



Zwolle

Bijlage XII

Programma van Eisen

Inhoudsopgave

1	Functionele eisen OOV	2
1.1	Balans tussen standaard inrichting en flexibiliteit	2
1.2	Signalen, aanmeldingen en casussen	2
1.2.1	Onderscheid signalen of aanmeldingen en casussen	2
1.2.2	Ontvangen van aanmeldingen en signalen	3
1.3	Vastleggen, bewerken, zoeken en vinden van gegevens	3
1.3.1	Vastleggen, koppelen en zoeken van entiteiten, aanmeldingen, signalen en casussen	4
1.3.2	Verrijking en analyse	4
1.3.3	Workflow	5
1.3.4	Wijze van vastleggen gegevens	6
1.4	Gebruiksvriendelijkheid	7
1.4.1	Gebruiksvriendelijk	7
1.4.2	Notificaties en signaleringen	7
1.4.3	Managen werkvoorraad en taken	7
1.5	Regievoering en samenwerking	8
1.5.1	Regievoering	8
1.5.2	Toegang en samenwerking met partners	8
1.5.3	Overleggen	8
1.5.4	Versturen en ontvangen van berichten	9
1.6	Data & rapportages	9
1.7	Conversie	10
1.8	Optie - Rechtmatigheidsonderzoeken Wmo en Jeugdwet en Sociale recherche	10
2	Architectuur en standaarden	11
2.1	Applicatiearchitectuur	12
2.2	Integratie	13
3	Informatiebeveiliging en privacy	16
4	Informatiebeheer	26
5	Functioneel beheer	27
6	Service level agreement (SLA)	28

1 Functionele eisen OOV

1.1 Balans tussen standaard inrichting en flexibiliteit

Het OOV-werkveld is zeer breed. We zoeken daarom naar de optimale balans tussen standaardinrichting en flexibiliteit bij de inrichting van werkprocessen, workflows, gegevensvelden en gebruikersschermen. Hierbij ondersteunt de standaardinrichting de organisatie met het bewaken van uniformiteit en de gebruiker met het behouden van overzicht en efficiënt samenwerken. De flexibiliteit zorgt ervoor dat de Oplossing ondersteunend is aan de specifieke vereisten van een werkproces en dat deze zo goed mogelijk aansluit bij de wensen en belevingswereld van de verschillende gebruikersgroepen.

Eis 1	De Oplossing biedt de Opdrachtgever de mogelijkheid om werkprocessen (zie Bijlage III en Bijlage IV) en workflows per werkproces afzonderlijk en naar eigen inzicht in te richten.
Eis 2	In de Oplossing kunnen (door de Opdrachtgever) per werkproces (zie Bijlage III en Bijlage IV), per fase van een werkproces en per soort entiteit verschillende gegevensvelden worden aangemaakt en toegevoegd als nieuw gegevensveld.
Eis 3	In de Oplossing kan door de Opdrachtgever per werkproces (zie Bijlage III en Bijlage IV) worden bepaald wat de gevraagde volgorde voor het invullen van gegevensvelden is en welke gegevensvelden verplicht moeten worden ingevuld en welke niet.
Eis 4	De Oplossing ondersteunt conditionele workflows, waarbij de vervolgstappen binnen een werkproces dynamisch worden bepaald op basis van bijvoorbeeld eerder gemaakte keuzes, ingevoerde gegevens of vastgestelde voorwaarden.

1.2 Signalen, meldingen en casussen

In ons werk maken we onderscheid tussen het behandelen van meldingen en signalen en het behandelen van casussen.

- Een **aanmelding** is een formeel verzoek om iets in behandeling te nemen en dit binnen een specifiek OOV-werkproces te beoordelen of op te pakken. Een melding wordt doorgaans door een ketenpartner of interne medewerker gedaan en heeft een duidelijk beoogd vervolgtraject, zoals het oppakken van lokale procesregie of triage op de Weegtafel Jeugd.
- Een **signaal** bevat informatie, bijvoorbeeld een waarneming of een melding die aandacht vraagt voor een persoon, groep, locatie, gebeurtenis of ontwikkeling die mogelijk relevant is voor de openbare orde, veiligheid of leefbaarheid. Een signaal kan aanleiding zijn voor nadere beoordeling, analyse of monitoring. Voorbeelden zijn een piketsignaal, een signaal over ondermijning via Meld Misdaad Anoniem of een signaal over een jongere dat wordt ingebracht bij het Vroegsignaleringsoverleg.
- Een **casus** is de toepassing van een werkproces op een entiteit, op een afgebakend moment in de tijd (met een start- en een einddatum). Het bestaat uit een samenhangend geheel van informatie, activiteiten en interventies rondom een specifieke entiteit of veiligheidsvraagstuk, met als doel een bepaald resultaat binnen een werkproces te bereiken. Een casus kan ontstaan naar aanleiding van één of meerdere signalen of meldingen, maar dat hoeft niet.

1.2.1 Onderscheid signalen of meldingen en casussen

Eis 5	In de Oplossing wordt onderscheid gemaakt in en een fasering aangebracht tussen de behandeling van een signaal of melding en de behandeling van een casus.
Eis 6	De Oplossing voorziet in de mogelijkheid om een nieuwe casus aan te maken naar aanleiding van een melding of signaal en deze melding of dit signaal te koppelen aan de betreffende nieuwe casus.
Eis 7	De Oplossing voorziet in de mogelijkheid om een melding of signaal toe te voegen aan een lopende casus of een afgesloten casus.

Eis 8	De Oplossing voorziet in de mogelijkheid om een nieuwe casus aan te maken zonder dat hier een aanmelding of signaal aan vooraf is gegaan.
Eis 9	De Oplossing voorziet in de mogelijkheid om meerdere casussen binnen een werkproces op te pakken onder één overkoepelende aanpak, bijvoorbeeld een gebiedsgerichte- of thema-/fenomeengerichte aanpak. Daarbij moet het mogelijk zijn om zowel op het niveau van de overkoepelende casus als de individuele casus informatie vast te leggen.

1.2.2 Ontvangen van aanmeldingen en signalen

We zoeken naar een Oplossing waarmee we op één plek aanmeldingen en signalen kunnen ontvangen, vastleggen, beoordelen en afhandelen.

Eis 10	De Oplossing bevat een functionaliteit om per werkproces aanmeldingen of signalen afkomstig vanuit verschillende bronnen en/of van verschillende actoren te ontvangen, vast te leggen, verrijken, beoordelen en routeren.
Eis 11	De Oplossing bevat een aanmeldingen- of signalenfunctionaliteit in de vorm van een webformulier of portaal. De input op dit formulier wordt automatisch in de aangeboden Oplossing geregistreerd als aanmelding of signaal en komt direct in de juiste werkbak van het betreffende werkproces terecht.
Eis 12	In de Oplossing moet een gebruiker (met de hiervoor benodigde rechten) een aanmelding of signaal handmatig kunnen invoeren.
Eis 13	De Oplossing voorziet in de mogelijkheid om de (aan)melder op de hoogte te brengen van ontvangst en afhandeling van de aanmelding of het signaal.
Eis 14	De Oplossing voorziet in de mogelijkheid om signalen vast te leggen in een logboekvorm, waar door verschillende gebruikers doorlopend aan gewerkt kan worden. Per log moeten in ieder geval de volgende gegevens kunnen worden vastgelegd: datum signaal, tijdstip signaal, een omschrijving van het signaal, uitgezette acties, besteedde tijd en naam van de behandelaar.
Eis 15	De Oplossing voorziet in de mogelijkheid om vanuit een signaal in het logboek direct een nieuwe casus aan te maken of het signaal te koppelen aan een lopende casus.

1.3 Vastleggen, bewerken, zoeken en vinden van gegevens

Het team OOV heeft te maken met multidisciplinaire en vaak complexe en langlopende casuïstiek rondom een entiteit: dit is meestal een persoon, maar kan ook een object, organisatie, locatie of groep zijn. Hierbij kan de betrokkenheid van team OOV door de tijd heen wisselen: soms zijn we op verschillende momenten in de tijd vanuit één of meerdere werkprocessen bij een entiteit betrokken (geweest) of vervullen we binnen een werkproces verschillende rollen (bijvoorbeeld eerst regisseur en later adviseur). Wij maken hierbij zelf onderscheid tussen:

- **Trigger** = een **signaal, aanmelding, bevinding** of analyse leidt ertoe dat een entiteit in beeld komt. Dit is de trigger (start) van de toepassing van een werkproces.
- **Entiteit** = alles waar een werkproces zich op kan richten, bijv. persoon, object, organisatie, locatie of groep.
- **Werkproces** = gestandaardiseerde manier van werken binnen het OOV-domein, gebaseerd op een gemeentelijke taak of bevoegdheid. Bijv. Lokale Aanpak Ondermijning of Procesregie.
- **Casus** = de concrete toepassing van een werkproces op een entiteit, op een bepaald moment in de tijd (dus met start- en eindmoment).
- **Rol OOV** = de betrokkenheid van OOV binnen een casus. Binnen een casus kan OOV verschillende rollen vervullen, afhankelijk van het werkproces en de fase waarin de casus zich bevindt. De rol bepaalt welke acties OOV uitvoert en welke verantwoordelijkheden gelden.

We zoeken naar een Oplossing waarin:

- Gegevens goed gestructureerd kunnen worden vastgelegd,
- Gegevens goed en eenvoudig vindbaar zijn,
- Gegevens gebruiksvriendelijk kunnen worden bewerkt, en
- Eventuele relatie(s) met andere werkprocessen binnen team OOV inzichtelijk zijn.

