

Programma van Eisen en Wensen

Multichannel oplossing (Bijlage D)

1. GENERIEKE EISEN EN WENSEN

Dit Programma van Eisen en Wensen bestaat uit de eisen en wensen waaraan u dient te voldoen tijdens de uitvoering van de overeenkomst.

A	Algemeen		Akkoord Ja/Nee
A1	Dienstverlening		
A1.1	De inschrijver biedt een servicedesk die fungeert als single point of contact voor alle 2e lijns supportvragen en incidentmeldingen vanuit de BsGW. Functioneel beheerders en de Helpdesk van BsGW vormen het eerst aanspreekpunt voor de gebruikers (eerste lijn.)	Eis	
A1.2	Ook op het gebied van servicemanagement biedt de inschrijver een single point of contact voor de servicemanager van BsGW. Escalaties lopen ook via dit contact.	Eis	
A1.3	De inschrijver garandeert dat deze beschikt over een flexibele organisatie, waarbij de geboden oplossing ook ten tijde van sterke afwijkingen ten opzichte van geprognostiseerd telefoonverkeer technisch nog steeds bereikbaar is.	Eis	
A1.4	In lijn met item A1.3 is de inschrijver verantwoordelijk voor het treffen van alle benodigde voorbereidingen ten behoeve van de afhandeling van in volume sterk fluctuerend inkomend en/of uitgaand telefoonverkeer.	Eis	
A1.5	De inschrijver voorziet in een telefonische helpdesk voor het melden van incidenten tijdens kantooruren tussen 08:30 en 17:30 uur. De helpdesk heeft één vast telefoonnummer.	Eis	
A1.6	De helpdesk is via email of servicedesk oplossing 24/7 bereikbaar.	Eis	

Programma van Eisen en Wensen

A1.7	Servicedeskmedewerkers communiceren in de Nederlandse taal en zijn vloeiend in woord en geschrift, minimaal op niveau C11 (CEFR(common European Framework of Reference))	Eis	
A1.8	Updates en onderhoud aan systemen vinden plaats buiten de kantoor tijden van BsGW.	Eis	
A1.9	De agent heeft intern en extern (thuiswerken) de beschikking over dezelfde functionaliteiten.	Eis	
A2	Financiële eisen		
A2.1	De inschrijver stuurt facturen naar één factuuradres: Belastingssamenwerking Gemeenten en Waterschappen T.a.v. afdeling Finance Kerkeveldlaan 2 Postbus 1275 6042 KG Roermond finance@bsgw.nl	Eis	
A2.2	De inschrijver vermeldt op facturen minimaal de navolgende onderdelen: - Betreffende afdeling; - Een door de BsGW aan te geven projectnummer en projectomschrijving; - Een door de BsGW aan te geven verplichtingnummer indien van toepassing; - De daadwerkelijk geleverde aantallen en soorten producten of diensten; - Afzonderlijke bedragen, en ook het totaalbedrag; - De datum of periode van levering; - Btw-nummer en bedrag; - KvK-nummer; - Het IBAN/ Bankrekeningnummer van de inschrijver.	Eis	
M	Multichannel oplossing		Akkoord Ja/Nee
M1	Techniek		
M1.1	De geboden oplossing betreft een Software as a service (SaaS) oplossing en voorziet in alle technische benodigheden (SIP trunks, enz.) om alle gevraagde vormen van communicatie (o.a. telefonie, enz.) van en naar BsGW.	Eis	

Programma van Eisen en Wensen

M1.2	Onderhoud en beheer zijn onderdeel van de geboden dienst.	Eis	
M1.3	De applicatie maakt gebruik van Single Sign-on en Azure AD integratie.	Eis	
M1.4	De inschrijver voorziet in een technische architectuurplaat van de oplossing. In deze plaat is onder andere het volgende zichtbaar: - Benodigde poorten; - Richting informatie en datastromen.	Eis	
M1.5	De inschrijver geeft duidelijke aan (schriftelijk dan wel in de bij M1.4 genoemde architectuurplaat), aan welke (applicatie) componenten aan de kant van BsGW dient te voldoen om de oplossing werkende te krijgen.	Eis	
M1.6	De inschrijver garandeert dat de oplossing op alle Windows-werkplekconcepten volledig functioneert (in ieder geval (maar niet gelimiteerd tot) Surface diverse types, HP 470 G8, Assus VivoBook Pro N705F, enz.	Eis	
M1.7	BsGW hanteert Microsoft Edge als standaard browser.	Eis	
M1.8	Er is een beheerportaal beschikbaar waar een beheerder centraal alle klantelingen kan beheren en standaard instellingen kan instellen en beheren.	Eis	
M1.9	De inschrijver is er verantwoordelijk voor dat gesprekken, ontvangen via de door BsGW beschikbaar gestelde 088 en 0800 nummers bij BsGW ontvangen kunnen worden. Met andere woorden de inschrijver voldoet als telefonie provider.	Eis	
M2	Kanalen		
M2.1	De oplossing moet ondersteuning bieden voor diverse communicatiekanalen, waaronder in ieder geval telefoon, e-mail, en live chat. Uitbreiding met sociale media zoals sms en WhatsApp is mogelijk.	Eis	
M2.2	Het is mogelijk prioriteit in te stellen per kanaal en over de kanalen heen.	Eis	
M2.3	Alle klantcontactkanalen zijn met elkaar verbonden en op elkaar afgestemd.	Eis	
M2.4	Het moet mogelijk zijn om klantinteracties naadloos over verschillende kanalen te volgen en te integreren, zodat klanten	Eis	

