Bijlage B – Programma van eisen

De in dit Programma van Eisen opgenomen eisen betreffen minimumeisen waaraan de inschrijving volledig moet voldoen. Indien een inschrijving niet voldoet aan één of meer van deze minimumeisen, is de inschrijving ongeldig en komt deze niet in aanmerking voor verdere beoordeling.

Contactcenter	
Eis 1	*Omnichannel klantcontact* De oplossing ondersteunt het afhandelen van klantcontact via telefonie, chat en e-mail binnen één centrale applicatie.
Eis 2	*Toekomstige communicatiekanalen* De oplossing maakt het mogelijk om in de toekomst aanvullende communicatiekanalen toe te voegen, eventueel modulair, zoals chat, WhatsApp en sociale media.
Eis 3	*Keuzemenu (IVR)* De oplossing ondersteunt een keuzemenu (IVR) waarbij routering mogelijk is op basis van de toetsen 0 t/m 9, * en #. Daarbij moet routering mogelijk zijn naar: • een volgend keuzemenu; • een meldtekst; • een vooraf ingestelde routering; • een wachtrij. Daarnaast geldt het volgende: • de timeout van een keuzemenu moet instelbaar zijn tussen 5 en 10 seconden; • na een timeout moet het mogelijk zijn om het keuzemenu te herhalen, een vooraf ingestelde routering te volgen of een beller in een wachtrij te plaatsen; • bellers moeten meerdere keuzes achter elkaar kunnen invoeren zonder meldteksten volledig te hoeven beluisteren.
Eis 4	*Meldteksten* De oplossing ondersteunt het afspelen van meldteksten aan bellers, zowel voorafgaand aan plaatsing in een wachtrij als tijdens het wachten in de wachtrij.
Eis 5	*Tijdelijke meldteksten* De oplossing maakt het mogelijk om tijdelijk aanvullende meldteksten toe te voegen voorafgaand aan plaatsing in een wachtrij.
Eis 6	*Beheer meldteksten* BVO NL moet zelfstandig en ad hoc meldteksten kunnen aanmaken, wijzigen, activeren en deactiveren.
Eis 7	*Autorisaties meldteksten* Het beheer van meldteksten moet beveiligd kunnen worden ingericht, zodat uitsluitend geautoriseerde personen wijzigingen kunnen doorvoeren.
Eis 8	*Text-to-speech* De oplossing ondersteunt minimaal het genereren van meldteksten via text-to-speech (TTS).

	Toelichting Het moet tevens mogelijk zijn om eigen audiobestanden toe te voegen zodat ook gebruik kan worden gemaakt van een stemacteur.
Eis 9	*Wachtrij & wachttijd* De oplossing informeert bellers tijdens het wachten over hun positie in de wachtrij en de verwachte wachttijd. *Toelichting* We verkiezen de geschatte wachttijd informatie voor de beller boven informatie over de wachtrij.
Eis 10	*Wachtrij* De oplossing speelt tijdens het wachten een bevestigingstoon af in plaats van wachtmuziek. *Toelichting* Wij kiezen ervoor om geen wachtmuziek aan te bieden.
Eis 11	*Mail- en gespreksroutering* De oplossing moet routering van telefonie en e-mail ondersteunen op basis van ingestelde routeringsregels en realtime beschikbaarheid van CS-medewerkers. *Toelichting* Daarbij moet routering onder andere mogelijk zijn op basis van: • beschikbaarheid van CS-medewerkers binnen een skill; • expertise of vaardigheden van CS-medewerkers; • aantal contacten in de wachtrij; • wachttijd van het langst wachtende contact; • tijdstip, dag van de week en datum; • ingestelde servicelevels; • vooraf ingestelde routeringsscenario's of prioriteiten.
Eis 12	*Routering op basis van kanaal* De oplossing ondersteunt routering naar specifieke CS-medewerkers op basis van kanaal, waaronder minimaal telefonie, e-mail en chat.
Eis 13	*Skill based routing* De oplossing ondersteunt routering op basis van toegekende specialisaties en vaardigheden van medewerkers, zodat interacties gericht kunnen worden toegewezen aan medewerkers met specifieke expertise.
Eis 14	*Routeringsmethoden* De oplossing ondersteunt verdeling van gesprekken op basis van verschillende routeringsmethoden, waaronder minimaal: • longest idle; • meest beschikbare medewerker.
Eis 15	*Beschikbaarheidsstatus* Medewerkers moeten binnen de oplossing afwijkende beschikbaarheidsstatussen kunnen instellen, zoals 'Vraagbaak', 'Intern beschikbaar' en 'Pauze'.

