende processen	14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform: Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.2 Beveiliging in ontwikkelings- en ondersteunende processen	14.2.5	Principes voor engineering van beveiligde systemen: Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen. *In geval van Commercial Of The Shelf (COTS) producten kan de norm op n.v.t. (let op: wél van toepassing in geval van maatwerk)*					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.2 Beveiliging in ontwikkelings- en ondersteunende processen	14.2.6	Beveiligde ontwikkelomgeving: Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling. *In geval van Commercial Of The Shelf (COTS) producten kan de norm op n.v.t. (let op: wél van*					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.2 Beveiliging in ontwikkelings- en ondersteunende processen	14.2.7	Uitbestede softwareontwikkeling: Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie. *In geval van Commercial Of The Shelf (COTS) producten kan de norm op n.v.t. (let op: wél van*					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.2 Beveiliging in ontwikkelings- en ondersteunende processen	14.2.8	Testen van systeembeveiliging: Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest. *In geval van Commercial Of The Shelf (COTS) producten kan de norm op n.v.t. (let op: wél van*					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.2 Beveiliging in ontwikkelings- en ondersteunende processen	14.2.9	Systeemacceptatietests: Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld. *In geval van Commercial Of The Shelf (COTS) producten kan de norm op n.v.t. (let op: wél van*					x
14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 14.3 Testgegevens	14.3.1	Bescherming van testgegevens: Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.					x

15 Leveranciersrelaties 15.1 Informatiebeveiliging in leveranciersrelaties	15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties: Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd					x
15 Leveranciersrelaties 15.1 Informatiebeveiliging in leveranciersrelaties	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of hiervoor					x
15 Leveranciersrelaties 15.1 Informatiebeveiliging in leveranciersrelaties	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.					x
15 Leveranciersrelaties 15.2 Beheer van dienstverlening van leveranciers	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers: Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.					x
15 Leveranciersrelaties 15.2 Beheer van dienstverlening van leveranciers	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers: Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.					x
16 Beheer van informatiebeveiligingsincidenten 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	16.1.1	Verantwoordelijkheden en procedures: Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen					x
16 Beheer van informatiebeveiligingsincidenten 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.					x
16 Beheer van informatiebeveiligingsincidenten 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging: Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.					x

16 Beheer van informatiebeveiligingsincidenten 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen: Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.					x
16 Beheer van informatiebeveiligingsincidenten 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	16.1.5	Respons op informatiebeveiligingsincidenten: Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.					x
16 Beheer van informatiebeveiligingsincidenten 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	16.1.6	Lering uit informatiebeveiligingsincidenten: Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.					x
16 Beheer van informatiebeveiligingsincidenten 16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	16.1.7	Verzamelen van bewijsmateriaal: De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.					x
17 Informatiebeveiligings-aspecten van bedrijfscontinuïteitsbeheer 17.1 Informatiebeveiligings-continuïteit	17.1.1	Informatiebeveiligingscontinuïteit plannen: De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.					x
17 Informatiebeveiligings-aspecten van bedrijfscontinuïteitsbeheer 17.1 Informatiebeveiligings-continuïteit	17.1.2	Informatiebeveiligingscontinuïteit implementeren: De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.					x