Daarbij willen we - uiteraard binnen de juridische kaders -:

- Voorkomen dat collega's binnen het team OOV langs elkaar heen werken, door onbedoeld met dezelfde entiteit(en) bezig te zijn,
- De vastgelegde informatie over één entiteit op één plek inzichtelijk kunnen maken,
- Ondersteund worden in het verrijken en analyseren van informatie,
- Onze betrokkenheid bij een entiteit door de tijd heen inzichtelijk kunnen maken,
- Wanneer de betrokkenheid wisselt, op de vastgelegde informatie voort kunnen bouwen.

1.3.1 Vastleggen, koppelen en zoeken van entiteiten, meldingen, signalen en casussen

Eis 16	De Oplossing voorziet in de mogelijkheid om, op elk moment in het proces, entiteiten te relateren aan andere entiteiten en daarbij aan te geven wat de (richting van) de relatie is. Bijvoorbeeld: Ouder-Kind en Kind-Ouder.
Eis 17	De Oplossing voorziet in de mogelijkheid om, op elk moment in het proces, entiteiten, meldingen, signalen en casussen over en weer aan elkaar te koppelen en daarbij aan te geven wat de (richting van) de relatie is.
Eis 18	De Oplossing voorziet in de mogelijkheid om (indien van toepassing) een entiteit waarop een melding, signaal betrekking heeft op de hoogte te brengen van de ontvangst daarvan en om in de Oplossing vast te leggen en te tonen of de entiteit op de hoogte is gebracht of niet.
Eis 19	De Oplossing biedt een zoekfunctionaliteit waarmee samenloop tussen meldingen, signalen, casussen en/of entiteiten kan worden geïdentificeerd. De zoekfunctionaliteit voldoet minimaal aan de volgende eigenschappen: • Automatisch identificeren van samenloop, op basis van (delen van) gegevens van minimaal één van de hoofdentiteiten. • Handmatig identificeren van samenloop, op basis van het uitvoeren van een zoekactie aan de hand van (delen van) gegevens van minimaal één van de vier hoofdentiteiten. • De zoekfunctionaliteiten kunnen worden toegepast op gestructureerde (gesloten invulvelden) en ongestructureerde informatie (open invulvelden).
Eis 20	In de Oplossing kunnen geïdentificeerde meldingen, signalen en/of casussen in ieder geval geraadpleegd worden op 'dat'-niveau.

1.3.2 Verrijking en analyse

Eis 21	De Oplossing voorziet in een labelfunctionaliteit waarmee meldingen, signalen en casussen binnen een werkproces gecategoriseerd kunnen worden op thema en (afhankelijke) subthema's. De (sub)thema's zijn per werkproces door de Opdrachtgever zelf in te richten op basis van lijstwerk. Het is mogelijk om meerdere labels toe te kennen aan een melding, signaal of casus.
Eis 22	De Oplossing voorziet in een labelfunctionaliteit waarmee meldingen, signalen en casussen gelabeld kunnen worden met risico-indicatoren. De risico-indicatoren zijn per werkproces door de Opdrachtgever zelf in te richten op basis van lijstwerk. Het is mogelijk om meerdere risico-indicatoren toe te kennen aan een melding, signaal of casus.

Eis 23	Een aanmelding, signaal en/of casus kan automatisch verrijkt worden door informatie uit in ieder geval de volgende openbare- en semiopenbare bronnen integraal via EnableU van gemeente Zwolle op te halen en vast te leggen: • BRP > Naam, adres, woonplaats, geboortedatum, geslacht BSN, zowel van betrokkene zelf als van het systeem van de betrokkene. • Handelsregister KvK > KVK-nummer, RSIN (optioneel), vestigingsnummer(optioneel), Rechtsvorm, naam, adres, e-mail, telefoonnummer, startdatum, Activiteiten (Sbi-codes), aandeelhouder/bestuurder/vennoot (naam, geboortedatum, adres) • Kadaster > adres kadastraal object, kadastrale aanduiding, koopjaar, koopsom, soort recht, eigenaar, naam, adres, woonplaats, geboortedatum.
Eis 24	De Oplossing voorziet in de mogelijkheid om mutaties in de basisregistraties (in ieder geval BRP en het Handelsregister) automatisch te verwerken en geeft daar een notificatie van.
Eis 25	De Oplossing voorziet in de mogelijkheid om gegevens van een entiteit handmatig vast te leggen / aan te vullen.
Eis 26	De Oplossing voorziet in de mogelijkheid om per entiteit, aanmelding, signaal of casus een geïntegreerd overzicht (vb. netwerkdiagram) te tonen waarin relaties met andere entiteiten, aanmeldingen, signalen en casussen in samenhang inzichtelijk worden gemaakt.
Eis 27	De Oplossing voorziet in de mogelijkheid om entiteiten, aanmeldingen, signalen en casussen geografisch op een kaart weer te geven, zodat locaties, onderlinge samenhang en ruimtelijke spreiding inzichtelijk kunnen worden gemaakt.
Eis 28	De Oplossing voorziet in de mogelijkheid om per entiteit, aanmelding, signaal of casus een tijdlijn weer te geven waarin relevante gebeurtenissen, activiteiten en/of betrokkenheid van OOV door de tijd heen inzichtelijk kunnen worden gemaakt.
Eis 29	De gebruiker kan selecteren welke onderdelen, relaties en detailniveaus in het netwerkdiagram, op de kaart of op de tijdlijn worden getoond, verborgen of gefilterd.
Eis 30	Voor het tonen en/of gebruik van kaarten wordt gebruik gemaakt van de Basiskaart Grootschalige Topografie (BGT) of Basisregistratie Topografie (BRT).

1.3.3 Workflow

Eis 31	De Oplossing voorziet in de mogelijkheid om per werkproces op verschillende plekken in dat werkproces conditionele keuzemenu's in te richten. Bijvoorbeeld bij de keuze voor een subthema (afhankelijk van thema) of de mogelijke bevindingen (bij afronding). De antwoord- en actiemogelijkheden zijn per werkproces door de Opdrachtgever zelf in te richten op basis van lijstwerk.
Eis 32	De Oplossing beschikt over een functionaliteit om de gebruiker te dwingen te controleren of alle criteria in een betreffende fase in een proces zijn ingevuld, voordat er door kan worden gegaan naar een volgende fase. Deze criteria kunnen zelf door de Opdrachtgever in de Oplossing worden aangepast en kunnen per werkproces verschillen.
Eis 33	De Oplossing voorziet in de mogelijkheid om een voltooide stap of fase in het werkproces te heropenen en daar ingevulde gegevens aan te passen, zonder dat overige gegevens wijzigen.
Eis 34	De Oplossing bevat een functionaliteit waarmee wordt bijgehouden op welk moment in de tijd een aanmelding, signaal of casus zich in een bepaalde fase of processtap van het werkproces bevond.
Eis 35	De Oplossing voorziet in de mogelijkheid om aan te vinken welke status een besluit op welk moment in de tijd heeft en houdt daar een logging van bij. Bijvoorbeeld datum conceptbesluit, datum zienswijze ingediend, datum definitief besluit.
Eis 36	De Oplossing bevat een overdrachtsfunctionaliteit waarmee een aanmelding, signaal of casus van het ene werkproces doorgezet kan worden naar een ander werkproces binnen de

	aangeboden Oplossing. Daarbij kan worden aangegeven welke vastgelegde gegevens beschikbaar moeten worden gesteld in het andere werkproces.
Eis 37	In de Oplossing kan een aanmelding, signaal of casus met opgaaf van reden administratief worden afgehandeld.
Eis 38	De Oplossing voorziet in de mogelijkheid om afgesloten casussen die zich nog binnen de bewaartermijn bevinden te heropenen en wijzigen. Daarbij moet kunnen worden vastgelegd waarom de casus heropend wordt.

1.3.4 Wijze van vastleggen gegevens

Eis 39	De Oplossing voorziet in een bijlagefunctionaliteit waarmee bijlagen (via drag en drop) kunnen worden toegevoegd aan een aanmelding, signaal of casus. Deze bijlagefunctionaliteit moet ondersteuning bieden voor het uploaden van verschillende bestandstypen, in ieder geval: PDF, DOCX, XLSX, JPEG, MP3, MP4, MSG.
Eis 40	De Opdrachtgever kan configureren welke metadata, kenmerken, labels of aanvullende informatie bij documenten/bijlagen worden kunnen worden vastgelegd, gefilterd en getoond.
Eis 41	De Oplossing voorziet in de mogelijkheid om documentatie (zoals een bijlage) toe te voegen aan een reeds afgesloten maar nog niet vernietigd(e) aanmelding, signaal of casus, zonder deze te moeten heropenen of de datum van afsluiten aan te passen.
Eis 42	In de Oplossing kan op meerdere manieren een locatie worden vastgelegd, in ieder geval door vastlegging van een adres, het omschrijven van de locatie of het aanwijzen op een kaart.
Eis 43	De Oplossing voorziet in de mogelijkheid om per aanmelding, signaal of casus contactmomenten te kunnen vastleggen in een contactenlogboek. Een log omvat minimaal een omschrijving van het contactmoment, met wie contact is geweest, de datum en gegevens van degene die de log heeft vastgelegd.
Eis 44	De Oplossing voorziet in de mogelijkheid om per aanmelding, casus of signaal aantekeningen of notities te kunnen vastleggen en daarbij aan te geven of deze informatie alleen bedoeld is voor intern gebruik.
Eis 45	De Oplossing voorziet in de mogelijkheid om datums in het verleden of de toekomst op te voeren.
Eis 46	De Oplossing voorziet in de mogelijkheid om binnen de Oplossing en dus zonder tussentijdse lokale opslag documenten aan te maken, op te slaan en te bewerken.
Eis 47	De Oplossing voorziet in een (brief)sjabloonfunctionaliteit, waarmee snel en eenvoudig middels door de Opdrachtgever opgestelde sjablonen gestandaardiseerde brieven of documenten gegenereerd kunnen worden. Per werkproces kunnen verschillende sjablonen beschikbaar worden gesteld. De Opdrachtgever kan de sjablonen zelf aanpassen, verwijderen of nieuwe toevoegen.
Eis 48	De Oplossing voorziet in de mogelijkheid om sjablonen automatisch te vullen met gegevens uit beschikbare gegevensvelden die al zijn gevuld.
Eis 49	De Oplossing voorziet in de mogelijkheid om een akkoord op een besluit vast te leggen in een audit-trail.
Eis 50	De Oplossing voorziet in de mogelijkheid om gegevens te exporteren of te delen. Daarbij kan de gebruiker selecteren welke gegevens, gegevensvelden en/of documenten in de export worden opgenomen.
Eis 51	De Oplossing registreert iedere export- of deelactie in een audit-trail en voorziet deze van metadata, waaronder ten minste de datum van de export, tijdstip van de export en de gebruiker die de export genereert. De Opdrachtgever kan bepalen welke exportformaten beschikbaar zijn voor gebruikers.