Eis 16	*Beschikbaarheidsstatus* Medewerkers moeten zich tijdelijk op niet-beschikbaar kunnen zetten.
Eis 17	*Informatie bij binnenkomende gesprekken* Een agent moet kunnen zien voor welke wachtrij een beller belt, zodat het gesprek voorbereid kan worden aangenomen.
Eis 18	*Nawerktijd* De oplossing ondersteunt nawerktijd voor CS-medewerkers. Daarbij geldt het volgende: • nawerktijd moet vooraf instelbaar zijn; • CS-medewerkers moeten nawerktijd zelf kunnen activeren of verlengen; • nawerktijd moet onderbroken kunnen worden door een andere status te activeren, zoals beschikbaar of pauze.
Eis 19	*Beheer van groepen en vaardigheden* Een senior medewerker of teammanager van BVO NL moet zelfstandig CS-medewerkers kunnen toevoegen aan telefoon- en e-mailgroepen en vaardigheden kunnen beheren, zonder afhankelijkheid van opdrachtnemer.
Eis 20	*Indeling in groepen* Een agent moet in minimaal tien telefoon- en/of e-mailgroepen kunnen worden ingedeeld.
Eis 21	*Afrondingscodes* CS-medewerkers moeten na afronding van een telefoongesprek of e-mailtaak een afrondingscode kunnen registreren ten behoeve van rapportages.
Eis 22	*Uitgaand telefoonnummer en e-mailadres* De oplossing ondersteunt het gebruik van verschillende telefoonnummers en e-mailadressen voor uitgaande communicatie. *Toelichting* Daarbij moet het mogelijk zijn om per uitgaand gesprek of e-mail een specifiek telefoonnummer of e-mailadres mee te sturen.
Eis 23	*Dashboard wachtrijen en prestaties* BVO NL wil beschikken over een dashboard waarop realtime inzicht bestaat in de actuele status van wachtrijen en de prestaties van groepen. Het dashboard moet: • zonder installatie van aanvullende software beschikbaar zijn via pc of laptop; • toegankelijk zijn voor medewerkers, senior medewerkers en teammanagers van de Cliëntservice. Minimaal de volgende gegevens moeten zichtbaar zijn: • aantal medewerkers binnen de groep; • aantal beschikbare medewerkers voor telefonie; • aantal beschikbare medewerkers voor e-mail; • aantal medewerkers in een alternatieve status, zoals pauze of overleg; • aantal medewerkers in gesprek; • servicelevel voor telefonie en e-mail; • aantal contacten in de wachtrij voor telefonie en e-mail; • langst wachtende contact voor telefonie en e-mail;

	• Totaal aantal afgehandelde contacten per tijdseenheid (bijvoorbeeld dag).
Eis 24	*Persoonlijk dashboard* Een agent heeft direct inzicht in statistieken over de eigen werkzaamheden op het gebied van telefonie en e-mail, bijvoorbeeld via een persoonlijk dashboard. Zowel realtime als via een samenvattend dag- of weekrapport.
Eis 25	*Rapportages* De oplossing ondersteunt realtime en historische rapportages ten behoeve van management en sturing. Rapportages moeten beschikbaar zijn op basis van rol gebaseerde autorisaties en minimaal inzicht bieden per: • agent; • groep; • Locatie; • telefoonnummer; • e-mailadres; • totale afdeling; • Bezettingsgraad medewerkers. Historische rapportages moeten beschikbaar zijn per dag, week, maand en jaar en over een zelf te selecteren periode.
Eis 26	*Trend- en historische analyses* De CCaaS-oplossing ondersteunt trend- en historische rapportages, zodat actuele prestaties kunnen worden vergeleken met eerdere perioden. *Toelichting* Historische gegevens moeten minimaal één kalenderjaar beschikbaar blijven.
Eis 27	*Warm doorverbinden* De oplossing ondersteunt warm doorverbinden, waarbij een gesprek met vooraankondiging kan worden doorverbonden naar een telefoongroep binnen de contactcenteromgeving.
Eis 28	*Expertgroepen* De oplossing maakt het mogelijk interacties met voorrang te routeren naar leden van expertgroepen. Daarnaast kunnen medewerkers interacties eenvoudig doorzetten naar andere medewerkers of leden van expertgroepen.
Eis 29	*E-mailsjablonen* De oplossing ondersteunt het gebruik van e-mailsjablonen.
Eis 30	*DTMF-signalen* De CCaaS-oplossing ondersteunt het versturen van DTMF-signalen via de softphone van de gebruiker.
Eis 31	*Meeluisterfunctie* De CCaaS-oplossing beschikt over een meeluisterfunctie voor coachings- en kwaliteitsdoeleinden.