17 Informatiebeveiligings-aspecten van bedrijfscontinuïteitsbeheer 17.1 Informatiebeveiligings-continuïteit	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren: De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.					x
17 Informatiebeveiligings-aspecten van bedrijfscontinuïteitsbeheer 17.2 Redundante componenten	17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten: Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.					x
18 Naleving 18.1 Naleving van wettelijke en contractuele eisen	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen: Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.					x

18 Naleving 18.1 Naleving van wettelijke en contractuele eisen	18.1.2	Intellectuele-eigendomsrechten: Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectueleeigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.					x
18 Naleving 18.1 Naleving van wettelijke en contractuele eisen	18.1.3	Beschermen van registraties: Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.					x
18 Naleving 18.1 Naleving van wettelijke en contractuele eisen	18.1.4	Privacy en bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.					x
18 Naleving 18.1 Naleving van wettelijke en contractuele eisen	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen: Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.					x
18 Naleving 18.2 Informatiebeveiligings-beoordelingen	18.2.1	Onafhankelijke beoordeling van informatiebeveiliging: De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.					x
18 Naleving 18.2 Informatiebeveiligings-beoordelingen	18.2.2	Naleving van beveiligingsbeleid en -normen: De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.					x
18 Naleving 18.2 Informatiebeveiligings-beoordelingen	18.2.3	Beoordeling van technische naleving: Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de					x
ISO 27017 Cloud IB							
6 Organiseren van informatiebeveiliging 6.3 Verhouding cloudservice klant en	CLD.6.3.1	Verantwoordelijkheden voor gedeelde informatiebeveiliging rollen bij het gebruik van de cloudservice moeten worden toegewezen aan					X
8 Beheer van bedrijfsmiddelen 8.1 Verantwoordelijkheid voor bedrijfsmiddelen	CLD.8.1.5	Bedrijfsmiddelen van de klant van de cloudservice die zich bij de cloudservice provider bevinden, moeten worden verwijderd en tijdig te worden geretourneerd indien nodig, bij het beëindigen van de clouddienst overeenkomst.					X
9 Toegangsbeveiliging 9.5 Toegangsbeveiliging in gedeelde virtuele omgevingen	CLD.9.5.1	De virtuele omgeving van een cloudservice klant, moet worden beveiligd tegen andere cloudservice klanten en onbevoegde personen.					X
9 Toegangsbeveiliging 9.5 Toegangsbeveiliging in gedeelde virtuele omgevingen	CLD.9.5.2	Virtuele machines in een cloud computing-omgeving moeten worden gehard om aan zakelijke eisen te voldoen.					X

12 Beveiliging bedrijfsvoering 12.1 Bedieningsprocedures en verantwoordelijkheden	CLD.12.1.5	Procedures voor administratieve handelingen in een cloud computing-omgeving moeten worden gedefinieerd, gedocumenteerd en gemonitord.					X
12 Beveiliging bedrijfsvoering 12.4 Verslaglegging en monitoren	CLD.12.4.5	De cloudservice klant moet in staat zijn om specifieke aspecten van de werking van de cloudservices te controleren.					X
13 Communicatiebeveiliging 13.1 Beheer van netwerkbeveiliging	CLD.13.1.4	Bij configuratie van virtuele netwerken moet configuratie consistentie tussen virtuele en fysieke netwerken worden geverifieerd op basis van het netwerkbeveiliging beleid van de cloud serviceprovider.					X
ISO 27018 Cloud Privacy							
Annex A Public Cloud A.2 Instemming en keuze	A.2.1	Verplichting samenwerking mbt Persoons Gegevens rechten. De public cloud Persoons Gegevens verwerker moet de cloudservice klant de middelen bieden om deze in staat te stellen aan zijn verplichting te voldoen om de uitoefening van de rechten van natuurlijke persoon op toegang tot, correctie en/of wissen van Persoons Gegevens mogelijk te maken.					X
A Public Cloud Persoons Gegevens bescherming A.3 Doelbinding en -specificatie	A.3.1	Doelbinding cloud persoonsgegevens. Persoonsgegevens die moeten worden verwerkt op basis van een contract, mogen niet worden verwerkt voor andere doelen dan conform instructies van de cloudservice klant.					X