1.4 Gebruiksvriendelijkheid

1.4.1 Gebruiksvriendelijk

Eis 52	De Oplossing voorziet in de mogelijkheid om per werkproces, per type informatieobject (zoals een aanmelding, signaal of casus) en per gebruikersgroep schermindelingen en overzichten in te richten, waarin de voor de gebruiker relevante informatie in één oogopslag kan worden weergegeven. De Opdrachtgever kan per werkproces, type informatieobject en gebruikersgroep bepalen welke onderdelen in daarin worden opgenomen en op welke wijze deze worden gepresenteerd.
Eis 53	De Oplossing ondersteunt doorklikmogelijkheden vanuit overzichten, visualisaties en dashboards naar onderliggende informatieobjecten, zoals aanmeldingen, signalen en casussen.
Eis 54	De Oplossing waarschuwt gebruikers bij de invoer van een datum die afwijkt van de verwachte waarde of periode en biedt de mogelijkheid de invoer te corrigeren.
Eis 55	De Oplossing voorziet in de mogelijkheid om automatisch deadlines te hangen aan lopende casussen, taken of werkzaamheden op basis van door de Opdrachtgever vastgestelde termijnen of doorlooptijden. De deadlines moeten in een individuele casus handmatig aangepast kunnen worden.
Eis 56	In de Oplossing is het opschorten van de beslistermijn op casusniveau mogelijk.

1.4.2 Notificaties en signaleringen

Om collega's te ondersteunen is er behoefte aan automatische notificaties die zij ontvangen in geval van bijvoorbeeld:

- *Het ontvangen van een aanmelding, signaal, taak, bericht of agenda;*
- *Het koppelen van een aanmelding, signaal of casus aan een aanmelding, signaal of casus waar de gebruiker regie op heeft;*
- *Samenloop tussen entiteiten;*
- *Nieuwe informatie die is toegevoegd door een andere gebruiker;*
- *Een naderende aflopende termijn.*

Eis 57	De Oplossing bevat een notificatiefunctie waarmee gebruikers geautomatiseerd statusupdates van specifieke gebeurtenissen ontvangen per e-mail (als ze geen vaste gebruiker zijn) of binnen de Oplossing (als ze een vaste gebruiker zijn). Welke notificaties een gebruiker krijgt, is afhankelijk van de rol die een gebruiker heeft binnen een casus. In de notificaties wordt geen inhoudelijke informatie gedeeld.
---------------	--

1.4.3 Managen werkvoorraad en taken

We zoeken een Oplossing die het mogelijk maakt om regie te voeren en overzicht te behouden op het niveau van werkprocessen, casussen en individuele gebruikers. De werkvoorraad van individuele gebruikers kan betrekking hebben op meerdere werkprocessen.

Eis 58	De Oplossing ondersteunt het beheersen van de persoonlijke werkvoorraad, waarbij in minimaal de volgende functionaliteiten wordt voorzien: • Persoonlijk overzicht van aanmeldingen, signalen en/of casussen die aan de gebruiker zijn toegewezen; • Persoonlijke actie-/takenoverzicht.
Eis 59	De Oplossing voorziet in de mogelijkheid om de persoonlijke werkvoorraad van een andere collega in te zien.

Eis 60	De Oplossing voorziet in de mogelijkheid om de getoonde werkvoorraad te filteren, bijvoorbeeld op werkproces, tijdsperiode, fase en rol.
Eis 61	De Oplossing ondersteunt het beheersen van de werkvoorraad per werkproces, waarbij in ieder geval een overzicht kan worden getoond met nieuwe en openstaande aanmeldingen, signalen en/of casussen, eventueel toegekende prioriteit en de fase van het werkproces waarin zij zich bevinden.

1.5 Regievoering en samenwerking

1.5.1 Regievoering

Eis 62	De Oplossing voorziet in de mogelijkheid om verplicht een behandelaar toe te wijzen aan een aanmelding, signaal of casus, om centrale regie te borgen. Deze behandelaar heeft als enige het recht om de status van de aanmelding, het signaal of de casus te veranderen. De rol van behandelaar moet overgedragen of overgenomen kunnen worden.
Eis 63	De Oplossing voorziet in de mogelijkheid om per werkproces aanmeldingen, signalen en/of casussen te prioriteren.
Eis 64	De Oplossing ondersteunt in het opstellen en actualiseren van een plan van aanpak in een casus en in het monitoren van de voortgang op de verschillende onderdelen.
Eis 65	De Oplossing voorziet in de mogelijkheid om meerdere taken, interventies, maatregelen en/of resultaten te verbinden aan een casus.
Eis 66	De Oplossing voorziet in de mogelijkheid om taken met deadline toe te wijzen aan gebruikers.
Eis 67	De Oplossing voorziet in de mogelijkheid om gestandaardiseerde takenlijsten te koppelen aan een casus aan de hand van een takenlijstsjabloon. De takenlijstsjablonen kunnen verschillen per werkproces, zodat ze adequate ondersteuning bieden voor het doorlopen van een veelvoorkomende set aan taken binnen een bepaald werkproces.

1.5.2 Toegang en samenwerking met partners

Voor het team OOV is in de uitvoering van de verschillende werkprocessen samenwerking en informatie-uitwisseling met verschillende ketenpartners cruciaal. Het gaat hierbij om zowel vaste als wisselende interne en externe ketenpartners.

Eis 68	De Oplossing voorziet in de mogelijkheid om zowel vaste als incidentele partners toegang te geven tot de Oplossing en met hen samen te werken en informatie uit te wisselen.
Eis 69	De Oplossing voorziet in de mogelijkheid om per werkproces een netwerk van partners toe te voegen.
Eis 70	De Oplossing bevat een zoekfunctionaliteit om in het netwerk van partners een specifieke partner op te zoeken. Het moet mogelijk zijn om te zoeken op naam en/of organisatie.
Eis 71	De Oplossing voorziet in de mogelijkheid om partners inzage- en/of bewerkingsrechten te geven op (delen van) een casus. Bijvoorbeeld om informatie, agenda's of notulen in te zien en/of informatie of een terugkoppeling vast te leggen. Zij ontvangen per e-mail een notificatie waarin zij worden gewezen op de nieuwe informatie of openstaande vragen of handelingen.
Eis 72	De Oplossing voorziet in de mogelijkheid om verrijgingsverzoeken naar partners te sturen, waarna zij de gevraagde informatie zelf in de Oplossing vast kunnen leggen.

1.5.3 Overleggen

Eis 73	De Oplossing ondersteunt het plannen en coördineren van een overlegvorm waar meerdere signalen, aanmeldingen en/of casussen besproken worden. Deze overleggen zijn gekoppeld aan één of meerdere werkprocessen, bijvoorbeeld de Casustafel Jeugd en Veiligheid.
Eis 74	De Oplossing ondersteunt het plannen en coördineren van multidisciplinaire overleggen, gekoppeld aan één casus (bijvoorbeeld een MDO over één specifieke casus).

Eis 75	De Oplossing bevat een agendafunctionaliteit, waarmee per overleg een agenda kan worden opgesteld door aanmeldingen, signalen, casussen en/of eventuele bespreekpunten te agenderen door deze te koppelen. De agenda kan worden gedeeld met de genodigden van het overleg.
Eis 76	De Oplossing ondersteunt het organiseren van een overleg, door per overleg zowel een vaste groep deelnemers als incidentele deelnemers te kunnen uitnodigen.
Eis 77	De Oplossing voorziet in de mogelijkheid om tijdens het overleg live te notuleren en de notulen die in dit overleg ontstaan direct te koppelen aan/vast te leggen in de besproken casus, aanmelding of het signaal.

1.5.4 Versturen en ontvangen van berichten

Eis 78	In de Oplossing kunnen gebruikers binnen een werkproces of een casus berichten naar elkaar sturen en ontvangen (beide binnen de Oplossing).
Eis 79	In de Oplossing kunnen berichten van gebruikers van en naar niet-gebruikers van de Oplossing worden gestuurd en ontvangen. De ontvangende partij krijgt een notificatie per e-mail waarin deze wordt gewezen op een nieuw bericht, vraag of taak. In de notificatie wordt geen inhoudelijke informatie gedeeld.