Programma van Eisen en Wensen

	een consistente ervaring krijgen, ongeacht het kanaal dat ze gebruiken.		
M2.5	De oplossing beschikt over een kennisbank oplossing ter ondersteuning van klanten en agenten. Hierbij kan o.a. worden gezocht met kenwoorden om een passend antwoord te krijgen	Eis	
M2.6	De oplossing bundelt alle tools die dagelijks door het klantcontactcentrum worden gebruikt zoals de planning software, het klanttevredenheidsonderzoek, de rapportagetool en de kennisbank.	Eis	
M2.7	Gesprekken, chats en mails kunnen naar een agent worden gepusht.	Eis	
M2.8	Per klantcontactkanaal kan de nawerktijd centraal worden ingesteld.	Eis	
M2.9	Het moet mogelijk zijn om al deze kanalen te integreren in één gecentraliseerd platform, zodat alle communicatie vanuit één interface kan worden beheerd.	Eis	
M2.10	Per klantcontactkanaal is mogelijk om taken toe te wijzen aan een collega of team	Eis	
M2.11	Per klantcontactkanaal kan gebruik worden gemaakt van (zelf in te richten) templates en standaardantwoorden	Eis	
M2.12	Gesprekken, chats en e-mails kunnen automatisch worden geregistreerd	Eis	
M2.13	Gesprekken, chats en e-mails kunnen handmatig aangevuld worden met behulp van kennisbankitems.	Eis	
M2.14	Er is een spellingcontrole beschikbaar bij alle vormen van schriftelijke communicatie.	Eis	
M2.15	De agent heeft een persoonlijk dashboard van alle klantcontactkanalen beschikbaar met de eigen statistieken en die van de groep.	Eis	
M2.16	Er kunnen per klantcontactkanaal campagnes en teams worden ingesteld.	Eis	
M2.17	Servicelevels voor alle klantcontactkanalen kunnen worden bewaakt.	Eis	
M2.18	Er is een aparte rol voor operationeel beheer (supervisor):	Eis	

Programma van Eisen en Wensen

	- Aanpassen agent status, waaronder: Inlog, bezet, nawerktijd en deactiveren van bel- en berichtgroepen; - Beheren van agenten, zoals het wijzigen, verwijderen van agenten en het aanpassen van profielen zoals, skills, wachtrijen, activiteiten, berichtgroep, enz.; - Aanpassen openingstijden, feestdagen en overige data; - Toevoegen en verwijderen van statuscodes.		
M2.19	De supervisor kan verder: - Zonder tussenkomst van een functioneel beheerder de calamiteiten tekst per wachtrij activeren en deactiveren; - Zonder tussenkomst van een functioneel beheerder de calamiteiten tekst wijzigen; - Heeft de beschikking over een bibliotheek van meldteksten; - Meldteksten kunnen snel worden samengesteld via tekst to speech.	Eis	
M2K1	Kanaal Telefonie		
M2K1.1	De oplossing moet self-servicefunctionaliteit bieden, zoals IVR (Interactive Voice Response) om klanten in staat te stellen eenvoudige taken zelfstandig uit te voeren.	Eis	
M2K1.2	Een telefonisch klantcontactkanaal kan, naar keuze van de aanbestedende dienst, bestaan uit één of meer van de onderstaande mogelijkheden: - Gesproken tekstmeldingen zoals; - o Welkomsttekst, - o Calamiteitentekst, - o Sluitingstekst (algemeen/feestdagen), - o Wachtrijteksten, - o Mededelingen, zoals opname van een gesprek; - Eén of meerdere IVR; - Eén of meerdere wachtrijen; - Eén of meerdere gespreksrouteringen; - Eén of meerdere gespreksverdelingen; - Mogelijkheid om naam/telefoonnummer in te spreken bij een wachtrij langer dan X minuten.	Eis	
M2K1.3	Een telefonisch klantcontactkanaal kan bereikbaar zijn via meerdere telefoonnummers, deze nummers kunnen dezelfde of andere call flows volgen.	Eis	