A Public Cloud Persoons Gegevens bescherming A.3 Doelbinding en -specificatie	A.3.2	Commercieel gebruik cloud persoonsgegevens. Persoonsgegevens die onder een contract verwerkt worden mogen niet worden gebruikt door de public cloud Persoons Gegevens verwerker voor marketingdoeleinden en advertenties, zonder uitdrukkelijke toestemming. Een dergelijke toestemming mag geen voorwaarde zijn voor de service.					X
A Public Cloud Persoons Gegevens bescherming A.5 Gegevensminimalisatie	A.5.1	Veilig wissen van tijdelijke bestanden. Tijdelijke bestanden en documenten moeten worden gewist of vernietigd binnen een gespecificeerde, gedocumenteerde periode.					X
A Public Cloud Persoons Gegevens bescherming A.6 Beperkingen voor gebruik, retentie en openbaarmaking	A.6.1	Melding van onthulling persoonsgegevens. Het contract tussen de public cloud Persoons Gegevens verwerker en de cloudservice klant vereist dat de public cloud Persoons Gegevens verwerker de cloudservice klant op de hoogte brengt van elk juridisch bindend verzoek tot openbaarmaking van Persoons Gegevens (conform de voorwaarden in het contract) door een wetshandhaving instantie, tenzij een dergelijke onthulling anderszins is verboden.					X
A Public Cloud Persoons Gegevens bescherming A.6 Beperkingen voor gebruik, retentie en openbaarmaking	A.6.2	Registratie van onthulling persoonsgegevens. Onthulling van Persoons Gegevens aan derden moet worden vastgelegd, inclusief welke Persoons Gegevens zijn vrijgegeven, aan wie en op welk tijdstip.					X

A Public Cloud Persoons Gegevens bescherming A.8 Openheid, transparantie en kennisgeving	A.8.1	Bekendmaking van uitbestede PG-verwerking. Wanneer de public cloud Persoons Gegevens verwerker gebruik maakt van onderaannemers voor de verwerking van PG, moeten deze vóór gebruik worden bekendgemaakt aan de relevante cloudservice klanten.					X
A Public Cloud Persoons Gegevens bescherming A.10 Verantwoording	A.10.1	Melding van een datalek met PG. De public cloud Persoons Gegevens verwerker moet de betrokken cloudservice klant onmiddellijk op de hoogte brengen van ongeoorloofde toegang tot Persoons Gegevens of ongeoorloofde toegang tot verwerkingsapparatuur of -faciliteiten, die leiden tot verlies, openbaarmaking of wijziging van PG.					X
A Public Cloud Persoons Gegevens bescherming A.10 Verantwoording	A.10.2	Bewaartermijn voor beveiligingsbeleid en richtlijnen. Kopieën van beveiligingsbeleid en operationele procedures moeten worden bewaard gedurende een vastgelegde periode voor vervanging (inclusief bijwerking)					X
A Public Cloud Persoons Gegevens bescherming A.10 Verantwoording	A.10.3	Teruggave, overdracht en verwijdering van persoonsgegevens. De public cloud Persoons Gegevens verwerker moet een beleid hebben met betrekking tot de retournering, overdracht en/of verwijdering van PII en moet dit beleid beschikbaar stellen aan de cloudservice klant.					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.1	Vertrouwelijkheids- of geheimhoudings overeenkomsten. Personen die onder verantwoordelijkheid vallen van de public cloud Persoons Gegevens verwerker en die toegang hebben tot Persoons Gegevens moeten voldoen aan vertrouwelijkheid eisen					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.2	Beperking van het maken van hardcopy-materiaal. Het maken van hardcopy-materiaal met Persoons Gegevens moet worden beperkt					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.3	Beheer en logging van gegevensherstel. Er moet een procedure zijn voor en een logboek van gegevensherstel activiteiten.					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.4	Gegevens beschermen op mobiele opslagmedia. Persoons Gegevens op media die de panden van de organisatie verlaten, moet een autorisatieprocedure volgen en mag alleen toegankelijk zijn voor bevoegd personeel (bijvoorbeeld door de betreffende gegevens te versleutelen).					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.5	Gebruik van niet-versleutelde draagbare opslagmedia en apparaten. Mobiele fysieke media en draagbare apparaten zonder encryptie mogen niet worden gebruikt, behalve waar dit onvermijdelijk is, en elk gebruik van dergelijke draagbare media en apparaten moet worden geregistreerd.					X