1.6 Data & rapportages

Rapportages met betrekking tot de gevraagde Oplossing komen op de volgende wijzen tot stand:

- *Via standaard (operationeel-tactische) rapportages beschikbaar in de nieuwe Oplossing.*
- *Via het eigen gemeente Zwolle dataplatform gebaseerd op Microsoft Azure Fabric.*

Buiten scope zijn

- *PowerBI op het systeem zelf*
- *Andere applicaties op het systeem zelf*
- *Rapportage builder op het systeem zelf*

Eis 80	De Oplossing voorziet in een rapportagefunctionaliteit, waarmee standaard operationeel-tactische rapportages in dashboardvorm beschikbaar worden gesteld.
Eis 81	De Oplossing voorziet in de mogelijkheid om voor elk werkproces een eigen dashboard te tonen, waarmee in ieder geval inzicht kan worden gegeven in: • De aard en omvang van signalen, aanmeldingen en casussen (bijv. aantallen, thema's, signaaltypen, geografische spreiding) • Kwaliteit en (doorloop)snelheid van de uitvoering van een werkproces • Ingezette interventies, maatregelen en resultaten
Eis 82	De Oplossing voorziet in de mogelijkheid om voor het geheel aan werkprocessen van OOV een dashboard tonen, waarmee in ieder geval inzicht wordt gegeven in de totale: • Aard en omvang van signalen, aanmeldingen en casussen (bijv. aantallen, thema's, geografische spreiding) • Kwaliteit en (doorloop)snelheid van de uitvoering van de verschillende werkprocessen
Eis 83	De Oplossing voorziet in de mogelijkheid om de rapportages/dashboards te filteren op basis van bijvoorbeeld een datumbereik, gebied, werkproces, thema, label en/of rol.
Eis 84	De Oplossing voorziet in de mogelijkheid om (geaggregeerde) managementsamenvattingen van de rapportages te kunnen exporteren als statisch document (bijv. PDF).
Eis 85	De stuur- en managementinformatie die in de Oplossing zelf kan worden gegenereerd, kan geëxporteerd worden naar ten minste .XLSX en .CSV.

Eis 86	De Oplossing moet alle data kunnen aanbieden aan het dataplatform van de gemeente Zwolle, gerealiseerd met Microsoft Fabric.
Eis 87	Data wordt op basis van een vastgestelde frequentie (minimaal dagelijks, maar bij voorkeur op ieder moment) mogelijk geleverd, ofwel: er is een mogelijkheid tot toegang tot gegevens van de opdrachtgever t.b.v. managementinformatie (ter gebruik voor het Zwolse dataplatform).
Eis 88	Inzicht in de metadata wordt meegeleverd/is inzichtelijk (definities van tabellen, kolommen, velden en de relaties tussen die velden m.b.v. een of meerdere databasediagram(men)).
Eis 89	In de nieuwe Oplossing kan de bestaande metadatering op dusdanige wijze worden opgenomen, dat hierop rapportages kunnen worden gebouwd.
Eis 90	Op alle metadata velden moet kunnen worden gerapporteerd.
Eis 91	De koppeling tussen de nieuwe OOV Oplossing en het gemeente Zwolle Dataplatform moet ge-audit kunnen worden.

1.7 Conversie

Eis 92	De gegevens en bestanden uit de huidige toepassing Smart Veiligheid van de C3 Group bij de gemeente Zwolle worden geconverteerd naar de nieuwe toepassing. Het betreft de modules Generieke applicatie OOV (GOOV) en Ondermijning. Hieronder vallen ook de gegevens van de netwerkpartners.
---------------	---

1.8 Optie - Rechtmatigheidsonderzoeken Wmo en Jeugdwet en Sociale recherche

Eis 93	De Oplossing kan regionaal worden ingezet. <i>Toelichting:</i> <i>Toezichthouders van de gemeente Zwolle voeren de rechtmatigheidsonderzoeken WMO en Jeugdwet uit voor – op dit moment – 7 andere gemeentes.</i> <i>De Sociale Recherche van de gemeente Zwolle voert werkzaamheden uit voor – op dit moment 9 – andere gemeenten.</i>
Eis 94	Een deel van de gegevensverwerking van de Sociale recherche (BOA Domein 5) valt onder de Wpg, diensgevolge moet deze verwerking Wpg-auditproof zijn. Deze auditvereisten zijn gebaseerd op: • wetten.nl - Regeling - Wet politiegegevens - BWBR0022463 • wetten.nl - Regeling - Besluit politiegegevens buitengewoon opsporingsambtenaren - BWBR0041971

2 Architectuur en standaarden

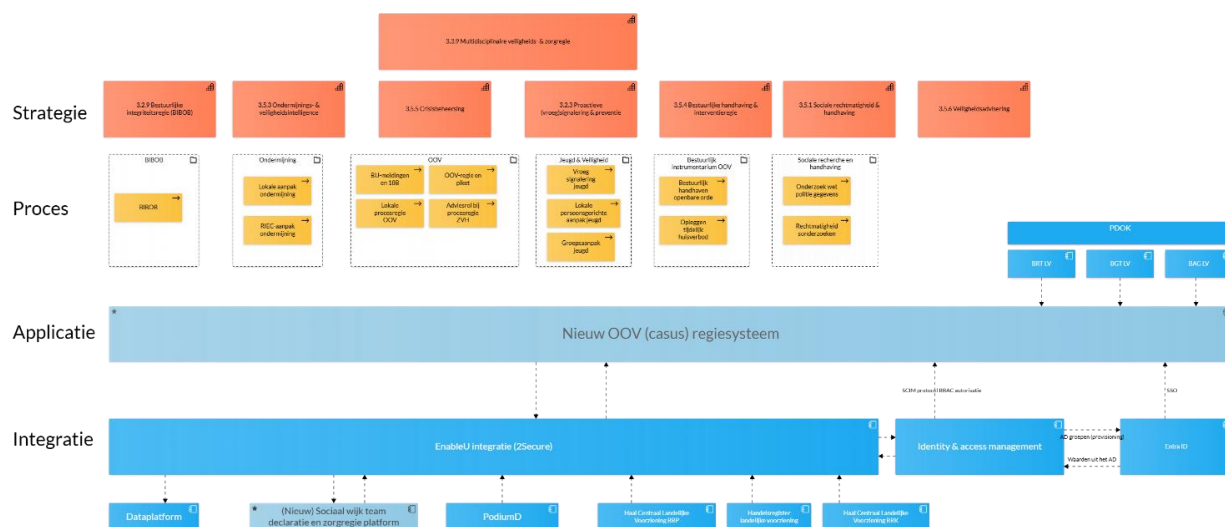
Beste inschrijver,

Zwolle staat op een belangrijk moment in de tijd waarbij open source software, common ground, soevereiniteit en autonomie belangrijke onderwerpen zijn. Als Zwolle hebben wij de keuze gemaakt om zoveel mogelijk af te stappen van monolitische saas applicaties die de data opsluiten en interoperabiliteit met het achterliggende applicatielandschap niet toelaten. Wij bewegen naar een (business) capability gebaseerde, datacentrische architectuur waarbij nieuwe applicaties feilloos passen binnen het ecosysteem van andere systemen. Deze architectuur eisen spelen daar expliciet op in.

Eis	Beschrijving
Eis 95	De Oplossing moet passen binnen de Zwolse architectuur, zoals beschreven in bijlagen: Bijlage XIII - Baseline Architectuur Gemeente Zwolle 2023 – 2024 Bijlage XIV - Architectuurprincipes Gemeente Zwolle' Bijlage XV - Enterprise architectuur principes 1.0 aanbesteding
Eis 96	De Oplossing wordt geleverd als SaaS-Oplossing, waarbij deze door of onder beheer van de inschrijver wordt gehost en technisch volledig onderhouden. Deze eis is onderdeel van het architectuurprincipe 3.26 SaaS, tenzij van Gemeente Zwolle .
Eis 97	De Oplossing dient benaderbaar te zijn via een fully qualified domein name.
Eis 98	De Inschrijver waarborgt dat de aangeboden Oplossing niet meer dan één major versie achterloopt ('neerwaartse compatibiliteit') op de open standaarden van het Forum Standaardisatie die voor de Oplossing van toepassing zijn. Aanpassingen in de standaarden worden door de Inschrijver verwerkt binnen 12 maanden nadat deze niet meer door Forum Standaardisatie als geldende standaard worden ondersteund. Daarnaast wordt de oude versie van de standaard nog minimaal 12 maanden ondersteund. Leverancier laat zien welke standaarden gehanteerd worden.
Eis 99	Authenticatie verloopt via Entra ID en autorisatie via de IAM-Oplossing van de opdrachtgever (Saviynt). De Oplossing ondersteunt SSO conform de standaarden van de opdrachtgever en ondersteunt minimaal SAML 2.0 en/of OpenID Connect (OIDC). De Oplossing is compatibel met Microsoft Entra ID.
Eis 100	De Oplossing betreft een standaard toepassing waarvan de functionaliteiten vaststaan. De geboden functionaliteit is gelijk aan die van andere klanten (op basis van best practices). Er worden geen Zwolle specifieke functionaliteiten ontwikkeld. Inschrijver geeft een kader mee over de configuratiemogelijkheden waar opdrachtgever gebruik van kan maken zonder risico's op uitval te lopen bij updates.
Eis 101	De Oplossing behoeft geen installatie op de werkplek.
Eis 102	De toegang tot systemen is altijd persoonsgebonden. Hierdoor is het gebruik van functionele accounts niet toegestaan. Inschrijver borgt dat functionele accounts niet gebruikt worden. Serviceaccounts ten behoeve van integratie zijn wel toegestaan mits ook voldaan wordt aan alle andere eisen van logging etc.
Eis 103	Inschrijver is in staat om integratie met achterliggende systemen te realiseren door aan te sluiten op de integratielaag van Gemeente Zwolle. Meer informatie over de integratielaag is te lezen in de paragrafen bij dit hoofdstuk.
Eis 104	Indien de Oplossing van inschrijver een (geautomatiseerd) algoritme bevat, dient deze na gunning transparant en uitlegbaar te zijn, mogelijk ter beoordeling aan te melden in het algoritmeregister.