Programma van Eisen en Wensen

M2K1.4	De wachtrij kan voorzien in tenminste onderstaande mogelijkheden: - Algemene wachttekst; - Tekst over de positie in de wachtrij; - Wachtmuziek.	Eis	
M2K1.5	De gespreksrouting is per klantcontactkanaal ten minste mogelijk op basis van: - Datum, feestdagen, dag en tijd; - Keuze van de beller met IVR-keuze; - Prioriteit; - Skills/vaardigheden van de KCC-agenten; - Telefoonnummer van de beller; - Beschikbaarheid medewerker.	Eis	
M2K1.6	De verdeling van gesprekken is ten minste mogelijk op basis van: - Longest idle; - Round robin; - Vaste volgorde.	Eis	
M2K1.7	Per lijn kunnen servicelevels ingesteld worden.	Eis	
M2K1.8	Als een agent een call mist gaat de klant door naar de eerstvolgende beschikbare agent, de duur voordat de call naar de volgende agent wordt doorgezet is per klantcontactkanaal in te stellen.	Eis	
M2K1.9	De KCC-applicatie beschikt over voicelogging voor het opnemen van (alle) telefoongesprekken voor kwaliteitsmonitoring en agressie preventie. Dit is per klantcontactkanaal in te schakelen. Indien ingeschakeld wordt de klant hier automatisch over geïnformeerd. Alle opnamen worden automatisch van het telefonieplatform verwijderd o.b.v. een door de aanbestedende partij in te stellen bewaartermijn. De opgenomen gesprekken moeten terug te zoeken zijn op agent, datum/tijd en telefoonnummer klant en eenvoudig te beluisteren.	Eis	
M2K1.10	De opname moet kunnen worden gestopt of direct na het gesprek kunnen worden verwijderd door de supervisor als de beller daarom verzoekt.	Eis	

M2K1.11	Bewaarde gesprekken, chats en e-mails kunnen worden geanonimiseerd ten behoeve van trainingsdoeleinden	Eis	
M2K1.12	Vaardigheden Call Agenten kunnen individueel en/of per groep gebruikersgroep worden ingesteld	Eis	
M2K1.13	Voor een Call Agent zijn minimaal de volgende functionaliteiten beschikbaar: - Met een dial pad en click to dial in- en extern bellen; - De microfoon gedurende de interactie aan/uit (mute) te schakelen; - Ruggenspraak en wachtstand, de beller krijgt in dat geval een wachtoon of wachtmelodie te horen. Aanbestedende dienst bepaalt of er een wachtoon of wachtmuziek wordt afgespeeld; - Na ruggenspraak heeft de agent de mogelijkheid het gesprek door te verbinden of te hervatten. - Gesprekken doorverbinden naar een andere bestemming (in- en extern, dit met aankondiging (warm) en koude overdracht; - Wachtwoorden kunnen door gebruikers zelf worden gewijzigd of hersteld - Op eenvoudige wijze de attentie en ondersteuning van de supervisor vragen; - Krijgt informatie over de beller voorafgaand aan het gesprek; - Gesprekken intern kunnen doorverbinden op naam, huntgroep of telefoonnummer.	Eis	
M2K1.14	De agent kan extern bellen met als Caller ID c.q. Calling Line Identification (CLI), naar keuze het telefoonnummer van de klantcontactkanalen, het persoonlijke nummer of anoniem.	Eis	
M2K1.15	Wachtrij functionaliteit: - Een agent kan in meerdere wachtrijen tegelijkertijd deelnemen. De keuze wordt vanuit een supervisor rol gemaakt; - De agent kan gedurende nawerktijd zijn beschikbaarheidsstatus eenvoudig veranderen in beschikbaar of bezet, - Informatie over de menukeuze die de beller heeft gemaakt.	Eis	

Programma van Eisen en Wensen

M2K1.16	Medewerkers kunnen met elkaar meeluisteren i.v.m. inwerken en coaching.	Eis	
M2K2	Kanaal Chat		
M2K2.1	Chatberichten en e-mails zijn opgemaakt in de huisstijl van BsGW	Eis	
M2K2.2	De chatwidget kan worden opgemaakt in de huisstijl.	Eis	
M2K2.3	De live chat is beschikbaar op basis van openingstijden én beschikbaarheid van agenten	Eis	
M2K2.4	Beschikt over de mogelijkheid om gebruik te maken van chatbots.	Eis	
M2K2.5	De oplossing biedt een chat functionaliteit die beschikbaar kan worden gesteld via de website van BsGW (www.bsgw.nl).	Eis	
M2K2.6	De oplossing biedt een chat functionaliteit die beschikbaar kan worden gesteld via Mijn_BsGW. Mijn_BsGW betreft een klant specifieke omgeving waarin persoonsgebonden gegevens worden getoond. Om gebruik te kunnen maken van deze chatoplossing dienen klanten eerst in te loggen via DigiD of eHerkenning op Mijn_BsGW.	Eis	
M2K2.7	Chats worden bewaard.	Eis	
M2K2.8	De bewaartermijn is eenvoudig in te stellen	Eis	
M2K2.9	Er kunnen templates en standaardantwoorden worden ingericht.	Eis	
M2K2.10	Er kunnen meerdere chats tegelijkertijd gevoerd worden door een agent.	Eis	
M2K3	Kanaal Mail		
M2K3.1	We kunnen vragen van klanten per e-mail beantwoorden. Klanten sturen ons een mail via Mijn BsGW op tijden dat de chat niet bemenst is of omdat ze dit kanaal prefereren.	Eis	
M2K3.2	De bewaartermijn is eenvoudig in te stellen.	Eis	
M2K3.3	Er kunnen templates en standaardantwoorden worden ingericht.	Eis	
M2K3.4	E-mails kunnen via een formulier op de website en/of Mijn BsGW worden gestuurd.	Eis	
M2K3.5	Er kan een bijlage worden toegevoegd.	Eis	
M3	Integratie met bestaande systemen		

