gemeente Barneveld

Bijlage 2AD - Programma van Eisen Meedoenplatform

Inhoudsopgave

1. Functionele eisen

Algemeen	
1.	De leverancier en het meedoenplatform voldoen aan landelijke wet- en regelgeving, ook na wijziging hiervan.
2.	De leverancier levert, implementeert en exploiteert een meedoenplatform gericht op het ontsluiten van gemeentelijke regelingen en maatschappelijke initiatieven voor Barneveldse inwoners met een laag inkomen.
3.	De leverancier levert een meedoenplatform dat het volledige proces ondersteunt. Dat wil zeggen dat de inwoner kan aanvragen, de gemeente kan toetsen en afhandelen, de inwoner de regeling(en) kan benutten, de gemeente het aanbod kan beheren en de financiële afwikkeling met de aanbieder/inwoner wordt verzorgd.
4.	Alle bestaande minimaregelingen kunnen in hun huidige inrichtingsvorm (zie AD 1.8) ontsloten worden.
5.	Het platform is v.w.b. de ontsluiting van minimaregelingen volledig ingericht en operationeel op 01 april 2026.
6.	Uiterlijk 01 juli 2026 zijn maatschappelijke initiatieven via het platform richting inwoners te ontsluiten.
7.	De leverancier van het platform biedt gedurende de looptijd van de overeenkomst gebruikersondersteuning en functioneel beheer.
8.	De leverancier factureert aan opdrachtgever voor 15 december 2025 de implementatiekosten conform overeenkomst volledig onder vermelding van een door opdrachtgever gegeven routenummer. Uitbetaling vindt plaats onder voorbehoud van oplevering conform afspraken.
9.	De leverancier factureert aan opdrachtgever de jaarlijkse kosten conform overeenkomst eenmaal per kalenderjaar onder vermelding van een door opdrachtgever gegeven routenummer.
10.	De leverancier verzorgt via het systeem de betalingen aan inwoners en aanbieders voortvloeiend uit het gebruik van minimaregelingen. Hoe dit plaatsvindt, inclusief financiële afwikkeling met opdrachtgever, wordt nader overeengekomen.
11.	Binnen de in de aanbesteding afgesproken prijzen zijn inwoners, gebruikers binnen de gemeente en aanbieders toe te voegen dan wel te verwijderen.
12.	De leverancier levert binnen de opdracht maximale inspanning om het gebruik door minima, de gemeente en aanbieders te bevorderen.
13.	De leverancier biedt de mogelijkheid om in de toekomst een andere gemeente aan te laten sluiten waarmee een samenwerkingsverband is afgesloten, waarvoor de opdrachtgever de uitvoering verzorgt. Hierbij blijven de gegevens wel gescheiden en heeft de andere gemeente een andere invulling van haar minimabeleid.