2.1 Applicatiearchitectuur

In onderstaand overzicht wordt de positionering van de gevraagde Oplossing binnen de applicatiearchitectuur weergegeven. Verdere details over integratie zijn te lezen in de volgende paragraaf.



Toelichting: strategie toont de capabilities (Wat), Proces geeft hier invulling aan (Hoe).

Bestuurlijke integriteitsregie	Het vermogen om integriteits- en risico-onderzoek uit te voeren om te voorkomen dat de gemeente onbewust georganiseerde criminaliteit of ondermijning faciliteert bij het verlenen van vergunningen, subsidies, overheidsopdrachten of vastgoedtransacties, conform de Wet BIBOB.
Ondernijmings- & veiligheidsintelligence	Het vermogen om veiligheidssignalen en ketenberichten uit diverse bronnen (zoals meldingen van inwoners, MMA, politierapportages en CORV-berichten) gestructureerd te ontvangen, te verifiëren en doelgericht te routeren naar de juiste interventie- of zorgketen.
Multidisciplinaire veiligheids- & zorgregie	Het vermogen om voor personen met complexe, domein overstijgende problematiek een integrale en persoonsgerichte aanpak te regisseren om escalatie te voorkomen en herstel te bevorderen.
Crisisbeheersing	Het vermogen om de organisatie en de stad voor te bereiden op, en te sturen tijdens, publieke noodsituaties en rampen in de fysieke leefomgeving.
Proactieve (vroeg)signalering & preventie	Het vermogen om proactief en informatiegestuurd risico's bij inwoners of groepen te identificeren (zoals schulden, radicalisering, of huiselijk geweld) door signalen uit interne en externe netwerken te combineren, en hierop ongevraagd actie te ondernemen vóórdat escalatie plaatsvindt.
Bestuurlijke handhaving & interventieregie	Het vermogen om via bestuursrechtelijke instrumenten en regisserende interventies de openbare orde, veiligheid en leefbaarheid te herstellen en te handhaven, specifiek gericht op het beëindigen van ernstige overtredingen of dreigende situaties in de fysieke en persoonlijke levenssfeer.
Sociale rechtmatigheid & handhaving	Het vermogen om de integriteit van het sociale stelsel te bewaken door middel van onderzoek naar de rechtmatige verstrekking van voorzieningen en het bestrijden van fraude.
Veiligheidsadvisering	Het vermogen om gevraagd en ongevraagd inhoudelijk en strategisch advies te leveren over openbare orde en veiligheidsrisico's, ter ondersteuning van de bestuurlijke besluitvorming, ruimtelijke ontwikkelingen en complexe maatschappelijke vraagstukken.

2.2 Integratie

In onderstaand overzicht zijn de koppelingen weergegeven waarin de gevraagde Oplossing moet voorzien. Dit betreft zowel in- als uitgaande koppelingen. De details van iedere koppeling zijn onder het overzicht in tabelvorm opgenomen.

Eis	Beschrijving
Eis 105	Integratie met het achterliggende applicatielandschap vindt plaats via de integratielaag van de gemeente Zwolle. Deze is gebaseerd op EnableU (2orchestrate, 2secure en 2distribute). De Oplossing realiseert een integratie met deze integratielaag.
Eis 106	Binnen de Oplossing worden minimaal de volgende standaarden gehanteerd waar gekoppeld moeten worden met gestandaardiseerde integraties: • API-standaarden conform standaarden zoals gedefinieerd binnen Common Ground. • De berichtenstandaard StUF-BG 3.10. • De standaardservice Standaard Zaak- en Documentservices 1.1, Zaak- en Documentservices 1.2 of vergelijkbare CMIS standaard. Integratie middels standaard API's (bv HaalCentraal) geniet daarbij de voorkeur.

Naam	
KP id	1
Applicatie bron	Aanbieder
Applicatie doel	EnableU
Onderdeel van proces	Integratie met het achterliggend applicatielandschap
Doel	Door middel van deze robuuste integratie is het mogelijk om data van de aangeboden Oplossing uit te wisselen met het achterliggende applicatielandschap en ook event based integration te realiseren zodat handelingen in de Oplossing leiden tot triggers in andere applicaties.
Gewenste uitwisseling	API of Webservice gebaseerd

Naam	
KP id	2
Applicatie bron	Dataplatform Microsoft Azure
Applicatie doel	EnableU
Onderdeel van proces	Generiek voor OOV-processen
Doel	Er is een verbinding tussen ons integratieplatform en Azure gerealiseerd. Hiermee is het mogelijk om ingest van data in het dataplatform te realiseren.
Gewenste uitwisseling	Ingest, API gebaseerd

Naam	
KP id	3
Applicatie bron	(nieuw) sociaal wijk team declaratie & zorgregie platform
Applicatie doel	EnableU
Onderdeel van proces	Procesregie Zorg en Veiligheid; Jeugd en Veiligheid; BIJ-meldingen
Doel	Ten tijde van de aanbesteding OOV loopt er ook een aanbesteding voor het sociaal wijkteam. Inzake jeugdwet en multidisciplinaire hulpverlening is het

	noodzakelijk om data uitwisseling en triggers tussen beide systemen te realiseren. Dat doen we met tussenstap van het integratieplatform
Gewenste uitwisseling	n.t.b.

Naam	
KP id	4
Applicatie bron	PodiumD
Applicatie doel	EnableU
Onderdeel van proces	BIBOB; Bestuurlijk handhaven Openbare Orde
Doel	Ter ondersteuning van in ieder geval BIBOB processen is het noodzakelijk om zaakinformatie over vergunning aanvragen inzichtelijk te krijgen in de OOV applicatie.
Gewenste uitwisseling	ZGW-API

Naam	
KP id	5
Applicatie bron	Haal centraal BRP
Applicatie doel	EnableU
Onderdeel van proces	Alle genoemde OOV-processen
Doel	Ter ondersteuning van verschillende processen bij het bevragen van de BRP data voor natuurlijke personen
Gewenste uitwisseling	HaalCentraal

Naam	
KP id	6
Applicatie bron	HR LV
Applicatie doel	EnableU
Onderdeel van proces	Ondermijning (lokaal + RIEC); BIBOB; Jeugd en Veiligheid; OOV-regie/piket; Bestuurlijk handhaven openbare orde
Doel	Ter ondersteuning van verschillende processen bij het bevragen van het Handelsregister voor bedrijven
Gewenste uitwisseling	Handelsregister Landelijke voorziening (KvK API's)

Naam	
KP id	7
Applicatie bron	Savyint IAM
Applicatie doel	EnableU & nieuw casusregiesysteem
Onderdeel van proces	IAM
Doel	Savyint IAM zal het centrale component zijn die met SCIM services en RBAC toegangstoewijzing en provisioning zal verzorgen. Hiermee borgen dat de juiste roltoewijzing plaatsvindt. Ook zal IAM gebruikt worden voor de system-to-system integratie. IAM heeft een sturende rol naar EntraID voor de AD groepen

	Let op Op termijn is het wenselijk om identiteiten af te nemen van ketenpartners zoals politie. Hiermee zal Savyint een federated identity opzetten waarmee externe identiteiten geautoriseerd worden voor de Oplossing.
Gewenste uitwisseling	HaalCentraal

Naam	
KP id	8
Applicatie bron	EntraID
Applicatie doel	Nieuw casusregiesysteem
Onderdeel van proces	SSO
Doel	EntraID voor het inregelen van SSO op basis van identity
Gewenste uitwisseling	ntb

De onderstaande gevoorzieningen zijn op te vragen via landelijke voorzieningen van het Kadaster.

PDOK = Publieke Dienstverlening Op de Kaart.

Het Kadaster levert een kaartvoorziening: PDOK met verschillende kaartlayers. De BasisRegistratie Topografie (BRT) is grofmazig. Dat is de defaultlayer van PDOK. Als je verder inzoomt kun je de kaartlaag BGT gebruiken (dat gaat automatisch als beide layers zijn geselecteerd). Binnen zo'n kaartlaag kun je op een object klikken en dan worden de (openbare) gegevens getoond, bij de BAG kaartlaag zijn dat o.a. gegevens over Pand en Verblijfsobject (Vbo) = adres. PDOK kan geconfigureerd worden.

Naam	
KP id	9
Applicatie bron	PDOK, gewenste configuratie: Layers om aan of uit te kunnen zetten: BRT, BGT, BAG (voor pand en verblijfsobject), BRK (percelen) en luchtfoto Standaard gemeente Zwolle tonen.
Applicatie doel	Nieuw OOV regiesysteem
Onderdeel van proces	Generiek voor OOV processen
Doel	Toepassen als basiskaart afhankelijk van het schaalniveau
Gewenste uitwisseling	Als service gebruiken (PDOK)

Naam	
KP id	10
Applicatie bron	BRK
Applicatie doel	EnableU
Onderdeel van proces	Alle genoemde OOV processen
Doel	Kadastrale gegevens beschikbaar voor OOV processen
Gewenste uitwisseling	HaalCentraal

3 Informatiebeveiliging en privacy

De eisen voor informatiebeveiliging en privacy zijn opgesteld voor de vervanging van het huidige veiligheidsregistratiesysteem. Het systeem verwerkt bijzondere persoonsgegevens in het kader van Openbare Orde en Veiligheid, en is kritisch voor de uitvoering van wettelijke taken. Derhalve worden hoge eisen gesteld aan het borgen de vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid van gegevens in het kader van informatiebeveiliging op basis van de Cyberbeveiligingswet, die vanaf 15 augustus 2026 in werking is getreden, de daarmee samenhangende versie van de Baseline Informatiebeveiliging Overheid, BIO2, en AVG compliance.