A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.6	Encryptie van Persoons Gegevens on the move. Persoons Gegevens die wordt verzonden via openbare datatransmissie netwerken moet vóór verzending worden gecodeerd.					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.7	Veilige verwijdering van hardcopies. Wanneer hardcopies worden vernietigd, moeten deze veilig worden vernietigd met behulp van mechanismen zoals horizontaal snijden, versnipperen, verbranden, vermalen, enz.					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.8	Uniek gebruik van gebruikers-ID's. Als meer dan één persoon toegang heeft tot opgeslagen PG, moet elk persoon een afzonderlijke gebruikers-ID hebben voor identificatie, authenticatie en autorisatie					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.9	Vastlegging van geautoriseerde gebruikers. Er moet een up-to-date vastlegging worden onderhouden van de gebruikers of profielen van gebruikers die geautoriseerde toegang hebben tot het informatiesysteem					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.10	Beheer van gebruikers-ID's. Gedeactiveerde of verlopen gebruikers-ID's mogen niet aan andere personen worden verstrekt					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.11	Contractmaatregelen. Contracten tussen de klant van de clouddienst en de Persoons Gegevens verwerker voor de openbare cloud moeten minimale technische en organisatorische maatregelen bevatten, om ervoor te zorgen dat de overeengekomen beveiligingsregelingen van kracht zijn en dat de gegevens niet worden verwerkt buiten de instructies van de Persoons Gegevens verantwoordelijke. Dergelijke maatregelen mogen niet eenzijdig worden afgezwakt door de public cloud Persoons Gegevens verwerker.					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.12	Uitbesteding verwerking persoonsgegevens. Contracten tussen de public cloud Persoons Gegevens verwerker en eventuele subcontractanten die Persoons Gegevens verwerken, moeten minimale technische en organisatorische maatregelen omvatten die voldoen aan de informatiebeveiliging- en PG-beveiligingsverplichtingen van de public cloudPersoons Gegevens verwerker. Dergelijke maatregelen mogen niet eenzijdig worden					X
A Public cloud Persoons Gegevens bescherming A.11 Informatiebeveiliging	A.11.13	Toegang tot gegevens op gebruikte media. De public cloud Persoons Gegevens verwerker moet ervoor zorgen dat wanneer gegevensopslagruimte wordt toegewezen aan een klant van de cloudservice, alle gegevens die eerder in die opslagruimte aanwezig waren, niet zichtbaar zijn voor die klant van de cloudservice.					X
A Public cloud Persoons Gegevens bescherming A.12 Vertrouwelijkheid compliance	A.12.1	Geografische locatie van persoonsgegevens. De public cloud Persoons Gegevens verwerker moet de landen waarin Persoons Gegevens mogelijk kunnen worden opgeslagen specificeren en documenteren					X

A Public cloud Persoons Gegevens bescherming A.12 Vertrouwelijkheid compliance	A.12.2	Beoogde bestemming van persoonsgegevens. Voor persoonsgegevens die worden verzonden via een datatransmissie netwerk moeten passende maatregelen worden genomen, om ervoor te zorgen dat de gegevens de beoogde bestemming bereiken					X
ISO/IEC 27701:2019 Bijlage A (normatief), bedoeld voor organisaties die als PII-verwerkingsverantwoordelijke optreden, al dan niet met gebruikmaking van PII-verwerkers.							
Voorwaarden voor verzamelen en verwerken Doeleinde identificeren en documenteren	A.7.2.1	De organisatie moet de specifieke doeleinden waarvoor de PII wordt verwerkt, identificeren en documenteren.					X
Voorwaarden voor verzamelen en verwerken Rechtsgrond identificeren	A.7.2.2	De organisatie moet de relevante rechtsgrond voor het verwerken van PII voor de geïdentificeerde doeleinden vaststellen, documenteren en eraan voldoen					X
Voorwaarden voor verzamelen en verwerken Vaststellen wanneer en hoe toestemming moet worden verkregen	A.7.2.3	De organisatie moet een proces vaststellen en documenteren aan de hand waarvan zij kan aantonen of, wanneer en hoe toestemming voor het verwerken van PII is verkregen van PII-betrokkenen.					X
Voorwaarden voor verzamelen en verwerken Toestemming verkrijgen en registreren	A.7.2.4	De organisatie moet toestemming van PII-betrokkenen verkrijgen en registreren overeenkomstig de gedocumenteerde processen.					X
Voorwaarden voor verzamelen en verwerken Privacyeffectbeoordeling	A.7.2.5	De organisatie moet beoordelen of een privacy-effectbeoordeling nodig is en deze indien van toepassing implementeren, telkens als er nieuwe verwerkingen van PII of veranderingen aan de bestaande verwerking van PII gepland zijn.					X