Eis 32	*Speech-to-text* De CCaaS-oplossing ondersteunt automatische speech-to-text transcriptie van gesprekken.
Service	
Eis 33	*Service Level Agreement en Dienst Afspraken Plan* Opdrachtnemer stelt uiterlijk bij implementatie, in afstemming met ons, een Service Level Agreement (SLA) en Dienst Afspraken Plan (DAP) op en houdt deze gedurende de looptijd van de overeenkomst actueel. In de SLA en het DAP worden minimaal afspraken vastgelegd over: • beschikbaarheid van de dienstverlening en de verschillende onderdelen van het communicatieplatform; • classificatie van storingen op basis van impact en urgentie; • reactietijden en functiehersteltijden per prioriteitsniveau; • bereikbaarheid van de servicedesk; • escalatieprocedures en contactpersonen; • preventief, correctief en innovatief onderhoud; • onderhoudsvensters en communicatie over gepland onderhoud; • monitoring van de dienstverlening; • rapportages over prestaties, beschikbaarheid en incidenten; • periodiek overleg over de dienstverlening; • procedures voor wijzigingen, releases en updates; • continuïteit en uitwijkmaatregelen bij verstoringen; • beveiligingsincidenten en meldprocedures; • KPI's, inclusief verplichte service credits, die van toepassing zijn bij het niet behalen van afgesproken serviceniveaus. Onder onderstaande begrippen verstaan wij in ieder geval: • Beschikbaarheid: de periode waarin de dienstverlening operationeel en bruikbaar is voor eindgebruikers, exclusief vooraf aangekondigd onderhoud. • Correctief onderhoud: het opsporen en herstellen van storingen en gebreken. • Functiehersteltijd: de periode tussen melding van een storing en volledig herstel van de functionaliteit. • Innovatief onderhoud: het beschikbaar stellen van nieuwe functionaliteiten, updates en doorontwikkelingen. • Preventief onderhoud: werkzaamheden gericht op het voorkomen van storingen en verstoringen. • Reactietijd: de tijd tussen melding van een storing en de eerste inhoudelijke reactie van Opdrachtnemer. • Servicelevels: de overeengekomen prestatienormen voor de dienstverlening. • Service-uren: de overeengekomen uren waarbinnen support en onderhoud beschikbaar zijn. • Storing: een technisch probleem waardoor de dienstverlening geheel of gedeeltelijk niet beschikbaar is of niet functioneert zoals overeengekomen.
Eis 34	*24/7 monitoring van de dienstverlening* Opdrachtnemer voert 24 uur per dag en 7 dagen per week actieve bewaking en monitoring uit op de beschikbaarheid, prestaties en continuïteit van de geleverde dienstverlening.
Eis 35	*Servicedesk en incidentmeldingen*

	Opdrachtnemer beschikt over een servicedesk die minimaal op Werkdagen bereikbaar is van 08.00 uur tot 17.00 uur voor het telefonisch melden van incidenten, storingen en serviceverzoeken.
Eis 36	*Communicatie bij storingen* Opdrachtnemer informeert ons actief bij storingen in het platform die impact hebben op de dienstverlening en/of bereikbaarheid. Communicatie vindt plaats conform de overeengekomen communicatiematrix en incidentmatrix.
Eis 37	*Hersteltijd kritische incidenten* De maximale hersteltijd voor een kritisch incident bedraagt 2 uur na melding van het incident. Indien het incident wordt veroorzaakt door een onderliggende derde partij of cloudleverancier, blijft Opdrachtnemer verantwoordelijk voor regie, escalatie en communicatie richting ons.
Eis 38	*Hersteltijd niet-kritische incidenten* De maximale hersteltijd voor een niet-kritisch incident bedraagt 8 uur na melding van het incident. *Toelichting* Een incident wordt als kritisch geclassificeerd indien het incident leidt tot ernstige verstoring van de dienstverlening, waaronder in ieder geval de volgende situaties: • alle gebruikers worden geraakt; • de oplossing geheel of gedeeltelijk niet beschikbaar of niet bruikbaar is; • één of meerdere servicenummers of klantingangen van de Cliëntservice niet bereikbaar zijn • Bij sterk verminderde gesprekskwaliteit zoals echo, verbroken gesprekken, waarbij één gesprekspartner de ander niet kan horen.
Eis 39	*Communicatieprocedure bij prio 1 storingen* Opdrachtnemer beschikt over een procedure voor communicatie bij prio 1 storingen, waarbij gedurende de storing Opdrachtnemer ons actief op de hoogte houdt van de voortgang, de impact, de vermoedelijke oorzaak, de getroffen maatregelen en het verwachte moment van herstel.
Eis 40	*Escalatieprocedure bij overschrijding servicelevels* Opdrachtnemer beschikt, als onderdeel van de SLA, over een escalatieprocedure die wordt toegepast bij een dreigende of daadwerkelijke overschrijding van de overeengekomen servicelevels en die minimaal de escalatieniveaus, verantwoordelijkheden, communicatielijnen en te nemen maatregelen beschrijft.
Eis 41	*Kwartaalrapportage dienstverlening* Opdrachtnemer levert per kwartaal een rapportage aan over de kwantitatieve en kwalitatieve dienstverlening. De rapportage bevat minimaal informatie over beschikbaarheid, incidenten, servicelevels, responstijden, hersteltijden, uitgevoerde onderhoudswerkzaamheden, trends, klachten en verbetermaatregelen.
Eis 42	*Beschikbaarheid CCaaS-oplossing* De beschikbaarheid van de CCaaS-oplossing bedraagt minimaal 99,95%, gemeten over een kalendermaand en exclusief vooraf aangekondigd onderhoud binnen het overeengekomen onderhoudsvenster.