Functioneel gebruik en toegankelijkheid	
14.	Het systeem bezit portals voor inwoners, aanbieders en de gemeente.
15.	Het platform beschikt over een openbare informatiepagina voor inwoners en andere gebruikers met daarop minimaal alle relevante informatie rondom het platform, de regelingen/ondersteuning, aanvragen, gebruik en aanbod.
16.	De inwoner kan een aanvraag volledig en rechtmatig doen om toegang tot de minima-ondersteuning te krijgen (aanvraag minimabeleid) binnen het platform, ondertekend met DigiD. Indien de inwoner kiest voor een aanvraag op papier, kan een medewerker van de gemeente na ontvangst de aanvraag digitaliseren, in proces brengen en aan het dossier toevoegen.
17.	De inwoner identificeert zich met DigiD of, in geval van een op papier ingediende aanvraag, een andere oplossing voorzien van 2-factor authenticatiemethode zonder authenticatie-app om toegang tot zijn/haar omgeving te krijgen.
18.	Een aanbieder logt in op het platform via eHerkenning of met een eigen gebruikersnaam en wachtwoord die hij zelf kan aanmaken. Bij gebruik van gebruiksnaam en wachtwoord moet de aanbieder inloggen met een 2 factor authenticatie methode.
19.	Het platform is flexibel in te richten. Nieuw of aangepast aanbod binnen een minimaregeling of maatschappelijk aanbod is binnen 1 werkdag beschikbaar voor inwoners.
20.	Een wijziging van bestaand of toevoeging van nieuw aanbod voor inwoners van aanbieders wordt beschikbaar na toestemming van de gemeente.
21.	Het platform registreert inwoners onder verschillende subgroepen met als doel inwoners gericht te kunnen informeren en gerichte data te kunnen ontsluiten.
22.	Binnen de gebruikersgroep ‘gemeente’ zijn er verschillende autorisatiemogelijkheden. De opdrachtgever bepaalt wie welke rechten heeft.
23.	Het systeem faciliteert volwaardige en volledige toetsing en controle door de gemeente op recht- en doelmatigheid.
24.	De leverancier ondersteunt met de inrichting van het platform het bevorderen van rechtmatig gebruik dan wel het voorkomen van misbruik.
25.	Signalen van mis- en oneigenlijk gebruik van minima-ondersteuning meldt de leverancier per omgaande aan de opdrachtgever.

Toegankelijkheid algemeen	
26.	De leverancier levert een oplossing die een toegankelijke gebruikerservaring biedt.
27.	De schermen van portalen voor inwoners en aanbieders zijn geschikt voor smartphone, tablet en computer. De schermen van het portaal voor de gemeente zijn geschikt voor tablet en computer. De schermen passen zich automatisch aan de schermafmetingen van het gebruikte apparaat aan.
28.	De portalen van het platform worden ingericht conform de huisstijl van de gemeente Barneveld en kent een organisatie specifieke URL (subdomein.barneveld.nl).
29.	In het systeem kunnen woon- en postadres afwijkend zijn.
30.	In het geval er een beschermingsbewindvoerder of curator is aangewezen, is dit zichtbaar en zijn de inlogmogelijkheden en wijzigingsrechten (zoals postadres en rekeningnummer) van de inwoner hierop aangepast.

Toegankelijkheid en gebruik inwoner	
31.	De inwoner kan binnen en met behulp van het platform een volledige en rechtmatige aanvraag doen, voorzien van alle benodigde bewijsstukken.
32.	De inwoner heeft (na aanvraag) een persoonlijke omgeving en behoudt deze tot in ieder geval een jaar na de laatste beoordeling op rechtmatigheid.
33.	Binnen de persoonlijke omgeving van de inwoner is minimaal het volgende beschikbaar bij/na het doen van de aanvraag: - status van aanvraag inzien - raadplegen, uploaden en downloaden van documenten - raadplegen van gelezen en ongelezen berichten - reageren op vragen (bijv. hersteltermijn of aanvullende informatie) - toestemming geven (of afwijzen) om digitaal berichten vanuit de gemeente te ontvangen.
34.	Binnen de persoonlijke omgeving van de inwoner is na toekenning van de aanvraag minimaal beschikbaar: - bericht aan/van gemeente verzenden/beantwoorden - per gezinslid zicht op alle beschikbare ondersteuning (incl. termijn) - inzetten van (een deel van) de beschikbare ondersteuning - per gezinslid zicht op ondersteuning die nog beschikbaar is of komt (incl. datum) - per gezinslid zicht op reeds benutte ondersteuning (incl. wanneer ingezet) - geldigheidsduur van de toekenning (bijv. nog 9 maanden tot hertoetsing) - zelfstandig aanpassen van contactgegevens - wijziging bankrekeningnummer aanvragen (gemeente controleert en keurt goed/af)
35.	De inwoner heeft binnen de persoonlijke omgeving informatie over waar en wanneer hij/zij met vragen terecht kan.