Eis	Beschrijving
Eis 107	GIBIT 2025 artikel 28 (Controlerecht en audits), artikel 31 (Verwerkersrelatie), artikel 32 (Informatiebeveiliging) en artikel 38 (Periodieke derdenverklaring) zijn onverkort van toepassing. Aanvullend geldt: • Inschrijver borgt dat de Oplossing gedurende de looptijd van de overeenkomst blijft voldoen aan toepasselijke wet- en regelgeving, waaronder de AVG en de Cyberbeveiligingswet (Cbw/NIS2). • Inschrijver beschikt gedurende de contractperiode over een actuele assuranceverklaring met betrekking tot de Oplossing (SOC 2 Type II of gelijkwaardig).
Eis 108	GIBIT 2025 artikel 12 (Garanties ten aanzien van personeel) en artikel 19 (Geheimhouding) zijn onverkort van toepassing. Aanvullend geldt: • Medewerkers van inschrijver en derden die werkzaamheden in opdracht van inschrijver verrichten aan de Oplossing of toegang hebben tot de Oplossing en/of gegevens beschikken bij aanvang van hun werkzaamheden over een Verklaring Omtrent het Gedrag (VOG) die niet ouder is dan drie jaar. • De inschrijver borgt dat deze medewerkers en derden minimaal jaarlijks een training volgen op het gebied van informatiebeveiliging, privacy (AVG) en het herkennen en melden van beveiligingsincidenten.
Eis 109	GIBIT 2025 artikel 22 (Toegang tot Data en autorisaties) en artikel 32 (Informatiebeveiliging) zijn onverkort van toepassing. Aanvullend geldt: De Oplossing implementeert sterke toegangsbeveiliging conform de principes ‘least-privilege’ en ‘need-to-know’, hiervoor gelden de volgende specifieke eisen: • Multi-Factor Authenticatie (MFA): ○ De Oplossing ondersteunt Multi-Factor Authenticatie (MFA). ○ Voor accounts die rechtstreeks binnen de Oplossing worden beheerd, kan MFA worden afgedwongen. ○ MFA is verplicht voor privileged-, beheer- en administratieve accounts. ○ De Oplossing ondersteunt minimaal twee onafhankelijke authenticatiefactoren. • Role-Based Access Control (RBAC): ○ Toegang wordt verleend op basis van rollen en verantwoordelijkheden. ○ Gebruikers krijgen uitsluitend toegang tot gegevens die noodzakelijk zijn voor hun functie. ○ Fijnmazige autorisaties worden ondersteund, waaronder autorisaties op het niveau van het werkproces, een casus of een deel van een casus. • In aanvulling op bovenstaande is het in de Oplossing mogelijk om een incidentele (keten)partner te voorzien van een precieze autorisatie op een lopende casus, waarbij

de ketenpartner een account in de Oplossing krijgt zonder dat het account via federatieve autorisatie (IAM) wordt gemaakt.

- Wachtwoordbeheer:
 - Waar wachtwoorden binnen de Oplossing nog worden toegepast wordt steeds voldaan aan de meest actuele NCSC-richtlijnen voor wachtwoorden
- Bevoorrechte toegang (privileged/admin):
 - Het verlenen, wijzigen en intrekken van privileged- of administratieve rechten wordt afzonderlijk geregistreerd in auditlogs.
 - Gebruik van privileged rechten is herleidbaar tot een individuele gebruiker.
 - Inschrijver kan aantonen dat privileged accounts en rechten periodiek worden beoordeeld.

Eis 110 GIBIT artikel 8 (Interoperabiliteitseisen, normen en standaarden) en GIBIT artikel 22 (Data-uitwisseling) blijven onverkort van toepassing.

Aanvullend geldt:

De Oplossing garandeert veilige en betrouwbare communicatie met interne en externe partijen, met de volgende specifieke eisen:

- Beveiligde verbindingen:
 - Alle communicatie verloopt via beveiligde verbindingen conform de laatst geldende NCSC-richtlijnen voor TLS: TLS 1.3 (minimaal), Sterke cipher suites (bv. AES-256-GCM) en Certificaatvalidatie (geen self-signed certificaten).
- PKI-overheid-certificaten:
 - Gebruik van PKI-overheid-certificaten waar vereist voor communicatie met overheidsdiensten.
- API's:
 - De Oplossing ondersteunt gestandaardiseerde API's gebaseerd op: RESTful principes, JSON als dataformat, OpenAPI-specificaties.
 - API-toegang wordt beveiligd met: OAuth 2.0 en OpenID Connect (met PKCE voor public clients), Rate limiting (om DoS-aanvallen te voorkomen) en IP-whitelisting (waar toepasselijk).
- E-mailbeveiliging:
 - Indien de Oplossing het sturen en ontvangen van e-mails ondersteunt, worden alle verplichte beveiligingsstandaarden toegepast conform Forum Standaardisatie ('pas toe of leg uit'-lijst).

Eis 111 De Oplossing implementeert robuuste (sterke/solide) netwerkbeveiliging om ongeautoriseerde toegang en netwerkdreigingen te voorkomen, met de volgende specifieke eisen:

- Netwerkscheiding en segmentatie:
 - Duidelijke logische scheiding tussen productie-, test- en ontwikkelomgevingen.
 - Netwerksegmentatie wordt toegepast om de impact van beveiligingsincidenten te beperken.
 - Toegang tussen netwerksegmenten en applicatiecomponenten wordt uitsluitend toegestaan op basis van expliciet geautoriseerde verbindingen.
 - Bescherming tegen netwerkdreigingen middels firewalls en IDS/IPS:
 - Firewalls beschermen het netwerk tegen ongeautoriseerde toegang, Intrusion Detection Systems (IDS) en Intrusion Prevention Systems (IPS) detecteren en blokkeren dreigingen.
 - Zero Trust-principes:
 - Continue authenticatie en autorisatie (geen vertrouwen op basis van netwerklocatie), Minimale toegang (least privilege) op netwerkniveau.
-

Eis 112 De inschrijver borgt dat de Oplossing en de onderliggende beheeromgeving beschermd zijn tegen malware, ransomware en andere vormen van schadelijke code, met de volgende specifieke eisen:

- Malwaredetectie en -preventie:
 - Passende maatregelen zijn ingericht om malware, ransomware en andere schadelijke code te voorkomen, detecteren en blokkeren.
 - Detectiemechanismen, en dreigingsinformatie worden actueel gehouden.
- Detectie en monitoring:
 - Voorzieningen voor continue detectie en monitoring van verdachte activiteiten worden toegepast waarbij minimaal EDR-, XDR- of aantoonbaar gelijkwaardige detectie- en responsmaatregelen actief zijn.
 - Beveiligingsmeldingen worden actief gemonitord en tijdig opgevolgd.
- Preventieve maatregelen:
 - Schadelijke bestanden en bijlagen worden gedetecteerd en geblokkeerd.
 - Verdachte bestanden of actieve content worden gecontroleerd in een geïsoleerde of gelijkwaardig beveiligde omgeving (Sandbox) voordat deze worden uitgevoerd.

Eis 113 De inschrijver hanteert een cryptografiebeleid dat voldoet aan NCSC-richtlijnen en ISO 27001, met de volgende specifieke eisen:

- Cryptografiebeleid:
 - Het gebruik van versleuteling is gedocumenteerd, inclusief: Toepassingsgebieden (bv. gegevens in rust en in transport), Goedgekeurde algoritmen (bv. AES-256, RSA-4096, ECC) en Sleutelbeheerprocedures.
- Gegevens in rust:
 - Alle persoonsgegevens (inclusief back-ups en databases) worden versleuteld conform: NCSC-richtlijnen (bv. AES-256-GCM) of een gelijkwaardige norm (bv. FIPS 140-2).
- Gegevens in transport:
 - Alle communicatie wordt versleuteld conform de laatst geldende NCSC-richtlijnen voor TLS, waarbij minimaal TLS 1.3 wordt toegepast.
- Sleutelbeheer:
 - Cryptografische sleutels worden: Veilig gegenereerd (bv. met een Hardware Security Module (HSM)), Veilig opgeslagen (bv. in een key management system), Veilig gedistribueerd (bv. via PKI) en Ingetrokken bij compromittering of beëindiging toegang.