Eis 43	*Kwaliteit SIP-verbindingen* De SIP-verbindingen ondersteunen een minimale MOS-waarde van 4.0, waarmee een uitstekende gesprekskwaliteit wordt gerealiseerd die vergelijkbaar is met vaste telefonie.
Eis 44	*Communicatie bij onderhoud buiten onderhoudsvenster* Indien onderhoud buiten het overeengekomen onderhoudsvenster noodzakelijk is en dit impact kan hebben op de werking van de CCaaS-oplossing, informeert Opdrachtnemer ons hierover voorafgaand aan de werkzaamheden.
Eis 45	*Bereikbaarheid servicedesk* Opdrachtnemer beschikt over een servicedesk die tijdens de overeengekomen service-uren telefonisch bereikbaar is voor geautoriseerde medewerkers van BVO NL, waarbij meldingen direct in behandeling kunnen worden genomen.
Eis 46	*SLA servicedesk bereikbaarheid* Opdrachtnemer geeft inzicht in de bereikbaarheid van de servicedesk voor zowel telefonie als e-mail, uitgedrukt in het percentage meldingen dat binnen een vastgesteld aantal seconden respectievelijk binnen een vastgestelde termijn wordt beantwoord. Opdrachtnemer bevestigt de bijbehorende SLA-normen die gedurende de looptijd van de overeenkomst van toepassing zijn. Opdrachtnemer voldoet in elk geval aan een bereikbaarheid van: op werkdagen tussen 08.00u en 17.30u.
Eis 47	*Contactpersonen dienstverlening* Opdrachtnemer wijst vaste contactpersonen aan voor operationeel, tactisch en strategisch overleg, waarbij de vervanging van deze contactpersonen is geborgd en wordt vastgelegd in de communicatiematrix. Eén persoon mag meerdere rollen vervullen.
Eis 48	*Klachtenafhandeling* Opdrachtnemer beschikt over een vastgelegde klachtenprocedure, dat onderdeel uitmaakt van de overeengekomen SLA, en is verantwoordelijk voor een tijdige en correcte afhandeling van klachten.
Eis 49	*Wijzigingsverzoeken* Onder een standaard change verstaan wij een vooraf gedefinieerde wijziging met een bekend proces, vaste doorlooptijd en vooraf overeengekomen voorwaarden of tarieven, zoals vastgelegd in de SLA, het DAP of andere contractdocumenten. Voor wijzigingen die niet als standaard change zijn aangemerkt, verstrekt opdrachtnemer binnen tien (10) werkdagen na ontvangst van het wijzigingsverzoek een schriftelijk voorstel. Dit voorstel bevat in ieder geval een plan van aanpak, de impact op de dienstverlening, de doorlooptijd, de benodigde inzet van resources en de bijbehorende kosten. *Toelichting* Indien BVO NL hierop schriftelijk akkoord geeft zal erbinnen vijftien (15) werkdagen worden aangevangen met de werkzaamheden.
Contactcenter/ Rooster	
Eis 50	*Ondersteuning roosterprocessen Cliëntservice* De oplossing ondersteunt de specifieke roosterbehoefte van de Cliëntservice, waaronder, bezetting, beschikbaarheid en taken.

	Toelichting De medewerkers van de Cliëntservice worden voor het HRM-gerelateerde roosterproces gepland in het bestaande corporate roostersysteem PlanIT/PPS. De ondersteuning mag plaatsvinden via functionaliteit binnen de CCaas, het bestaande roostersysteem, via een aanvullende oplossing of via een geautomatiseerde koppeling, bijvoorbeeld op basis van Excel of Power Automate.
CCaas	
Eis 51	*Monitoring audiokwaliteit gesprekken* De oplossing monitort en registreert automatisch de gespreks- en audiokwaliteit van gesprekken per agent. De oplossing biedt inzicht in structurele kwaliteitsproblemen, zodat wij kunnen signaleren bij welke CS-medewerkers sprake is van onvoldoende gespreks- en audiokwaliteit, bijvoorbeeld als gevolg van thuiswerken en/of netwerkproblemen.
Eis 52	*Gesprekskwaliteit telefonie* De oplossing ondersteunt telefonie met een consistente en bruikbare gesprekskwaliteit, waarbij audiokwaliteit kan worden gemonitord en geanalyseerd per gebruiker of gesprek.
Contactcenter/Skills	
Eis 53	*Specialisaties telefonie en e-mail* Voor telefonie kunnen minimaal 5 specialisaties worden ingericht. Voor e-mail kunnen minimaal 2 specialisaties worden ingericht. Aan een agent kunnen meerdere specialisaties worden toegekend, met een minimum van 3 specialisaties per agent.
Kantoortelefonie	
Eis 54	*Beschikbaarheid telefonie* De telefoniedienstverlening is beschikbaar voor alle geautoriseerde gebruikers binnen de overeengekomen servicevensters.
Eis 55	*Telefoniefunctionaliteit* De oplossing ondersteunt inkomende en uitgaande telefonie, doorverbinden, wachtrijen, groepsoproepen, voicemail en nummerweergave.
Eis 56	*Continuïteit bereikbaarheid* De oplossing ondersteunt voorzieningen om de telefonische bereikbaarheid van de Cliëntservice en andere kritieke telefoonnummers bij storingen of uitval te behouden of zo snel mogelijk te herstellen, bijvoorbeeld via automatische failover, routering of alternatieve afhandeling van gesprekken.
Eis 57	*Nummerbeheer* Opdrachtnemer ondersteunt het beheren, toewijzen, wijzigen en migreren van telefoonnummers en servicenummers.
Eis 58	*Integratie Microsoft Teams* De CCaaS is geïntegreerd met Microsoft Teams via Extend of Unify en realiseert daarmee: • Synchronisatie van beschikbaarheid • Call routing naar wachtrijen / skill-based routing • Toetsinvoer of spraakgestuurde keuzes • Start/ stop opname van gesprekken