Toegankelijkheid en gebruik gemeente	
36.	Zodra in een dossier een handeling nodig is (zoals bij een mutatie, hersteltermijn of heronderzoek) is dit zichtbaar en geprioriteerd in de workflow.
37.	Het is mogelijk om zowel de volledige workflow van het team (Servicepunt) als de individuele workflow (unieke gebruiker) te raadplegen.
38.	Het is mogelijk dossiers of de workload automatisch onder gebruikers te verdelen en/of over te dragen.
39.	Op inwonersniveau is een waarschuwingsfunctionaliteit beschikbaar waarin aantekeningen kunnen worden gemaakt. Deze komt direct bij raadplegen van het dossier naar voren (bijv. bewind, geheim nummer of agressief gedrag) en is niet zichtbaar voor de inwoner.
40.	De gemeente ziet in een dossier, naast de eigen functionaliteit, alle informatie die een inwoner tot zijn/haar beschikking heeft (zie o.a. eisen 33 en 34).
41.	Binnen een dossier is zoeken op inhoud, bericht of contactmoment mogelijk.
42.	Het is zowel automatisch als handmatig mogelijk om termijnen in te regelen en te bewaken.
43.	Aanvragen op papier, documenten en berichten zijn (zo veel mogelijk automatisch) aan het dossier van een inwoner toe te voegen.
44.	De mogelijkheid bestaat om aantekeningen in het dossier van een inwoner te plaatsen die alleen zichtbaar zijn voor de gemeente.
45.	De gemeente kan mutaties in de workflow (zowel automatisch als handmatig) controleren en desgewenst goed-/afkeuren.

46.	Aanvragen van inwoners zijn volledig behandelen en af te handelen.
47.	De gemeente kan aanbod voor inwoners automatisch dan wel handmatig beschikbaar maken.
48.	De gemeente kan mutaties van inwoners controleren en goedkeuren/afwijzen.
49.	De gemeente kan (gemotiveerd) nieuw en veranderd aanbod goedkeuren, een wijzigingsvoorstel doen dan wel afwijzen.
50.	De gemeente kan aanbieders (tijdelijk) blokkeren of verwijderen.
51.	De gemeente kan standaard/geautomatiseerd en incidenteel berichten aan (sub)groep inwoners sturen.
52.	De gemeente kan per inwonersgroep of individuele gebruiker een pakket aan regelingen activeren of in geval van aanbieders aanbod activeren.

Toegankelijkheid en gebruik aanbieders	
53.	Een potentieel toekomstig aanbieder kan bij de gemeente via het platform een verzoek indienen om aanbieder te worden binnen een minimaregeling en/of als maatschappelijk initiatief.
54.	Een aanbieder kan binnen zijn account/omgeving van toepassing zijnde bedrijfs- en crediteurgegevens vastleggen en wijzigen.
55.	Een aanbieder kan zijn aanbod zelfstandig in het platform opstellen en deze kenbaar maken richting de gemeente.
56.	De aanbieder ontvangt bericht zodra de gemeente het aanbod heeft beoordeeld (afwijzen, wijzigingsvoorstel, goedkeuren).
57.	Zodra de inwoner de aangeboden ondersteuning van de aanbieder wil benutten, krijgt de aanbieder hiervan bericht.
58.	Zodra de aanmelding van de inwoner door de aanbieder is verwerkt/opgepakt, registreert de aanbieder dit in het systeem. De inwoner ontvangt hiervan automatisch een bericht uit het systeem.
59.	In geval van minima-ondersteuning, wordt de gemeentelijke vergoeding aan de aanbieder beschikbaar gesteld nadat de aanbieder heeft geregistreerd dat de aanmelding van de inwoner is geeffectueerd.