Programma van Eisen en Wensen

M3.1	De oplossing moet kunnen integreren met bestaande systemen binnen de organisatie, zoals onze belastingapplicatie Gouw IT, website BsGW en Kennisbank van Polly.	Eis	
M3.2	Middels een koppeling, bij voorkeur API, kan interactie plaatsvinden met de belasting applicatie van Gouw IT.	Eis	
M3.3	Het moet mogelijk zijn om klantgegevens via de klantkaart vanuit de belastingapplicatie te tonen op het moment dat een agent een beller krijgt aangeboden.	Eis	
M3.4	Het platform verzamelt alle klantgegevens (realtime) en combineert deze in een klantprofiel. Agenten beschikken, ongeacht het kanaal dat de klant gebruikt, over alle informatie die ze nodig hebben over de klant.	Eis	
M3.5	BsGW maakt veelal gebruik van derde partijen die als een dienst extra agenten beschikbaar stellen. Deze partijen werken vaak met hun eigen oplossingen. BsGW wil zo geruisloos mogelijk samen kunnen werken met dergelijke partijen, doormiddel van een eenvoudige interactie tussen beide oplossingen.	Eis	
M4	Schaalbaarheid en flexibiliteit		
M4.1	De oplossing moet schaalbaar zijn en kunnen meegroeien met de behoeften van de organisatie, zowel in termen van het aantal gebruikers als het aantal ondersteunde contactkanalen.	Eis	
M4.2	Bij BsGW is er sprake van piekperiodes, waarbij het aantal binnenkomende gesprekken kan oplopen tot 2.000 per dag. Gedurende deze periode dient het aantal beschikbare lijnen eenvoudig schaalbaar te zijn.	Eis	
M4.3	Het systeem moet uitgebreide configuratieopties bieden, zodat workflows, processen en gebruikersrechten kunnen worden aangepast aan de specifieke vereisten van de organisatie.	Eis	
M4.4	Het systeem moet modulair zijn opgebouwd, zodat functionaliteit kan worden toegevoegd of verwijderd op basis van de specifieke behoeften van de organisatie.	Eis	
M5	Real-time monitoring en rapportage	Eis	
M5.1	De oplossing moet voorzien zijn van uitgebreide mogelijkheden voor real-time monitoring van communicatiekanalen en prestaties van agenten.	Eis	

M5.2	Via dashboards/wallboards zijn wordt o.a. de volgende realtime informatie getoond: - Wachtrij lengte; - Gemiddelde wachttijden; - Wachtijd; - Agent statussen (aantal beschikbaar, in gesprek, nawerk); - Gesplitst naar inkomend en uitgaande gesprekken; - Gespreksduur; - Service Level; - Aantal gesprekken; - Aantal verbroken gesprekken.	Eis	
M5.3	Het moet gedetailleerde rapportagefunctionaliteit bieden om inzicht te geven in de prestaties, productiviteit en klanttevredenheid van het KCC. Onder andere onderstaande is opgenomen in de standaard rapportages: - First call resolution; - Gemiddelde wachttijd; - Servicelevel; - Percentage bellers dat de wachtrij verlaat tijdens het wachten; - Percentage bellers dat de bezettoon te horen krijgt en hierdoor wordt geblokkeerd; - Gemiddelde gesprekstijd; - Gemiddelde afhandeltijd; - Gemiddelde nawerktijd; - Gedetailleerde agent-rapportage; - Er is een gedetailleerde supervisor-rapportage, enz.	Eis	
M5.4	Het wallboard moet de informatie van meerdere klantengangen (tot max. 4) kunnen tonen.	Eis	
M5.5	Managementinformatie: - De supervisor-rol heeft de beschikking over minimaal 10 rapportage sjablonen over de klantengang (agent view, beschikbaarheid, gemiste en afgehandelde oproepen); - De supervisor kan rapportages opstellen op basis van beschikbare parameters en/of filters; - Standaardrapportages moeten ad hoc, in batch automatisch en periodiek kunnen worden gegenereerd. - Het moet mogelijk te zijn om automatisch aan het begin van elke werkdag, werkweek, en werkmaand een dag-/	Eis	