Eis 114 De Oplossing borgt de integriteit van gegevens gedurende vastlegging, verwerking, opslag en uitwisseling, met de volgende specifieke eisen:

- Invoervalidatie:
 - De Oplossing valideert invoer op juistheid, volledigheid, formaat en toegestane waarden om te voorkomen dat onjuiste, malafide of gemanipuleerde invoer kan leiden tot onjuiste gegevensverwerking, gegevenscorruptie of beveiligingsincidenten.
 - Consistente gegevensverwerking:
 - Integriteitscontroles worden toegepast om ongeautoriseerde wijzigingen te detecteren. (bv. checksums, hashes)
 - Gegevensmutaties worden consistent verwerkt waarbij gegevensverlies, dubbele verwerking of onvolledige transacties worden voorkomen
 - De consistentie van relaties tussen gerelateerde informatieobjecten, entiteiten en dossiers wordt geborgd. (bv. met foreign keys in databases).
 - Audittrail:
-

-
- Alle wijzigingen aan persoons-, dossier- en zaakgegevens worden herleidbaar vastgelegd
 - De audittrail bevat minimaal:
 - Wie de wijziging heeft uitgevoerd?;
 - Wat is gewijzigd?;
 - Wanneer is de wijziging uitgevoerd?;
 - Welke waarde voor de wijziging van toepassing was?.
 - Integriteit van gegevensuitwisseling:
 - De Oplossing waarborgt de integriteit van gegevensuitwisseling met ketenpartners en overheidsvoorzieningen door toepassing van passende cryptografische beveiligingsmaatregelen.
 - Back-upintegriteit:
 - Back-ups worden voorzien van integriteitscontroles (bv. hashes) om te verifiëren dat herstelde back-ups niet zijn gewijzigd of beschadigd.
-

Eis 115 De Oplossing legt relevante beveiligings- en verwerkingsgebeurtenissen vast in controleerbare en tegen manipulatie beschermde loggegevens, met de volgende specifieke eisen:

- Vastlegging van gebeurtenissen
 - De Oplossing registreert minimaal:
 - inlogpogingen (geslaagd en mislukt);
 - raadplegen, wijzigen, verwijderen, verstrekken en exporteren van gegevens;
 - wijzigingen in autorisaties en bevoorrechte rechten;
 - relevante systeem- en beveiligingsgebeurtenissen.
 - Inhoud loggegevens
 - Elke logregistratie bevat minimaal:
 - gebruiker of systeemidentiteit (herleidbaar);
 - uitgevoerde actie;
 - betrokken object (bijvoorbeeld dossier, document of gegeven);
 - datum en tijdstip;
 - resultaat van de actie (geslaagd of mislukt).
 - Logging van persoonsgegevens:
 - Voor verwerking van persoonsgegevens wordt aanvullend vastgelegd:
 - de aard van de verwerking (raadplegen, wijzigen, verwijderen, verstrekken of exporteren);
 - de bron van de gegevens indien van toepassing.
 - Bescherming van loggegevens:
 - Loggegevens zijn beschermd tegen ongeautoriseerde wijziging, verwijdering en manipulatie door middel van passende technische maatregelen, zoals: Write-Once-Read-Many (WORM) opslag, cryptografische controles of vergelijkbare voorzieningen (Digitale handtekeningen of hashes).
 - Bewaartermijn:
 - Loggegevens worden minimaal één jaar bewaard, tenzij wet- of regelgeving of toepasselijke auditvereisten een langere bewaartermijn voorschrijven.
 - Bij beveiligingsincidenten of onderzoeken kunnen relevante loggegevens gedurende een langere periode worden bewaard.
 - Kloksynchronisatie:
 - Systemen die loggegevens genereren maken gebruik van gesynchroniseerde tijdsbronnen zodat gebeurtenissen betrouwbaar kunnen worden gecorrigeerd..
-

Eis 116 De Oplossing integreert met centrale monitoringvoorzieningen voor tijdige detectie van incidenten, met de volgende specifieke eisen:

-
- SIEM/SOC-integratie:
 - Loggegevens worden geïntegreerd met een Security Information and Event Management (SIEM) en Security Operations Center (SOC).
 - Actieve monitoring:
 - Loggegevens worden actief gemonitord op: Afwijkingen (bv. ongebruikelijke inlogpogingen) en Beveiligingsincidenten (bv. brute force-aanvallen).
 - Opvolging meldingen:
 - Beveiligingsmeldingen worden: Binnen 1 uur geanalyseerd en Binnen 24 uur opgevolgd (afhankelijk van ernst).
-

Eis 117 GIBIT 2025 artikel 32.2, 32.6 en 32.7 (Informatiebeveiligingsincidenten) zijn onverkort van toepassing.

Aanvullend geldt:

De inschrijver beschikt over gedocumenteerde processen voor de detectie, analyse en afhandeling van informatiebeveiligingsincidenten, met de volgende specifieke eisen:

- Beveiligingsincidenten:
 - De inschrijver beschikt over een formeel proces voor registratie, classificatie, analyse en opvolging van beveiligingsincidenten.
 - Incidenten worden geclassificeerd op basis van risico en impact.
 - Kritieke beveiligingsincidenten worden onverwijld opgepakt en volgens de overeengekomen SLA-escalaties behandeld.
 - De leverancier documenteert de oorzaak van significante beveiligingsincidenten en treft corrigerende en preventieve maatregelen om herhaling te voorkomen.
 - Meldtermijnen (Cbw/NIS2):
 - De inschrijver meldt een mogelijk significant beveiligingsincident onverwijld, maar in ieder geval binnen een termijn, zodat opdrachtgever aan de in de Meldplicht Cbw opgelegde termijnen kan voldoen:
 - Een initiële melding uiterlijk binnen 24 uur na ontdekking, met aard, omvang en voorlopige impactinschatting.
 - Een nadere melding uiterlijk binnen 72 uur, met aanvullende analyse van ernst, impact en getroffen maatregelen.
 - Periodieke updates gedurende het incident.
 - Een eindrapportage binnen een redelijke termijn na afhandeling van het incident, met oorzaak, impact, getroffen maatregelen en verbeteracties.
 - Datalek (AVG):
 - Bij een vermoedelijk datalek of privacy-incident wordt de opdrachtgever: Onverwijld (binnen 24 uur na ontdekking) geïnformeerd en De melding bevat minimaal:
 - Aard van het incident.
 - Oorzaak (voor zover bekend).
 - Categorieën van gegevens en betrokkenen.
 - Impact en omvang.
 - Genomen en voorgenomen maatregelen.
 - Gezamenlijk actieplan:
 - Bij ernstige incidenten stelt de inschrijver samen met de opdrachtgever een gezamenlijk actieplan op.
 - Incident Response Oefeningen:
 - De inschrijver voert minimaal jaarlijks een incident response oefening uit (bv. tabletop exercise) en rapporteert hierover.
 - Forensisch onderzoek na cyberbeveiligingsincident:
-

-
- De inschrijver beschikt over forensische onderzoeksmogelijkheden voor diepgaande analyse van incidenten. Dit betekent in ieder geval technische diepgang (bit-niveau/ontleden van kwaadaardige code) en procedurele diepgang met behoud van chain of custody. De inschrijver mag hiervoor een extern specialistisch bureau inschakelen.
-

Eis 118 GIBIT 2025 artikel 10.14, 10.15 en 10.16 en GIBIT artikel 44 (Beheer en Onderhoud) zijn onverkort van toepassing.

Aanvullend geldt:

De inschrijver borgt professioneel IT-beheer voor de Oplossing, met de volgende specifieke eisen:

- Patch- en Updatebeheer:
 - De inschrijver installeert kritieke beveiligingsupdates binnen 7 dagen en overige updates binnen 30 dagen.
 - Kwetsbaarhedenbeheer:
 - De inschrijver identificeert, classificeert en volgt kwetsbaarheden maandelijks op, waarbij Kritieke/Hoog-kwetsbaarheden (Bv. CVSS>7.0) binnen 14 dagen worden opgelost.
 - Software Lifecycle:
 - De Oplossing maakt uitsluitend gebruik van ondersteunde software (met actieve beveiligingsupdates).
 - End-of-Life (EOL) software wordt voorafgaand aan EOL vervangen.
 - Hardeningsrichtlijnen:
 - De inschrijver configureert de systemen en componenten conform actuele NCSC-hardeningsguides of CIS benchmarks, waarbij afwijkingen maandelijks worden getoetst, hersteld of verklaard.
 - Configuratiebeheer:
 - De inschrijver borgt dat configuraties consistent, gecontroleerd en aantoonbaar conform beveiligingsrichtlijnen zijn.
 - Capaciteitsbeheer:
 - De inschrijver borgt dat de beschikbaarheid en performance bij piekbelasting geborgd blijft.
 - Remote Management:
 - De inschrijver borgt dat beheer op afstand verloopt via beveiligde verbindingen, met geauthenticeerde toegang en gelogde sessies.
 - Dataverwijdering:
 - De inschrijver borgt dat gegevens op opslagmedia, systemen en infrastructuurcomponenten bij buitengebruikstelling, vervanging of hergebruik aantoonbaar en onherstelbaar worden verwijderd.
-

Eis 119 De inschrijver past formele procedures toe voor het beheersen van wijzigingen aan de Oplossing, met de volgende specifieke eisen::

- Informatiebeveiligingseisen aan wijzigingsbeheer:
 - Wijzigingen worden vooraf beoordeeld op risico's voor continuïteit, informatiebeveiliging en gegevensintegriteit.
 - Wijzigingen worden getest voordat deze in productie worden genomen.
 - Voor wijzigingen met een verhoogd risico is een rollback-procedure beschikbaar.
 - De inschrijver kan aantonen dat wijzigingen gecontroleerd, gedocumenteerd en geautoriseerd zijn uitgevoerd.
-

Eis 120 De Oplossing borgt hoge beschikbaarheid en herstelcapaciteit bij calamiteiten binnen de gestelde RPO en RTO, met de volgende specifieke eisen als aanvulling op de GIBIT artikel 32.5:

- Back-up en Herstel:
 - De inschrijver waarborgt een Recovery Point Objective (RPO) van maximaal 1 werkdag door middel van back-ups, datareplicatie of een combinatie daarvan.
 - De inschrijver beschikt over herstelbare back-upvoorzieningen waarmee gegevens kunnen worden teruggezet naar een eerder herstelpunt. De frequentie van back-ups, snapshots en/of replicatie is passend bij de overeengekomen RPO.
 - De inschrijver borgt dat back-ups bestand zijn tegen cyberaanvallen, waaronder ransomware, door toepassing van de 3-2-1-1-0 back-upstrategie:
 - Minimaal 3 kopieën van data (productie + back-ups);
 - Opslag op minimaal 2 verschillende media of opslagtechnologieën;
 - Minimaal 1 kopie wordt offsite opgeslagen op een fysiek gescheiden locatie;
 - Minimaal 1 kopie is immutabel en beschermd tegen wijziging of verwijdering (bijv. air-gapped of write-once storage);
 - Back-ups worden regelmatig gecontroleerd en getest, zodat herstel zonder fouten (0 errors) aantoonbaar is.
 - Back-ups of gelijkwaardige herstelvoorzieningen worden opgeslagen in ten minste twee geografisch gescheiden datacenters, regio's of beschikbaarheidszones binnen de EU/EER.
 - De inschrijver borgt dat herstelprocedures minimaal jaarlijks technisch worden getest en aantoonbaar gevalideerd.
 - De inschrijver borgt een bewaartermijn van de back-up van minimaal twee maanden.
- Hersteltijd:
 - De inschrijver waarborgt een Recovery Time Objective (RTO) van maximaal 24 uur, waarbij het herstel de volledige beschikbaarheid van functionaliteit en data omvat.
- Continuïteits- en herstelbeheer:
 - De inschrijver beschikt over gedocumenteerde continuïteits- en herstelprocedures voor de aangeboden SaaS-dienst.
 - De continuïteits- en herstelprocedures worden minimaal jaarlijks getest en geëvalueerd.
 - De inschrijver kan aantonen dat de overeengekomen RPO- en RTO-doelstellingen kunnen worden gerealiseerd.
- Disaster Recovery:
 - De inschrijver beschikt over een Disaster Recovery Plan (DRP) voor de aangeboden SAAS-dienst.
 - Het DRP wordt minimaal jaarlijks getest, inclusief een technische failover- of hersteltest (waar mogelijk).
 - De resultaten van de test worden gedocumenteerd en leiden zo nodig tot verbetermaatregelen.