	• Transcriptie van calls, analyse van data • Rapportages naar BI • IVR-keuze zichtbaar voor de agent bij binnenkomend gesprek • uitgebreide agentstatussen • onderlinge zichtbaarheid van agentstatus • actuele wachtrijstatistieken • beheer van wachtrijen door supervisors, • het vastleggen van gespreksresultaten of notities • het onderscheid kunnen maken tussen beschikbaarheid voor cliënten en voor collega's De integratie is bovendien zodanig opgezet dat de media in de Teams cloud blijven, zoals bedoeld in het Beschrijvend Document of de bijlagen.
Eis 59	*Ondersteuning mobiele telefonie* De oplossing ondersteunt telefonie via desktop, webbrowser en mobiele apparaten.
Eis 60	*Gesprekskwaliteit telefonie* De oplossing ondersteunt stabiele gesprekskwaliteit en monitoring van audiokwaliteit.
Eis 61	*Gebruikersbeheer telefonie* Geautoriseerde beheerders kunnen gebruikers, nummers, wachtrijen en telefonie-instellingen zelfstandig beheren.
Eis 62	*Rapportages telefonie* De oplossing biedt inzicht in het gebruik, de beschikbaarheid en de prestaties van de telefoniedienstverlening. Daartoe moeten de volgende gegevens worden geproduceerd vanuit de CCaaS oplossing: • Aantal afgehandelde calls • Aantal cliënten in de wachtrij • Aantal inkomende calls • Aantal medewerkers beschikbaar • Aantal medewerkers in de groep • Aantal medewerkers in gesprek • Aantal uitgaande calls • Actuele wachttijd • Cliënt tevredenheid enquêteresultaten • Duur medewerker in bepaalde status, zoals beschikbaar, pauze of overleg • Gemiddelde afhandeltijd • Gemiddelde antwoordsnelheid • Gemiddelde gespreksduur • Gemiddelde nawerktijd • Gespreks- en audiokwaliteit • Missed calls • Service Level Individueel • Service Level van de groep • Totaal per kolom en geheel

	Het tonen van deze gegevens moet worden ingedeeld naar soort gebruiker (medewerker, team en management) zoals beschreven in bijlage K van het Beschrijvend Document, bij het kopje "rapportages".
Security en Privacy	
Eis 63	Opdrachtnemer heeft een gedocumenteerd informatiebeveiligingsbeleid en een persoon of functie te hebben aangewezen die verantwoordelijk is voor informatiebeveiliging.
Eis 64	Opdrachtnemer screent de eigen medewerkers die toegang hebben tot data van en/of over BVO NL. Dit omvat minimaal het overleggen van een Verklaring Omtrent het Gedrag (VOG) met een relevant screeningsprofiel (bv. voor omgang met vertrouwelijke gegevens), voor zover wettelijk toegestaan, en het laten ondertekenen van een geheimhoudingsverklaring.
Eis 65	Opdrachtnemer zorgt dat de eigen medewerkers, die toegang hebben tot data van en/of over BVO NL, periodiek bewustwordingstraining volgen op het gebied van informatiebeveiliging en privacy.
Eis 66	Opdrachtnemer hanteert een adequaat wachtwoordbeleid (complexiteit, lengte, periodieke wijziging).
Eis 67	Opdrachtnemer beschermt systemen die voor BVO NL worden ingezet, tegen malware met up-to-date anti-malware software.
Eis 68	Opdrachtnemer heeft een proces voor het detecteren, registreren en reageren op informatiebeveiligingsincidenten.
Eis 69	Opdrachtnemer meldt, alle informatiebeveiligingsincidenten die (mogelijk) impact hebben op BVO NL of haar data, onverwijld en uiterlijk binnen de contractueel afgesproken termijn, aan BVO NL.
Eis 70	Opdrachtnemer beveiligt kantoren en datacenters, waar BVO NL data wordt verwerkt of opgeslagen, fysiek tegen ongeautoriseerde toegang.
Eis 71	Opdrachtnemer garandeert dat alle fysieke media die vertrouwelijke data van BVO NL bevatten, veilig op worden geslagen en getransporteerd. Bij verzending dient gebruik gemaakt te worden van een traceerbare en betrouwbare koeriersdienst.
Eis 72	Opdrachtnemer garandeert dat de gegevens die niet langer nodig zijn, op een veilige en gecertificeerde manier worden vernietigd.
Eis 73	Opdrachtnemer verleent medewerking aan de periodieke beoordelingen door BVO NL, zoals een Quick Scan of een leveranciersgesprek, om de naleving van de overeengekomen eisen te toetsen.
Eis 74	Bij beëindiging van de overeenkomst dient opdrachtnemer alle data van BVO NL veilig en gecertificeerd te vernietigen of te retourneren, en daarvan aantoonbaar bewijs te overleggen.
Eis 75	Opdrachtnemer heeft een formeel proces voor risicomanagement en voert periodiek risicobeoordelingen uit op de dienstverlening aan BVO NL.