Voorwaarden voor verzamelen en verwerken Overeenkomsten met PII-verwerkers	A.7.2.6	De organisatie moet een schriftelijke overeenkomst hebben met elke PII-verwerker waarvan zij gebruikmaakt en moet bewerkstelligen dat de overeenkomsten met PII-verwerkers ingaan op de implementatie van de passende beheersmaatregelen in bijlage B.					X
Voorwaarden voor verzamelen en verwerken Gezamenlijke PII verwerkingsverantwoordelijke	A.7.2.7	De organisatie moet respectievelijke rollen en verantwoordelijkheden vaststellen voor het verwerken van PII (met inbegrip van eisen voor de bescherming en beveiliging van PII) met een mede-PII-verwerkingsverantwoordelijke.					X
Voorwaarden voor verzamelen en verwerken Registraties met betrekking tot het verwerken van PII	A.7.2.8	De organisatie moet de noodzakelijke registraties ter ondersteuning van haar verplichtingen voor het verwerken van PII vaststellen en op beveiligde wijze bijhouden.					X
Verplichtingen naar PII-betrokkenen Verplichtingen naar PII-betrokkenen vaststellen en nakomen	A.7.3.1	De organisatie moet haar verplichtingen vanwege wet- en regelgeving en haar zakelijke verplichtingen naar PII-betrokkenen in verband met het verwerken van hun PII vaststellen en documenteren en voorzien in de middelen om aan deze verplichtingen te voldoen.					X
Verplichtingen naar PII-betrokkenen Informatie voor PII-betrokkenen vaststellen	A.7.3.2	De organisatie moet de aan PII-betrokkenen te verstrekken informatie met betrekking tot de verwerking van hun PII en het moment waarop die informatie verstrekt wordt, vaststellen en documenteren					X

Verplichtingen naar PII-betrokkenen Informatie geven aan PII-betrokkenen	A.7.3.3	De organisatie moet PII-betrokkenen voorzien van duidelijke en gemakkelijk toegankelijke informatie waarin de PII-verwerkingsverantwoordelijke wordt geïdentificeerd en de verwerking van hun PII wordt beschreven.					X
Verplichtingen naar PII-betrokkenen In een mechanisme voorzien om toestemming aan te passen of in te trekken	A.7.3.4	De organisatie moet voorzien in een mechanisme waarmee PII-betrokkenen hun toestemming kunnen aanpassen of intrekken.					X
Verplichtingen naar PII-betrokkenen In een mechanisme voorzien om bezwaar te maken tegen verwerking	A.7.3.5	De organisatie moet voorzien in een mechanisme waarmee PII-betrokkenen bezwaar kunnen maken tegen de verwerking van hun PII.					X
Verplichtingen naar PII-betrokkenen Toegang, correctie en/of wissen	A.7.3.6	De organisatie moet beleidsregels, procedures en/of mechanismen implementeren om te voldoen aan haar verplichtingen naar PII-betrokkenen met betrekking tot toegang tot en het corrigeren en/of wissen van hun PII.					X
Verplichtingen naar PII-betrokkenen erplichtingen van PII-verwerkingsverantwoordelijken om derden te informeren	A.7.3.7	De organisatie moet derden met wie PII is gedeeld, in kennis stellen van alle aanpassingen, intrekkingen of bezwaren met betrekking tot de gedeelde PII, en hiervoor passende beleidsregels, procedures en/of mechanismen implementeren.					X
Verplichtingen naar PII-betrokkenen Een kopie verstrekken van verwerkte PII	A.7.3.8	De organisatie moet in staat zijn een kopie van de verwerkte PII te verstrekken wanneer de PII-betrokkene daarom verzoekt.					X
Verplichtingen naar PII-betrokkenen Omgaan met verzoeken	A.7.3.9	De organisatie moet beleidsregels en procedures definiëren en documenteren voor het omgaan met en reageren op legitieme verzoeken van PII-betrokkenen.					X
Verplichtingen naar PII-betrokkenen Geautomatiseerde besluitvorming	A.7.3.10	De organisatie moet verplichtingen, met inbegrip van juridische verplichtingen, naar de PII-betrokkenen identificeren en oppakken die voortkomen uit door de organisatie genomen besluiten die verband houden met de PII-betrokkene, uitsluitend gebaseerd op geautomatiseerde verwerking van PII.					X
Privacy by design' en 'privacy by default' Het verzamelen beperken	A.7.4.1	De organisatie moet het verzamelen van PII beperken tot het minimum dat relevant, proportioneel en nodig is voor de geïdentificeerde doeleinden.					X
Privacy by design' en 'privacy by default' Het verwerken beperken	A.7.4.2	De organisatie moet het verwerken van PII beperken tot wat toereikend, relevant en nodig is voor de geïdentificeerde doeleinden.					X