Communicatie	
60.	Standaardteksten op de informatiepagina en in het meedoenplatform die de opdrachtgever niet zelf kan wijzigen zijn geschreven op B1-taalniveau of eenvoudiger.
61.	Alle communicatie met de ondersteuningsorganisatie van de leverancier is in het Nederlands.
62.	De leverancier stelt voor live-gang van het platform een communicatieplan op, gericht op inwoners binnen de doelgroep, hun omgeving en aanbieders. Deze wordt in samenspraak met de opdrachtgever opgesteld en na vaststelling uitgevoerd.
63.	Alle berichtgeving wordt ingeregeld dan wel incidenteel verzonden na goedkeuring van een geautoriseerde medewerker van de gemeente.
64.	In de applicatie kunnen door de opdrachtgever sjablonen worden aangemaakt, gewijzigd en verwijderd om documenten aan te maken. In deze sjablonen kunnen gegevens uit de applicatie worden samengevoegd met tekstblokken. Ook kunnen tekstblokken optioneel worden getoond op basis van de gegevens in de applicatie.

65.	Alleen een geautoriseerde medewerker van de opdrachtgever (of de leverancier op verzoek van de opdrachtgever) is bevoegd om standaard documentatie/sjablonen aan te passen.

Rapportage	
66.	De applicatie moet standaard rapportages hebben voor operationele en tactische besturing van de geïmplementeerde workflows. In de rapportages moet minimaal gefilterd kunnen worden op gebruikersrol, regeling, periode en peildatum.
67.	De opdrachtgever kan zonder tussenkomst van de leverancier op elk gewenst tijdstip een standaard managementrapportage vervaardigen.
68.	De standaard managementrapportage bevat minimaal: - Aantallen huishoudens en hoeveel volwassenen en kinderen per huishouden. - Aantallen per type inkomen en eventuele combinaties. - Aantallen per inkomenspercentages <100%, <110% en <120% - Aantal maatwerktoekenningen - Potentiële doelgroep in percentage afgezet tegen bereik. - Per minimaregeling of maatschappelijk initiatief aantallen rondom beschikbaarheid en gebruik. - Mutaties (zoals instroom, uitstroom incl. reden). - Monitoring verloop gebruik (0-meting en verandering in de tijd) - Gemaakte kosten, verwachte uitgaven en potentieel financieel risico. - Omvang doelgroep verdeeld naar wijkniveau/postcodegebied.
69.	De opdrachtgever kan met een rapportage-tool analyses uitvoeren op alle gegevens en informatie die in het systeem zijn vastgelegd.

Beveiliging en autorisatie van gegevens	
70.	De gemeente Barneveld kan zelf de benodigde rollen binnen de gebruikerstypen definiëren in de applicatie en daar de autorisaties aan toekennen.
71.	Autorisatieprofielen voor de verschillende gedefinieerde rollen kunnen worden gewijzigd. Het is mogelijk om bepaalde vertrouwelijke zaken standaard af te schermen.
72.	De applicatie heeft de mogelijkheid, DAT en WAT informatie zorgvuldig te scheiden. Autorisaties kunnen aldus enkel gericht zijn op het zien van DAT informatie (algemene informatie over de inwoner en zijn interacties) of de WAT informatie (de DAT informatie plus de inhoudelijke details). De inrichting kent meerdere rollen, zodat medewerkers alleen bij gegevens kunnen die zij nodig hebben voor hun werk.
73.	De inlogmethode voor interne gebruikers via de werkplek van de gemeente Barneveld is Single Sign On (SSO). Buiten deze omgeving wordt ingelogd met twee factor authenticatie.
74.	Het systeem biedt de mogelijkheid om toegang tot en wijziging van persoonsgegevens te loggen. De opdrachtgever moet zelf de logging en monitoring kunnen uitvoeren en parameters hiervoor kunnen bepalen.
75.	De applicatie moet ingericht zijn om informatie te verwerken conform BBN2 classificatie.