Eis 76	Opdrachtnemer beschermt alle PGI en andere vertrouwelijke data van BVO NL met encryptie, zowel tijdens transport (in-transit, bv. TLS 1.3+) als bij opslag (at-rest, bv. full disk of database encryption), gebruikmakend van actuele, industrie-standaard algoritmes (conform NCSC).
Eis 77	Opdrachtnemer hanteert een formeel wijzigingsbeheerproces. Opdrachtnemer commiteerd zich eraan dat BVO NL vooraf geïnformeerd wordt over significante wijzigingen in de dienstverlening, infrastructuur of sub-leveranciers.
Eis 78	Opdrachtnemer heeft een formeel vulnerability managementproces voor het periodiek scannen, identificeren en classificeren van kwetsbaarheden in alle systemen die voor BVO NL worden ingezet.
Eis 79	Opdrachtnemer heeft een patch managementproces om kritieke en hoge risico kwetsbaarheden tijdig te mitigeren, conform industrie-standaarden en/of contractueel vastgelegde termijnen.
Eis 80	Opdrachtnemer maakt periodiek back-ups van alle data en configuraties van BVO NL, conform de contractueel overeengekomen Recovery Point Objective (RPO).
Eis 81	Opdrachtnemer slaat back-ups veilig op, fysiek en/of logisch gescheiden van de productieomgeving, en te beschermen tegen ongeautoriseerde toegang en wijziging.
Eis 82	Opdrachtnemer legt de inzet van onderaannemers (sub-verwerkers) die BVO NL data verwerken vooraf ter goedkeuring voor aan BVO NL. De opdrachtnemer legt dezelfde beveiligingseisen op aan haar onderaannemers inclusief auditrechten.
Eis 83	Opdrachtnemer heeft een gedocumenteerd en getest Business Continuity Plan (BCP) en Disaster Recovery Plan (DRP) om de beschikbaarheid van de dienst te garanderen conform de contractuele afspraken (RTO/RPO).
Eis 84	Opdrachtnemer heeft een gedocumenteerde exit-procedure die beschrijft hoe, op verzoek van BVO NL, alle data op een veilige en volledige manier kan worden geëxporteerd in een leesbaar en bruikbaar formaat.
Eis 85	Opdrachtnemer verleent BVO NL het recht om (of via een onafhankelijke derde) audits uit te voeren op de naleving van de overeengekomen beveiligingseisen.
Eis 86	Opdrachtnemer heeft processen om de integriteit en authenticiteit van software- en hardwarecomponenten te waarborgen gedurende de levenscyclus (anti-manipulatie).
Eis 87	Opdrachtnemer verleent, op verzoek van BVO NL, medewerking aan (forensisch) onderzoek na een incident, inclusief het veiligstellen en aanleveren van relevante logs en ander digitaal bewijsmateriaal.
Eis 88	Opdrachtnemer voert jaarlijks een onafhankelijke penetratietest uit op de omgeving die voor BVO NL wordt gebruikt. Een management-samenvatting van de resultaten en het plan van aanpak voor bevindingen dient jaarlijks met BVO NL te worden gedeeld.
Eis 89	Opdrachtnemer garandeert en verschaft zekerheid, dat producten functioneren zoals bedoeld, zonder ongewenste functionaliteit, en dat componenten authentiek en ongewijzigd zijn.

Eis 90	Opdrachtnemer test de gedocumenteerde exitstrategie periodiek en deelt op verzoek van BVO NL de resultaten van deze test, om aan te tonen dat een soepele overdracht van data en diensten haalbaar is binnen de afgesproken termijnen.
Eis 91	Opdrachtnemer voert jaarlijks een hersteltest (restore test) uit om de integriteit van de back-ups en de effectiviteit van de herstelprocedure te valideren, conform de contractueel overeengekomen Recovery Time Objective (RTO). Een samenvatting van de testresultaten dient jaarlijks met BVO NL te worden gedeeld.
Eis 92	Opdrachtnemer wijst een vaste, benoemde contactpersoon voor informatiebeveiliging aan voor strategisch overleg met BVO NL.
Eis 93	Opdrachtnemer dient een actueel geldig NEN 7510:2024-certificaat of ISO 27001-certificaat. Jaarlijks een samenvatting van auditbevindingen en opvolgplan delen met BVO NL.
Eis 94	Opdrachtnemer dient een gedocumenteerd ISMS te hebben met PDCA-cyclus (beleid, risicoanalyse, interne audits, managementreview), inclusief jaarlijkse risicobeoordeling specifiek voor de BVO NL-dienstverlening. Jaarlijks wordt een managementrapportage gedeeld met BVO NL waarin het bewijs geleverd wordt voor de correcte werking.
Eis 95	Opdrachtnemer dient kwartaalrapportages te leveren over beveiligingsstatus: KPI's (patchlevels, incidenten, anomalieën), uitkomsten scans/penetratietests en auditbevindingen. Meldingen aan de AP of NCSC/Z-Cert dienen overlegd te worden aan BVO NL.
Eis 96	Opdrachtnemer erkent verwerking van persoonsgegevens (inclusief metadata in logs/netwerkverkeer) en sluit een verwerkersovereenkomst (AVG-art. 28) met BVO NL (naar het format van BVO NL), inclusief DPIA-ondersteuning bij wijzigingen.
Eis 97	Opdrachtnemer garandeert dat alle data, logs en beheerconfiguraties van BVO NL (inclusief cloud-beheerportalen) uitsluitend verwerkt/opgeslagen worden binnen de EER, of met expliciete schriftelijke goedkeuring en gelijkwaardig beschermingsniveau. Dit is inclusief support (bijvoorbeeld bij het overnemen van schermen).
Eis 98	Opdrachtnemer garandeert dat alle beheeraccounts (t.b.v. firewall, NAC, Wi-Fi, switches, cloud-portals) een MFA vereisen en dat gebruik gemaakt wordt van least-privilege principe en dat gebruik wordt gemaakt van rolgebaseerd toegangsbeheer met periodieke review (kwartaal). Er geldt een verbod op gedeelde accounts.
Eis 99	Opdrachtnemer garandeert een strikte logische en fysieke scheiding tussen het beheer van de cryptografische sleutels en de versleutelde data. Indien de data echter wordt gehost binnen een gecertificeerde EU-soevereine cloud, volstaat een strikte logische isolatie. De sleutels (inclusief back-ups) worden opgeslagen in een gecertificeerde Hardware Security Module (HSM) of een toegewijde Key Vault. Bij gebruik van een EU-soevereine cloud mag hiervoor gebruik worden gemaakt van de native, door de cloudprovider beheerde Key Management Services (KMS). Het gebruik van hard-coded keys in broncode of configuratiebestanden is strikt verboden. Het sleutelbeheer voldoet aantoonbaar aan de actuele richtlijnen van het NCSC of gelijkwaardige Europese cloudbeveiligingsstandaarden.