	week-/ maandrapport te genereren van de vorige periode. - Gegevens en rapportages moeten geëxporteerd kunnen worden en leesbaar voor medewerkers. Het bestandsformaat moet gangbaar zijn (minimaal *.odf, *.xlsx en *.csv); - Gegevens van in- en uitgaande gesprekken moeten apart zichtbaar zijn per klantingang. Dit zijn o.a.: - o Welk nummer belt; - o Welke agent neemt op; - o De menukeuze van de beller; - o Tijdstip en datum gesprek. - o Wachtijd voordat de klant iemand aan de telefoon heeft - o De gespreksduur - o Opnieuw in de wachtrij; - De applicatie moet de servicegraad uit kunnen rekenen van elk van de ingangen op basis van real-time en historische gegevens. (De parameters hiervoor moeten per klant-ingang instelbaar zijn.) Dit op ieder moment ten behoeve van de dashboard informatie.		
M5.6	Kwaliteit monitoren: - De supervisor kan op elk gewenst moment vanaf zijn werkplek meeluisteren met een agent. Voor de beller of de agent is dit niet merkbaar. - De supervisor moet in het kader van gespreksopname en coaching, de gesprekken van elke individuele agent kunnen opnemen en terugluisteren op haar/zijn eigen werkplek. - De opgenomen gesprekken moeten door de supervisor opgeslagen kunnen worden op een door de aanbestedende dienst te bepalen plek in haar netwerk in reguliere bestandsstandaarden zoals .WAV en .mp3. - De opnamen kunnen door supervisor en beheerder eenvoudig worden teruggezocht op agent, datum, tijd, lengte van gesprekken, beller en eventuele caller ID's. - Het afluisteren van opgenomen gesprekken kan alleen door daarvoor geautoriseerde personen.	Eis	
M5.7	Agenten hebben inzicht in eigen prestaties op het gebied van kwaliteit en kwantiteit.	Eis	

Programma van Eisen en Wensen

M5.8	De kwaliteit van gesprekken, chats en email kan worden gemonitord en gemeten.	Eis	
M6	Gebruiksvriendelijkheid en training		
M6.1	De inschrijver levert een opleiding voor de supervisor. Lever een specificatie van de onderwerpen van de opleiding.	Eis	
M6.2	De oplossing moet intuïtief en gebruiksvriendelijk zijn, zowel voor agenten als voor beheerders.	Eis	
M6.3	Het moet training en ondersteuning bieden om agenten snel vertrouwd te maken met het systeem en effectief te laten werken.	Eis	
M7	Prijs en licentiemodel		
M7.1	Het licentiemodel moet transparant en schaalbaar zijn en geen verborgen kosten bevatten.	Eis	
M7.2	Alle mogelijk te berekenen kosten, inclusief doorschakel kosten zijn opgenomen in het prijzenblad.	Eis	
M7.3	Het licentiemodel is op basis active named users. Dit betekent dat alleen wordt gefactureerd over het totale aantal unieke ingelogde gebruikers over een bepaalde periode.	Eis	
M7.4	Het systeem moet flexibele licentieopties/modules bieden, zodat organisaties alleen betalen voor wat ze gebruiken en kunnen opschalen naarmate hun behoeften groeien.	Eis	
M7.5	In het prijzenblad wordt naast de totaalprijs van de oplossing de prijs per individuele module benoemd.	Eis	
M8	Informatiebeveiliging en Privacy		
M8.1	De oplossing moet voldoen aan alle relevante beveiligingsnormen en -voorschriften, zoals GDPR (AVG) en de archiefwet.	Eis	
M8.2	Het moet beveiligingsfuncties bieden, zoals encryptie van gegevens, role-based access control en audit trails.	Eis	
M8.3	De inschrijver is ISO-27001/2 gecertificeerd, of gelijkwaardig.	Eis	
M8.4	Aanpassingen als gevolg van wijzigingen in relevante wet- en regelgeving dienen op de ingangsdatum te zijn doorgevoerd en werkend opgeleverd.	Eis	