76.	Alle data moet binnen de Europese Economische Ruimte (EER) verwerkt worden (uitspraak Schrems II). Dit geldt voor de (back up) servers en de (back up) servers van eventuele subverwerkers. De data moet versleuteld worden opgeslagen.
77.	Het systeem is op een dusdanige wijze ingericht dat de opdrachtgever zelf gehoor kan geven aan het recht op inzage, correctie en verwijdering van gegevens. Via een ID moet makkelijk en snel te achterhalen zijn of iemands persoonsgegevens worden verwerkt en indien nodig geëxporteerd worden in een leesbaar format.
78.	De leverancier werkt bij beëindiging van het contract onvoorwaardelijk mee aan het beschikbaar stellen van de data en andere informatie om de overdracht aan de nieuwe leverancier te bespoedigen cq te verbeteren. De leverancier maakt daartoe - conform artikel 26 van de Gibit - een exit-plan die met de opdrachtgever wordt afgestemd.
79.	Er wordt een verwerkersovereenkomst afgesloten, zoals ook is opgenomen in artikel 28 van de GIBIT. De verwerkersovereenkomst is identiek aan de meest recente versie van de standaard verwerkersovereenkomst van de VNG.
80.	De leverancier werkt mee aan een DPIA die de opdrachtgever uitvoert. De DPIA moet zijn goedgekeurd en vastgesteld voordat de applicatie in gebruik wordt genomen.

2 Niet functionele eisen

Algemeen	
81.	De applicatie wordt geleverd als een SaaS (applicatie als een service) of een managed service (leverancier host de applicatie specifiek voor een klant).
82.	De ICT prestatie voldoet (aangetoond met een WCAG-EM rapport) of voldoet nog niet aan alle geldende technische WCAG richtlijnen. Wanneer aan niet aan alle richtlijnen voldaan wordt, neemt de leverancier maatregelen om daaraan wel te voldoen. Uiterlijk 6 maanden na de oplevering van de ICT prestatie, toont leverancier de opdrachtgever een WCAG-EM rapport. Leverancier laat jaarlijks verbeteringen zien, zodanig dat gestreefd wordt naar een A-status.

Service en beschikbaarheid	
83.	Aan de overeenkomst wordt een SLA toegevoegd. De leverancier geeft aan welke SLA-voorstellen hij heeft, wat de KPI's van de diensten zijn inclusief de bijbehorende kosten. Bij de definitieve gunning worden afspraken gemaakt over welke SLA van toepassing zal zijn.
84.	De leverancier stelt aan het einde van de implementatiefase een DAP (Dossier Afspraken en Processen) op samen met de opdrachtgever. De eerste door beide partijen goedgekeurde DAP wordt toegevoegd als bijlage aan de overeenkomst tussen partijen. Als er wijzigen zijn, wordt de DAP bijgewerkt. Nieuwe versies van de DAP hoeven niet aan de overeenkomst te worden toegevoegd mits beide partijen akkoord zijn met de wijzigingen. In de DAP wordt o.a. opgenomen welke overleggen er zullen worden ingepland, welke contactpersonen er zijn voor welke activiteiten (inclusief contractgegevens), wat de inhoud is van de maanrapportages, hoe processen verlopen (denk aan melden van incidenten, aanvragen van wijzigingen en escalaties), etc.
85.	De opdrachtgever heeft voor het melden van vragen, storingen, of wijzigingsvoorstellen één loket bij de leverancier (n.l. de supportdesk). Dit loket houdt de contactpersoon bij de opdrachtgever op de hoogte van het verloop en de voortgang van de melding binnen de gestelde SLA.
86.	De leverancier biedt een portaal voor aan- en afmeldingen van storingen, opvragen van statusinformatie, indienen change verzoeken en het stellen van vragen over bijvoorbeeld facturen e.d.
87.	Verstoringen, wijzigingen (o.a. nieuwe versies) in de dienstverlening van de leverancier worden doorgegeven via het portaal.
88.	De portalen voor inwoners en aanbieders hebben dagelijks tussen 08.00 en 23.00 uur een servicelevel van minimaal 98% beschikbaarheid.
89.	Het portaal voor de gemeente heeft een servicelevel van minimaal 98% beschikbaarheid op werkdagen tussen 08:00 en 17:00.
90.	Onderhoud van de leverancier vindt plaats buiten genoemde kantoortijden (eis 86).
91.	Het toegangsscherm van de portalen en back-office omgeving moet via een link (URL) op een informatiepagina op het internet op te starten zijn.
92.	Alle functionele beheertaken met betrekking tot de applicatie kunnen worden uitgevoerd terwijl gebruikers zijn ingelogd.