Privacy by design' en 'privacy by default' Juistheid en kwaliteit	A.7.4.3	De organisatie moet bewerkstelligen en documenteren dat PII gedurende de volledige levenscyclus van de PII zo juist, volledig en actueel is als nodig is voor de doeleinden waarvoor de PII wordt verwerkt.					X
Privacy by design' en 'privacy by default' Doelstellingen voor minimale PII-verwerking	A.7.4.4	De organisatie moet doelstellingen voor minimale gegevensverwerking en de mechanismen (zoals het niet-identificeerbaar maken) die worden gebruikt om die doelstellingen te bereiken, definiëren en documenteren.					X

Privacy by design' en 'privacy by default' PII aan het einde van de verwerking nietidentificeerbaar maken en wissen	A.7.4.5	De organisatie moet PII wissen of omzetten in een vorm waardoor PII-betrokkenen niet langer geïdentificeerd of geheridentificeerd kunnen worden, zodra de originele PII niet meer nodig is voor het (de) geïdentificeerde doeleinde(n)					X
Privacy by design' en 'privacy by default' Tijdelijke bestanden	A.7.4.6	De organisatie moet bewerkstelligen dat tijdelijke bestanden die als gevolg van het verwerken van PII worden aangemaakt, binnen een gespecificeerde, gedocumenteerde periode volgens gedocumenteerdeC191:C209 procedures worden verwijderd (bijv. gewist of vernietigd).					X
Privacy by design' en 'privacy by default' Bewaring	A.7.4.7	De organisatie mag PII niet langer bewaren dan nodig is voor de doeleinden waarvoor de PII wordt verwerkt.					X
Privacy by design' en 'privacy by default' Verwijdering	A.7.4.8	De organisatie moet beschikken over gedocumenteerde beleidsregels, procedures en/of mechanismen voor de verwijdering van PII.					X
Privacy by design' en 'privacy by default' Beheersmaatregelen voor de overdracht van PII	A.7.4.9	De organisatie moet via een netwerk voor gegevensoverdracht verzonden PII (bijv. aan een andere organisatie) onderwerpen aan passende beheersmaatregelen die ervoor zijn ontworpen om te bewerkstelligen dat de gegevens hun beoogde bestemming bereiken					X
PII delen, doorgeven en verstrekken De grondslag voor doorgifte van PII tussen rechtsgebieden identificeren	A.7.5.1	De organisatie moet de relevante grondslag voor de doorgifte van PII tussen rechtsgebieden identificeren en documenteren					X
PII delen, doorgeven en verstrekken Landen en internationale organisaties waaraan PII kan worden doorgegeven	A.7.5.2	De organisatie moet de landen en internationale organisaties specificeren en documenteren waaraan PII mogelijk kan worden doorgegeven.					X
PII delen, doorgeven en verstrekken Registraties van doorgifte van PII	A.7.5.3	De organisatie moet doorgiften van PII aan of vanuit derden registreren en samenwerking bewerkstelligen met die derden ter	oor organisaties die als PII-verwerker optreden, al dan niet met gebruikmaking van PII-onderaannemers.				X
PII delen, doorgeven en verstrekken Registraties van de verstrekking van PII aan derden	A.7.5.4	De organisatie moet de verstrekking van PII aan derden registreren, met inbegrip van welke PII is verstrekt, aan wie en wanneer..					X
ISO/IEC 27701:2019 Bijlage B (normatief), bedoeld voor gebruik door organisaties die als PII-verwerker optreden, al dan niet met gebruikmaking van PII-onderaannemers.							
Voorwaarden voor verzamelen en verwerken Overeenkomst met de klant	B.8.2.1	De organisatie moet waar relevant bewerkstelligen dat de overeenkomst voor het verwerken van PII ingaat op de rol van de organisatie bij het ondersteunen van de verplichtingen van de klant (rekening houdend met de aard van de verwerking en de informatie die beschikbaar is voor de organisatie).					X
Voorwaarden voor verzamelen en verwerken Doeleinden van de organisatie	B.8.2.2	De organisatie moet bewerkstelligen dat namens een klant verwerkte PII uitsluitend wordt verwerkt voor de doeleinden die worden aangegeven in de schriftelijke opdracht van de klant					X

Voorwaarden voor verzamelen en verwerken Gebruik voor marketing en reclame	B.8.2.3	De organisatie mag krachtens een overeenkomst verwerkte PII niet voor marketing- en reclamedoeleinden gebruiken zonder vast te stellen dat daarvoor vooraf toestemming is verkregen van de desbetreffende PII-betrokkene. De organisatie mag het geven van die toestemming niet als voorwaarde stellen voor het ontvangen van de dienst.					X