Programma van Eisen en Wensen

M8.5	De oplossing beschikt over een niet muteerbare audit trail om van elk van onderstaande handelingen te registreren door wie de handeling op welk moment werd uitgevoerd: - Raadplegen; - Creëren/Toevoegen; - Wijzigen/Verwijderen; - Archiveren/Vernietigen/Overdragen.	Eis	
M8.6	Alle gegevens zijn en blijven te allen tijde eigendom van de Opdrachtgever, zijn ten alle tijden toegankelijk en mogen door de Inschrijver niet voor andere doeleinden worden gebruikt of ter beschikking worden gesteld.	Eis	
M8I1	Informatiebeveiliging algemeen		
M8I1.1	De oplossing moet voldoen aan alle relevante beveiligingsnormen en -voorschriften, zoals GDPR (AVG) en de archiefwet.	Eis	
M8I1.2	Het moet beveiligingsfuncties bieden, zoals encryptie van gegevens, role-based access control en audit trails.	Eis	
M8I1.3	De inschrijver is ISO-27001/2 gecertificeerd, of gelijkwaardig.	Eis	
M8I1.4	Aanpassingen als gevolg van wijzigingen in relevante wet- en regelgeving dienen op de ingangsdatum te zijn doorgevoerd en werkend opgeleverd.	Eis	
M8I1.5	De oplossing beschikt over een niet muteerbare audit trail om van elk van onderstaande handelingen te registreren door wie de handeling op welk moment werd uitgevoerd: - Raadplegen; - Creëren/Toevoegen; - Wijzigen/Verwijderen; Archiveren/Vernietigen/Overdragen.	Eis	
M8I1.6	Alle gegevens zijn en blijven te allen tijde eigendom van de Opdrachtgever, zijn ten alle tijden toegankelijk en mogen door de Inschrijver niet voor andere doeleinden worden gebruikt of ter beschikking worden gesteld.	Eis	
M8I1.7	Informatiebeveiligingseisen worden onderdeel van het contract.	Eis	
M8I1.8	In de overeenkomst tussen Opdrachtnemer en Opdrachtgever behoort een exit strategie te zijn opgenomen waarbij zowel een aantal bepalingen over exit zijn opgenomen, als een aantal condities die aanleiding kunnen geven tot een exit.	Eis	

Programma van Eisen en Wensen

M8I1.9	Opdrachtnemer moet een beveiligingsorganisatie gedefinieerd hebben waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden (TVB) van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.	Eis	
M8I2	Informatiebeveiliging software		
M8I2.1	De noodzakelijke bedrijfs- en beveiligingsfuncties binnen het veranderingsgebied behoren te worden vastgesteld met organisatorische en technisch uitgangspunten.	Eis	
M8I2.2	Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.	Eis	
M8I2.3	De leverancier behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven.	Eis	
M8I2.4	Het softwarepakket behoort mechanismen te bevatten voor normalisatie en validatie van invoer en voor schoning van de uitvoer.	Eis	
M8I2.5	Sessies behoren authentiek te zijn voor elke gebruiker en behoren ongeldig gemaakt te worden na een time-out of perioden van inactiviteit.	Eis	
M8I2.6	Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.	Eis	
M8I2.7	Het softwarepakket past versleuteling toe op de communicatie van gegevens die passend bij het classificatieniveau is van de gegevens en controleert hierop.	Eis	
M8I2.8	Softwarepakketten behoren de identiteiten van gebruikers vast te stellen met een mechanisme voor identificatie en authenticatie.	Eis	
M8I2.9	Het softwarepakket behoort een autorisatiemechanisme te bieden.	Eis	
M8I2.10	De rechten die gebruikers hebben binnen een softwarepakket (inclusief beheerders) zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.	Eis	

Programma van Eisen en Wensen

M8I2.11	Het softwarepakket biedt signaleringsfuncties voor registratie en detectie die beveiligd zijn ingericht.	Eis	
M8I2.12	Softwarepakketten behoren veilige API's te gebruiken voor import en export van gegevens.	Eis	
M8I2.13	Softwarepakketten behoren mechanismen te bieden om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.	Eis	
M8I3	Informatiebeveiliging Clouddiensten		
M8I3.1	De CSP voorziet de CSC in een systeembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.	Eis	
M8I3.2	IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC.	Eis	
M8I3.3	De CSP behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labels, eigenaarschap en locatie.	Eis	
M8I3.4	De CSP heeft een actuele architectuur vastgelegd die voorziet in een raamwerk voor de onderlinge samenhang en afhankelijkheden van de IT-functionaliteiten.	Eis	
M8I3.5	Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.	Eis	
M8I3.6	De herstelfunctie van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.	Eis	
M8I3.7	Data ('op transport', 'in verwerking' en 'in rust') met de classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.	Eis	
M8I3.8	Gearchiveerde data behoren gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van de CSC/data-eigenaar te kunnen worden vernietigd.	Eis	