Autorisatie en logging	
93.	De identificatie en authenticatie van medewerkers vindt plaats op basis van de opdrachtgever identity store (Azure Active Directory), op basis van de actuele Microsoft-standaard (SAML 2.0 protocol).
94.	Sessies behoren authentiek te zijn voor elke gebruiker en worden automatisch inactief na een instelbaar aantal minuten en afgebroken na een (nader af te spreken) vaste tijd.
95.	Correcte en foutieve toegang tot de applicatie wordt gelogd.
96.	De gegevens over wie welke handelingen in de applicatie met welk doel heeft uitgevoerd wordt gelogd, en zijn raadpleegbaar voor de medewerkers die voor het toezicht ervoor verantwoordelijk zijn of kunnen via een standaard koppeling worden ingeladen in analyse- en monitoromgeving. N.B. hieronder vallen ook gegevensuitwisselingen met andere systemen
97.	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
98.	De loggegevens moeten voor beheerders toegankelijk zijn via een GUI of API.
99.	De loggegevens zijn instelbaar door en beschikbaar voor de opdrachtgever. Minimaal 2 jaar of langer bij een vermoed beveiligingsincident.

Gebruikerstoegankelijkheid en workflow	
100.	In de (algemene) werkvoorraad is het mogelijk om prioritering aan te geven en te wijzigen en een overzicht te maken.
101.	De applicatie heeft (zo visueel mogelijk) een overzicht en inzicht in de prioriteit, status, termijnsignalering en behandeld medewerker van actieve workflows.
102.	De applicatie ondersteunt het bewaken, signaleren en inregelen van termijnen in workflows die aan de verschillende wetgevingen verbonden zijn of gemeentelijk zijn bepaald. In een workflow kan opschorting van deze termijn met variabele duur plaatsvinden.
103.	De workflows in het systeem zijn zaakgericht ingericht of kunnen worden ingericht. Dit betekent dat: - Alle gecreëerde en ontvangen Informatie in een workflow wordt opgeslagen in een digitaal zaakdossier - Het zaakdossier krijgt metadata voor de vernietiging of bewaren ervan - De aanvrager op de hoogte wordt gehouden van de voortgang van zijn aanvraag (statusmeldingen)

Documentbeheer en archivering	
104.	De applicatie moet de verschillende bestandformaten kunnen uploaden en vastleggen: o.a. Excel, ODS, Word, ODT, PDF. PNG, BMP, JPEG, JPG, GIF, MP3, MP4, WAV, WMA, WMV.
105.	Bij een wijziging van de bewaartermijn in de gemeentelijke selectielijst, kunnen de betreffende metadata worden aangepast
106.	De applicatie kan een lijst genereren van de te vernietigen (of over te brengen) Informatieobjecten op basis van jaar van vernietiging of overbrenging
107.	De datum voor het vernietigen of overbrengen van Informatieobjecten (indien van toepassing) kan automatisch berekend worden

108.	De in de applicatie opgeslagen data blijft duurzaam toegankelijk (vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en toekomstbestendig; voor iedereen die daar recht op heeft en voor zo lang als noodzakelijk) gedurende de looptijd van de leveranciersovereenkomst
109.	Informatieobjecten en bijbehorende metadata kunnen onherstelbaar worden vernietigd op basis van de opgegeven waardering en/of bewaartermijn en ingangsdatum bewaartermijn. Dat geldt voor alle door de leverancier gebruikte fysieke en virtuele opslaglocaties
110.	De leverancier kan garanderen dat geen gegevens meer terug in productie omgeving kunnen worden geplaats na formele vernietiging. (vaak staan gegevens nog op server leverancier, of in backups).
111.	Informatieobjecten worden voorzien van metadata over waardering, bewaartermijn, ingangsdatum bewaartermijn. De Informatieobjecten worden die aangemaakt in één workflow krijgen dezelfde waardering, bewaartermijn, en ingangsdatum bewaartermijn.
112.	Van de vernietiging kan een verklaring worden opgeleverd, waarin minimaal wordt aangegeven om welke informatie het gaat.