Voorwaarden voor verzamelen en verwerken Opdracht die inbreuk oplevert	B.8.2.4	De organisatie moet de klant in kennis stellen indien, naar haar mening, een verwerkingsopdracht inbreuk oplevert op toepasselijke wet- en/of regelgeving					X
Voorwaarden voor verzamelen en verwerken Verplichtingen van klanten	B.8.2.5	De organisatie moet de klant voorzien van de passende informatie zodat de klant kan aantonen dat hij aan zijn verplichtingen voldoet.					X
Voorwaarden voor verzamelen en verwerken Registraties met betrekking tot het verwerken van PII	B.8.2.6	De organisatie moet de benodigde registraties vaststellen en onderhouden ter ondersteuning van het aantonen van het voldoen aan haar verplichtingen (zoals gespecificeerd in de desbetreffende overeenkomst) voor het verwerken van PII namens een klant.					X
Verplichtingen naar PII-betrokkenen Verplichtingen naar PII-betrokkenen	B.8.3.1	De organisatie moet de klant van de middelen voorzien om te voldoen aan zijn verplichtingen met betrekking tot PII-betrokkenen.					X
Privacy by design' en 'privacy by default' Tijdelijke bestanden	B.8.4.1	De organisatie moet bewerkstelligen dat tijdelijke bestanden die als gevolg van het verwerken van PII worden aangemaakt, binnen een gespecificeerde, gedocumenteerde periode volgens gedocumenteerde procedures worden verwijderd (bijv. gewist of vernietigd).					X
Privacy by design' en 'privacy by default' Retournering, doorgifte of verwijdering van PII	B.8.4.2	De organisatie moet de mogelijkheid bieden om PII op beveiligde wijze te retourneren, over te dragen en/of te verwijderen. Zij moet haar beleid ook aan de klant ter beschikking stellen.					X
Privacy by design' en 'privacy by default' Beheersmaatregelen voor de overdracht van PII	B.8.4.3	De organisatie moet via een netwerk voor gegevensoverdracht verzonden PII onderwerpen aan passende beheersmaatregelen die ervoor zijn ontworpen om te bewerkstelligen dat de gegevens hun beoogde bestemming bereiken.					X
PII delen, doorgeven en verstrekken Grondslag voor doorgifte van PII tussen rechtsgebieden	B.8.5.1	De organisatie moet de klant tijdig informeren over de grondslag voor de doorgiften van PII tussen rechtsgebieden en over eventuele voorgenomen veranderingen in dit opzicht, zodat de klant bezwaar kan maken tegen dergelijke veranderingen of de overeenkomst kan beëindigen					X
PII delen, doorgeven en verstrekken Landen en internationale organisaties waaraan PII kan worden doorgegeven	B.8.5.2	De organisatie moet de landen en internationale organisaties specificeren en documenteren waaraan PII mogelijk kan worden doorgegeven.					X
PII delen, doorgeven en verstrekken Registraties van de verstrekking van PII aan derden	B.8.5.3	De organisatie moet de verstrekking van PII aan derden registreren, met inbegrip van welke PII is verstrekt, aan wie en wanneer.					X

PII delen, doorgeven en verstrekken Kennisgeving van verzoeken om verstrekking van PII	B.8.5.4	De organisatie moet de klant kennis geven van eventuele juridisch bindende verzoeken om verstrekking van PII.					X
PII delen, doorgeven en verstrekken Juridisch bindende verstrekking van PII	B.8.5.5	De organisatie moet alle verzoeken om de verstrekking van PII afwijzen die niet juridisch bindend zijn, de desbetreffende klant raadplegen alvorens PII te verstrekken en contractueel overeengekomen verzoeken om het verstrekken van PII waarvoor de desbetreffende klant autorisatie heeft gegeven, accepteren.					X
PII delen, doorgeven en verstrekken Bekendmaking van onderaannemers die worden ingezet voor het verwerken van PII	B.8.5.6	De organisatie moet de klant op de hoogte stellen over de eventuele inzet van onderaannemers voor het verwerken van PII aan voordat zij worden ingezet.					X
PII delen, doorgeven en verstrekken Betrokkenheid van een onderaannemer voor het verwerken van PII	B.8.5.7	De organisatie mag alleen een onderaannemer voor het verwerken van PII inschakelen overeenkomstig de overeenkomst met de klant.					X
PII delen, doorgeven en verstrekken Verandering van onderaannemer voor het verwerken van PII	B.8.5.8	De organisatie moet, indien zij algemene schriftelijke autorisatie heeft, de klant in kennis stellen van voorgenomen veranderingen met betrekking tot het toevoegen of vervangen van onderaannemers voor het verwerken van PII, en de klant daarmee de gelegenheid bieden bezwaar te maken tegen die veranderingen.					X