Programma van Eisen en Wensen

M8I3.9	CSC-gegevens behoren tijdens transport, bewerking en opslag duurzaam geïsoleerd te zijn van beheerfuncties en data van en andere dienstverlening aan andere CSC's, die de CSP in beheer heeft.	Eis	
M8I3.10	De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden.	Eis	
M8I3.11	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.	Eis	
M8I3.12	Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.	Eis	
M8I3.13	Gevoelige data van CSC's behoort conform het overeengekomen beleid inzake cryptografische maatregelen tijdens transport via netwerken en bij opslag bij CSP te zijn versleuteld	Eis	
M8I3.14	De onderlinge netwerkconnecties (koppelvlakken) in de keten van de CSC naar de CSP behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken.	Eis	
M8I3.15	Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende IT-platforms en kunnen met standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (portabiliteit) naar andere CSP's.	Eis	
M8I3.16	Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Eis	
M8I3.17	Bij multi-tenancy wordt de CSC-data binnen clouddiensten, die door meerdere CSC's worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines	Eis	
M8I4	Informatiebeveiliging Toegangsbeveiliging		
M8I4.1	Ter bescherming van authenticatie-informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	Eis	
M8I4.2	Een formele registratie- en afmeldprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Eis	

Programma van Eisen en Wensen

M8I4.3	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle type gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Eis	
M8I4.4	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Eis	
M8I4.5	Een formeel autorisatieproces dient geïmplementeerd te zijn voor het beheersen van de toegangsrechten van alle medewerkers en externe gebruikers tot informatie en informatieverwerkende faciliteiten.	Eis	
M8I4.6	Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Eis	
M8I4.7	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Eis	
M8I4.8	Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbeleid.	Eis	
M8I4.9	Ter ondersteuning van autorisatiebeheer moeten binnen de daartoe in aanmerking komende applicaties technische autorisatievoorzieningen, zoals: een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten, beschikbaar zijn.	Eis	
M8I4.10	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Eis	
M8I5	Informatiebeveiliging communicatie		
M8I5.1	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Eis	
M8I5.2	Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen 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.	Eis	
M8I5.3	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).	Eis	

Programma van Eisen en Wensen

M8I5.4	Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	Eis	
M8I5.5	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.	Eis	
M8I5.6	De filterfuncties van gateways en firewalls behoren zo te zijn geconfigureerd, dat inkomend en uitgaand netwerkverkeer wordt gecontroleerd en dat daarbij in alle richtingen uitsluitend het vanuit beveiligingsbeleid toegestaan netwerkverkeer wordt doorgelaten.	Eis	
M8I5.7	Een VPN behoort een strikt gescheiden end-to-end-connectie te geven, waarbij de getransporteerde informatie die over een VPN wordt getransporteerd, is ingeperkt tot de organisatie die de VPN gebruikt.	Eis	
M8I5.8	Ter bescherming van de vertrouwelijkheid en integriteit van de getransporteerde informatie behoren passende cryptografische beheersmaatregelen te worden ontwikkeld, geïmplementeerd en ingezet.	Eis	
M8I5.9	Draadloos verkeer behoort te worden beveiligd met authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.	Eis	
M8I5.10	Authenticatie van netwerk-nodes behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.	Eis	
M8I5.11	Logbestanden van informatiebeveiligingsgebeurtenissen in netwerken, behoren te worden gemaakt en bewaard en regelmatig te worden beoordeeld (op de ernst van de risico's).	Eis	
M8I5.12	De beveiligingsarchitectuur behoort de samenhang van het netwerk te beschrijven en structuur te bieden in de beveiligingsmaatregelen, gebaseerd op het vigerende bedrijfsbeleid, de leidende principes en de geldende normen en standaarden.	Eis	
M8I6	Informatiebeveiliging BIO		
M8I6.1	Cryptografische toepassingen voldoen aan passende standaarden.	Eis	
M8I6.2	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De	Eis	

Programma van Eisen en Wensen

	risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.		
M8I6.3	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt/ geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Eis	
M8I6.4	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	Eis	
M8I6.5	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Eis	
M8I6.6	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Eis	
M8I6.7	Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de pastoe-of-leg-uit lijst, gebruik gemaakt van de actuele versie van Digikoppeling.	Eis	
M8I6.8	Maak gebruik van PKI overheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontleen.	Eis	
M8I6.9	Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	Eis	
M8I6.10	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te	Eis	

	beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.		
M8I6.11	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	Eis	
M8I6.12	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Eis	
M8I6.13	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Eis	
M8I6.14	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Eis	
M8I6.15	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Eis	
M8I6.16	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	Eis	
M8I6.17	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).	Eis	
M8I6.18	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Eis	
M8I6.19	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	Eis	

M8I6.20	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	Eis	
M8I6.21	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	Eis	
M8I6.22	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Eis	
M8I6.23	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Eis	
M8I6.24	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	Eis	
M8I6.25	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	Eis	
M8I6.26	Ingeval van PKI overheid-certificaten: hanteer de PKI overheid-eisen ten aanzien van het sleutelbeheer. In overige situaties: hanteer de standaard ISO 11770 voor het beheer van cryptografische sleutels.	Eis	
M8I6.27	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	Eis	
M8I6.28	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt/ geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Eis	
M8I6.29	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	Eis	