Beveiliging gegevens	
113.	Gegevens en informatie worden versleuteld opgeslagen en uitgewisseld met andere applicaties met een passende standaard. De versleuteling wordt gedaan volgens actuele NCSC c.q. OWAPS richtlijnen Cryptograhic
114.	De leverancier en zijn toeleveranciers geven opvolging aan de beveiligingsadviezen van de opdrachtgever en meldt beveiligingsincidenten aan de opdrachtgever (aan de functionaris gegevensbescherming, CISO). De leverancier stelt de opdrachtgever direct (uiterlijk binnen 8 uur) op de hoogte van veiligheidsincidenten (bijvoorbeeld een datalek of security-incident) en de bijbehorende ICT-oplossingtermijn. De leverancier informeert hierbij over het feit of de 'bedreiging' wel of niet adequaat is opgelost en de eventuele gevolgen en impact van het veiligheidsincident als wel het oplossen hiervan.
115.	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.
116.	De leverancier laat periodiek door een onafhankelijke organisatie penetratietesten uitvoeren en rapporteert hierover minimaal eens per jaar aan de CISO van de opdrachtgever.
117.	De processen en het verwerken van gegevens in de applicatie en koppelingen moeten voldoen aan "privacy by default" (zie hiervoor Handleiding Privacy by Design van Ministerie van Justitie en Veiligheid)

Applicatie wijzigingen en raadplegingen	
118.	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van applicaties tijdig, geautoriseerd en getest worden doorgevoerd.

119.	Onverhoopt foutieve applicatie of systeemwijzigingen zijn eenvoudig en binnen 4 uur terug te draaien zonder de verdere consistentie en werking van de applicatie negatief te beïnvloeden
120.	De applicatie is dusdanig schaalbaar dat geen beperking plaatsvindt in de hierin opgeslagen gegevens informatie, aantallen gebruikers, transacties of parameter instellingen. Automatisch worden hiervoor hardware-middelen bijgeschakeld.
121.	Het op grote schaal raadplegen van de gegevens of informatie van de applicatie voor o.a. analyses mag geen invloed hebben op de prestaties van de applicatie.
122.	De doorlooptijd voor een rapportage is afhankelijk van de totaal opgevraagde gegevensset, niet van de hoeveelheid aanwezige gegevens. Rapportages genereren mag niet langer duren 1 minuut. Uitgaand van voldoende netwerk bandbreedte tussen de locatie waar de applicatie wordt gehost en gebruiker.
123.	Transacties, raadplegingen mogen niet langer duren van 1,5 seconden in 90% van de gevallen. Zoekschermen moeten binnen 5 seconden een resultaat opleveren. Dit bij 100 gelijktijdige gebruikers en voldoende netwerk bandbreedte tussen de locatie waar de applicatie wordt gehost en gebruiker.