Eis 100	Opdrachtnemer zorgt voor een oplossing die voldoet aan NIS2 (risicoanalyse, supply-chain security, vulnerability disclosure).
Eis 101	Opdrachtnemer erkent dat alle data, metadata, logginginformatie, configuraties en afgeleide gegevens van BVO NL eigendom blijven van BVO NL. Leverancier verkrijgt geen zelfstandige gebruiksrechten anders dan noodzakelijk voor uitvoering van de dienstverlening. BVO NL kan continu, op ieder willekeurig moment, bij al haar data.
Eis 102	Het beheren van Identiteiten, toegang tot applicaties en autorisaties gebeurt volgens het RBAC-model en doet BVO NL voor het gehele landschap met een IAM-tool (HelloID). Uw oplossing staat provisioning en deprovisioning toe van Identiteiten en Autorisaties vanuit HelloID.
Eis 103	Opdrachtnemer beschikt over een actief securitymonitoringproces inclusief detectie van afwijkend gedrag, privilege misuse, ongeautoriseerde toegangspogingen en verdachte netwerkactiviteiten.
Eis 104	Opdrachtnemer beschikt over een vulnerability disclosure beleid inclusief meldproces voor beveiligingskwetsbaarheden.
Eis 105	Opdrachtnemer verstrekt inzicht in End-of-Life- en End-of-Support-data van gebruikte software-, firmware- en hardwarecomponenten.
Eis 106	Opdrachtnemer waarborgt de integriteit, authenticiteit en herleidbaarheid van softwarecomponenten binnen de leveringsketen.
Eis 107	Opdrachtnemer heeft aantoonbaar de eisen uit NEN7512 en NEN7513 geïmplementeerd (in geval van cliëntdata).
Eis 108	Opdrachtnemer heeft aantoonbaar technische en organisatorische maatregelen getroffen ter bescherming van persoonsgegevens, om te voldoen aan de AVG.
Eis 109	Belangrijke kaders voor toegang zijn need-to-know, need-to-use, logging en tweewegauthenticatie voor de toegang tot persoonsgegevens. Deze worden aantoonbaar toegepast door Opdrachtnemer.
Eis 110	Opdrachtnemer voldoet en blijft voldoen aan vigerende wetgeving waaronder maar niet uitsluitend AVG (GDPR), WABVPZ, WGBO, en faciliteert het gaan voldoen aan toekomstige toepasbare wetgeving waaronder maar niet uitsluitend WDO en WEGIZ. Indien van toepassing, ook voldoen aan Archiefwet.
Eis 111	Datalekken dienen binnen 24 uur gemeld te worden bij BVO NL wanneer persoonsgegevens van BVO NL betrokken zijn.
Eis 112	Opdrachtnemer heeft een vastgestelde procedure voor de afhandeling van een datalek en om deze te onderzoeken. Hierin zijn stakeholders vastgesteld om deze te informeren.
Eis 113	Opdrachtnemer gaat akkoord met het invullen en ondertekenen van de verwerkersovereenkomst van Bevolkingsonderzoek Nederland (bijlage bijsluiten) en legt aan evt. onderaannemer/sub-verwerker soortgelijke bepalingen op.