M8I6.30	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Eis	
M8I6.31	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld	Eis	
M8I6.32	Het back-upproces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	Eis	
M8I6.33	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	Eis	
M8I6.34	Opdrachtnemer garandeert een maximale downtime van 16 uur (2 werkdagen) in alle voorkomende gevallen (RTO = 16 uur). Dit betreft de maximaal acceptabele downtime in geval van een calamiteit.	Eis	
M8I6.35	Opdrachtnemer garandeert een maximaal data verlies van 8 uur (1 werkdag) in alle voorkomende gevallen (RPO = 8 uur). Dit betreft het maximaal acceptabele data verlies in geval van een calamiteit.	Eis	
M8P1	Informatiebeveiliging Privacy supplement		
M8P1.1	Opdrachtnemer heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereid, een actuele VOG, een actuele verklaring omtrent het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht.	Eis	
M8P1.2	De applicatie biedt de mogelijkheid om op aangeven van betrokkene, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen.	Eis	
M8P1.3	Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.	Eis	

Programma van Eisen en Wensen

M8P1.4	De applicatie behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	Eis	
M8P1.5	De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.	Eis	
M8P1.6	Iedere applicatie kent een duidelijk verwerkingsdoel, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de applicatie, de transportpaden, de middleware, de opslagvoorzieningen en is hierop getoetst.	Eis	
M8P1.7	Een applicatie, en iedere Functie binnen deze applicatie, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere doorgifte, verwerking door de applicatie en verwerking binnen een functie alleen de daarvoor noodzakelijke persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de opslagvoorzieningen, de transportpaden en de middleware. Het implementatiemodel is getoetst.	Eis	
M8P1.8	De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.	Eis	
M8P1.9	De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruikt wordt, waarbij het verbergen van verwerkingen het uitgangspunt is.	Eis	
M8P1.10	De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	Eis	
M8P1.11	Het doel van de verwerking van persoonsgegevens en van de toegang zijn welbepaald, gerechtvaardigd en uitdrukkelijk omschreven, waarbij de toegang naar keuze rol gebaseerd en waar nodig taak gebaseerd wordt verstrekt. Aanvullend vindt logging en monitoring plaats.	Eis	

Programma van Eisen en Wensen

M8P1.12	De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.	Eis	
M8P1.13	Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.	Eis	
M8P1.14	De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.	Eis	
M8P1.15	De organisatie behoort fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, op passende wijze ingericht te hebben, zodat enkel medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt geregistreerd.	Eis	
M8P1.16	De applicatie behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	Eis	
M8P1.17	De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.	Eis	
M8P1.18	De organisatie behoort een proces te hebben ingericht en afspraken te hanteren, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruiken, waarbij enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt en verwijdering van persoonsgegevens mogelijk is.	Eis	
M8P1.19	De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.	Eis	
M8P1.20	De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de	Eis	

Programma van Eisen en Wensen

	instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.		
M8P1.21	De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	Eis	
B	Beschikbaarheid		Akkoord Ja/Nee
B1	Beschikbaarheid en betrouwbaarheid		
B1.1	De oplossing moet een hoge beschikbaarheid en betrouwbaarheid bieden om continuïteit van de dienstverlening te waarborgen.	Eis	
B1.2	Het moet redundante systemen en failover-mogelijkheden bieden om downtime te minimaliseren.	Eis	
B1.3	De oplossing beschikt over voldoende lijnen om aan de vraag tijdens de piekperiodes te kunnen voldoen.	Eis	
W	Wensen		Akkoord Ja/Nee
W1	De inzet van AI biedt de mogelijkheid om de klantervaring te verbeteren.	Wens	
W2	Geregistreerde contacten kunnen met de belastingapplicatie worden uitgewisseld. Contacten kunnen bijvoorbeeld ingelezen worden in de contactregistratie van de belastingapplicatie. Bij voorkeur via een rechtstreekse koppeling zoals bijvoorbeeld API.	Wens	
W3	Het is mogelijk geregistreerde contacten te exporteren naar diverse standaardformaten, zoals bijvoorbeeld .xlsx, .csv, enz.	Wens	
W4	Het is in de toekomst mogelijk om historische kenmerken van het laatste gesprek, laatst geselecteerde agent en CLIP in te zetten t.b.v. data- en trendanalyse.	Wens	
W5	BsGW maakt op dit moment gebruik van de Kennisbank van Polly. Deze kennisbank wordt gebruikt door de agenten van BsGW, maar ook de belastingplichtigen/klanten van BsGW. Dit laatste kan middels de integratie van de Polly kennisbank in de website van BsGW (www.bsgw.nl). Indien de oplossingen een over een kennis bank beschikt die we in de huidige website naadloos kunnen integreren, zou dat zeer wenselijk zijn.	Wens	