Foutbestendigheid en integriteit	
124.	Bij het invoeren van gegevens moet worden gecontroleerd of de gegevens het formaat en waarde hebben waarmee zij worden opgeslagen of worden opgevraagd. Ook worden waarschijnlijkheid controles uitgevoerd op ingevoerde gegevens of kunnen worden ingericht.
125.	De foutafhandeling in de applicatie is dusdanig ontworpen dat: - een begrijpelijke foutmelding wordt getoond aan de gebruikers. - de gebruikers na de foutmelding kunnen doorwerken in applicatie.
126.	Bij het invoeren van gegevens moet worden gecontroleerd of de gegevens het formaat en waarde hebben waarmee zij worden opgeslagen of worden opgevraagd. Ook worden waarschijnlijkheid controles uitgevoerd op ingevoerde gegevens of kunnen worden ingericht.
127.	Wanneer een transactie door een gebruiker of fout in de applicatie wordt afgebroken dan brengt de applicatie de gegevens weer in de consistente toestand voor de transactie.
128.	De leverancier heeft een back-up-, disaster- en recoveryprocedure die gedocumenteerd, getest, operationeel en goedgekeurd is door de opdrachtgever. De basis hiervoor zijn de afgesproken RTO en RPO. De test moet minimaal één keer per jaar worden uitgevoerd en gerapporteerd aan de CISO van de opdrachtgever.
129.	Een back-up is ‘onmuteerbaar’ dus kan niet meer worden aangepast of verwijderd vanaf de originele locatie nadat die is weggeschreven. De verwijdering van back-ups dan alleen door een geautoriseerd verwijderingsproces.
130.	De back-up wordt versleuteld opgeslagen volgens actuele NCSC c.q. OWASP-richtlijnen Cryptograhic
131.	Dataverlies bij verstoring (RPO) is maximaal 1 uur.
132.	De dienstverlener doorloopt vóór het in productie nemen van de dienst of applicatie een ICT-beveiligingsassessment DigiD, zoals bedoeld in- en volgens-de eisen die Logius stelt aan aansluithouders, specifiek Serviceorganisaties. Zie hiervoor https://www.logius.nl/onze-dienstverlening/toegang/digid/ict-beveiligingsassessments-digid.

	De specifieke eisen die worden gesteld aan een Serviceorganisatie, staan hier: https://www.logius.nl/onze-dienstverlening/toegang/digid/ict-beveiligingsassessments-digid/it-auditrapportage-voor-digid.
133.	De leverancier levert van het initiële ICT-beveiligingsassessment DigiD een TPM/RSO aan, volgens de normen van Logius, te vinden op eerdergenoemde webpagina.
134.	De leverancier levert vervolgens jaarlijks, uiterlijk op 31 oktober van het jaar, een TPM/RSO aan volgens de normen van Logius.

Koppelingen	
135.	De applicatie is te koppelen met minimaal: - Microsoft Outlook - Key2Datadistributie - DigD - eHerkenning - Zorgned - Suite4SociaalDomein - Bank (i.v.m. betaalopdrachten)
136.	Het versturen van e-mailberichten vanuit de applicatie vindt plaats via de mailserver van de opdrachtgever.
137.	Koppelingen tussen applicatie houden geen status bij tijdens het uitwisselingen van gegevens. Wanneer een uitwisseling niet is gelukt, moet de applicatie of gebruiker de uitwisseling opnieuw opstarten. Wel worden fouten bij de uitwisseling gelogd.
138.	De applicatie kan API's van andere externe applicaties gebruiken om gegevens of informatie te kunnen muteren of een mutatie c.q. actie kunnen initiëren.
139.	De leverancier gebruikt veilige API's voor import en export van gegevens, bijvoorbeeld MS Power BI (OWASP ASVS 2020: V13).
140.	De te leveren applicatie heeft standaard koppelingen om gegevens en informatie die zijn vastgelegd in de applicatie te muteren (wijzigen, toevoegen, verwijderen) door andere applicaties.
141.	De te leveren applicatie heeft standaard API-koppelingen om gegevens en informatie die zijn vastgelegd in de applicatie op te halen.
142.	Koppelingen worden technisch uitgevoerd volgens (inter)nationale standaarden: • REST (REpresentational State Transfer) • JSON (JavaScript Object Notation) • W3C webservices (SOAP/XML) • StUF ZGW en BG etc
143.	De gegevens of informatie moet een via beveiligde verbindingen worden uitgewisseld tussen de applicaties en tussen eindgebruiker en applicatie volgens meest recente richtlijnen van NCSC.