Eis 114	Opdrachtnemer zal de toegang en de autorisaties die zijn verleend ten behoeve van de uitvoering van de dienst(en) enkel voor dat doeleinde(n) gebruiken en niet voor andere doeleinden.
Eis 115	Opdrachtnemer heeft een privacyverklaring waarin de wijze van verwerking van persoonsgegevens beschreven is, evenals hoe een betrokkene zijn rechten uit kan oefenen. In geval van relatie verwerker-verwerkingsverantwoordelijke, werkt Leverancier actief mee bij AVG-verzoeken van betrokkenen.
Eis 116	Opdrachtnemer heeft een vastgesteld privacy beleid en heeft procedures ingericht waarbij de verantwoordelijkheid is vastgelegd. De verdeling van taken en verantwoordelijkheden hierin zijn gewaarborgd.
Eis 117	Opdrachtnemer heeft een actueel register van verwerkingsactiviteiten (verwerkingsregister).
Eis 118	Opdrachtnemer geeft de garantie dat de bij opdracht betrokken medewerkers, zich committeren aan en zich gedragen conform de bij opdrachtgever vigerende huisregels waaronder informatiebeveiliging. De opdrachtgever stelt deze desgevraagd vooraf ter beoordeling beschikbaar aan u.
Eis 119	Opdrachtnemer heeft een functionaris gegevensbescherming aangesteld of zal deze aanstellen (waar van toepassing).
Eis 120	Opdrachtnemer garandeert dat de geleverde AI-systemen volledig voldoen aan de verplichtingen uit de Europese AI-verordening (AI Act). Opdrachtnemer overlegt hiertoe op eerste verzoek een formele risicoclassificatie van het systeem, evenals het achterliggende kwaliteitsbeheersysteem (bij voorkeur ISO/IEC 42001 gecertificeerd). Indien sprake is van een hoog-risico AI-systeem, overlegt Opdrachtnemer de vereiste EU-conformiteitsverklaring en de technische documentatie conform de wettelijke vereisten.
IT Eisen	
Eis 121	Uw SAAS-applicatie heeft een API layer met read en write mogelijkheden en u kunt dit aantonen doordat de API layer gepubliceerd is.
Eis 122	De API layer staat direct ter beschikking; zonder aanvullende voorwaarden kan BVO direct beginnen met ontwikkel- en testactiviteiten en daarna de in productiename van één of meer integraties (zowel inkomende als uitgaande).
Eis 123	U stelt gedurende de contractperiode ten behoeve van eis API-2 een acceptatieomgeving ter beschikking.
Eis 124	De API layer heeft een minimale beschikbaarheid(sgarantie) groter dan 99,5% per maand, gemeten op een window van 0:00u tot 23:59u.
Eis 125	U ondersteunt in elk geval gangbare standaarden zoals JSON/Rest en/of XML.
Eis 126	U kunt uitleggen hoe u de top 10 belangrijkste risico's met API's mitigeert, zoals beschreven in: https://owasp.org/API-Security/editions/2023/en/0x11-t10/.

Eis 127	De API layer is opgezet via een zero-trust architectuur (zoals plaatsing achter een reverse proxy met IP white listing, of vergelijkbaar).
Eis 128	De applicatie is een moderne cloud oplossing; dus volledig Web-based en Saas, gebaseerd op een 3-tier software architectuur. Het is een native oplossing: er zitten geen legacy componenten verscholen in de architectuur. Er zijn geen technische implicaties (zoals benodigde VPN-verbindingen of plug-ins). De applicatie is SSO volgend via MS Azure.
Eis 129	Sessie-timeout (browser) moet in te stellen zijn (na XX minuten inactiviteit).
Eis 130	U levert desgevraagd adequate documentatie over het database schema zodat BVO database-relaties en eigenschappen van attributen kan begrijpen.
Eis 131	Geleverde applicatiediensten zijn compatible met actuele gangbare browsers: Google Chrome, Microsoft Edge, Safari.
Eis 132	Indien SaaS-dienst output voor bewerking door eindgebruikers van kantoortoepassingen levert, dan zijn deze opgebouwd in gangbare formaten zoals XML, CSV, XBRL.
Eis 133	Voor koppelingen, integratie, imports en export vindt data-uitwisseling plaats. U kunt uitleggen hoe u hierbij de lijst open standaarden (https://www.forumstandaardisatie.nl/open-standaarden) hanteert volgens het "Pas Toe of Leg Uit" principe.
Eis 134	Herstelmaatregelen, waaronder back-up en recovery procedures, zijn geïmplementeerd en worden periodiek getest.
Eis 135	Op de SAAS-omgeving wordt periodiek (minimaal 1x per jaar) uitwijktest uitgevoerd en de resultaten worden gedeeld met BVO.
Eis 136	U garandeert dat BVO te allen tijde eigenaar is van al haar data in uw oplossing. BVO kan continu, op ieder willekeurig moment, bij al haar data.
Eis 137	De data van BVNO NL moet in een gangbaar formaat geëxporteerd kunnen worden en ter beschikking gesteld (XML, CSV, XBRL).
Eis 138	U stelt in een afgesproken formaat en binnen een afgesproken termijn, de data van BVO aan BVO ter beschikking.
Eis 139	Uw oplossing heeft ten behoeve van provisioning de daartoe benodigde API/ endpoints.
Eis 140	Aan de gebruikers in uw applicatie worden rollen toegekend zodanig dat rechten via deze rollen kunnen worden gedefinieerd (RBAC).
Eis 141	Voor alle beoogde gebruikers (dus ook applicatiebeheerders) dat de applicatie Single Sign On (SSO) volgend is via Azure en met MFA.