Eis 121 GIBIT 2025 artikel 34 (Dienstverlening op afstand-algemeen) en GIBIT artikel 39 (Waarborgen continuïteit) zijn onverkort van toepassing.

Aanvullend geldt:

De inschrijver borgt veilige hosting van de Oplossing, met de volgende specifieke eisen:

- Cloud- en Hostingleveranciers:
-

-
- De inschrijver borgt dat alle onderaannemers voldoen aan gelijkwaardige informatiebeveiligingseisen (eventueel aangevuld met ISO 27017/27018 bij cloudOplossingen) en contractuele afspraken worden geborgd.
 - Hostinglocatie:
 - De inschrijver borgt dat Oplossing wordt gehost binnen de Europese Economische Ruimte (EER) en verwerking van gegevens vindt uitsluitend binnen de EER plaats.
 - De inschrijver borgt dat data niet toegankelijk is voor derden (inclusief autoriteiten buiten de EER) zonder voorafgaande toestemming van de opdrachtgever.
 - Transparantie:
 - De inschrijver is transparant over de gebruikte hostinglocaties en geeft op verzoek inzicht in de locaties.
 - Redundantie en spreiding:
 - De inschrijver borgt dat de infrastructuur redundant en gespreid is om beschikbaarheid en continuïteit te borgen.
 - Beschikbaarheidsniveau:
 - De inschrijver host de Oplossing in een datacenter- of cloudomgeving die aantoonbaar voorziet in onderhoud aan kritische infrastructuur zonder onderbreking van de dienstverlening en beschikt over voldoende redundantie om uitval van afzonderlijke componenten op te vangen (vergelijkbaar met Tier III van het Uptime Institute).
 - Logische en fysieke scheiding:
 - De inschrijver borgt dat de Oplossing logisch en waar nodig fysiek zijn gescheiden van andere klanten, waarbij de gegevens van verschillende klanten niet toegankelijk zijn voor elkaar.
-

Eis 122 De Oplossing voldoet aan actuele standaarden voor applicatiebeveiliging en veilige softwareontwikkeling, met de volgende specifieke eisen:

- Secure Coding:
 - De inschrijver borgt dat de software wordt ontwikkeld volgens de NCSC-richtlijnen voor secure coding, ISO 27034 (Application Security) of vergelijkbaar en aantoonbaar vrij is van kwetsbaarheden uit de OWASP Top 10.
 - Security by Design:
 - De inschrijver borgt dat beveiliging structureel onderdeel is van het ontwikkelproces, waaronder ontwerp (bv. threat modeling), ontwikkeling en testen (inclusief code reviews en beveiligingstesten).
 - Beveiligingstesten:
 - De inschrijver voert minimaal 1 keer per jaar beveiligingstesten uit, waaronder: penetratietesten door een onafhankelijke partij, Static Application Security Testing (SAST), en Dynamic Application Security Testing (DAST).
 - De inschrijver mitigeert de bevindingen binnen 30 dagen (afhankelijk van risicoclassificatie).
 - Software-integriteit:
 - De inschrijver borgt de integriteit van software en broncode tijdens de ontwikkel-, build-, test- en releaseketen. Hierbij worden maatregelen toegepast voor versiebeheer, wijzigingscontrole en verificatie van de herkomst en integriteit van softwarecomponenten.
-

Eis 123 GIBIT artikel 25 (Software Bill of materials) is onverkort van kracht
De inschrijver borgt veilig leveranciersmanagement en ketenbeveiliging, waarbij periodiek de leveranciersbeoordeling van inschrijver wordt besproken in het jaarlijks overleg conform Eis

152. Onderwerpen zijn in ieder geval de compliance met de informatiebeveiligingseisen, financiële stabiliteit en kwaliteit van dienstverlening van de leveranciers van inschrijver.

Eis 124 GIBIT artikel 10.17 en 10.18 en GIBIT artikel 32.6 zijn onverkort van kracht.

Aanvullend geldt:

De inschrijver levert regelmatig rapportages en neemt deel aan periodiek overleg, met de volgende specifieke eisen:

- Rapportagefrequentie:
 - De inschrijver levert minimaal per kwartaal een beveiligingsrapportage op.
 - Inhoud rapportages
 - De rapportage bevat ten minste:
 - kwetsbaarheden en opvolging (inclusief resultaten van beveiligingstesten)
 - patchmanagementstatus
 - afwijkingen van hardeningsrichtlijnen
 - beveiligingsincidenten en opvolging
 - testresultaten van continuïteitstesten
 - Periodiek overleg:
 - Rapportages worden besproken in een kwartaaloverleg met opdrachtgever.
 - Proactieve Meldingen:
 - De inschrijver meldt proactief wijzigingen en ontwikkelingen die impact hebben op beveiliging of privacy.
-

Eis 125 Basisvereiste

GIBIT artikel 31 (Verwerkersrelatie) en GIBIT artikel 21.2 en 22.5 zijn onverkort van kracht.

Aanvullend geldt:

De Oplossing verwerkt persoonsgegevens conform de AVG en past privacy by design en privacy by default toe, met de volgende specifieke eisen:

- AVG-Compliance
 - De inschrijver borgt dat de verwerking van persoonsgegevens voldoet aan de AVG-beginselen, waaronder:
 - rechtmatigheid, behoorlijkheid en transparantie;
 - doelbinding;
 - dataminimalisatie;
 - juistheid;
 - opslagbeperking;
 - integriteit en vertrouwelijkheid;
 - verantwoordingsplicht.
 - Dataclassificatie:
 - De Oplossing ondersteunt door opdrachtgever gedefinieerde gegevensclassificaties voor dossiers, documenten en andere informatieobjecten.
 - De Oplossing ondersteunt het toepassen van deze classificaties ten behoeve van autorisaties, logging, verwerking, rapportages en bewaartermijnen..
 - Data-eigendom:
 - De inschrijver borgt dat alle gegevens die binnen de Oplossing worden verwerkt eigendom van de opdrachtgever blijven.
 - De inschrijver verkrijgt geen gebruiks- of exploitatierechten anders dan noodzakelijk voor de uitvoering van de overeenkomst.
 - Verwerking buiten EER:
 - Indien persoonsgegevens buiten de EER worden verwerkt, gebeurt dit uitsluitend na voorafgaande schriftelijke toestemming van opdrachtgever en met passende waarborgen conform de AVG
-

-
- DPIA:
 - De inschrijver levert op verzoek tijdig alle relevante informatie ten behoeve van een DPIA en ondersteunt actief bij het identificeren en mitigeren van privacyrisico's.
-

Eis 126 De Oplossing ondersteunt privacybeschermende verwerking van persoonsgegevens.

- Rechten van betrokkenen:
 - De Oplossing en dienstverlening ondersteunen de opdrachtgever bij het voldoen aan de rechten van betrokkenen conform de AVG.
 - De Oplossing biedt functionaliteiten voor inzage (dossierexport), correctie, verwijdering (voor zover toegestaan), beperking van verwerking en dataportabiliteit.
 - Anonimisering en pseudonimiseren:

De Oplossing ondersteunt anonimisering en pseudonimisering van persoonsgegevens, waarbij geanonimiseerde gegevens niet langer herleidbaar zijn tot een natuurlijke persoon.
 - Gegevensstromen:
 - De Oplossing biedt inzicht in herkomst, verwerking, verstrekking en opslaglocaties van gegevens.
 - Dataminimalisatie:
 - De Oplossing past waar mogelijk dataminimalisatie toe door gebruik van brongegevens en beperking van gegevensopslag.
 - Productiegegevens in testomgevingen
 - Productiegegevens (waaronder persoonsgegevens) worden niet gebruikt in test- of ontwikkelomgevingen. Er wordt gebruik gemaakt van gesynthetiseerde of geanonimiseerde data, tenzij gebruik van productiegegevens noodzakelijk is voor migratie- of conversiewerkzaamheden. Hierover worden nadere afspraken gemaakt.
-

4 Informatiebeheer

Op grond van de Archiefwet dient informatie gedurende de wettelijke bewaartermijn duurzaam toegankelijk opgeslagen te worden. De gemeente stelt daarom eisen aan de inrichting, het beheer en de uitvoering van functionaliteiten voor het toepassen en bewaken van bewaartermijnen.

Daarnaast is de gemeente verplicht informatie na afloop van de vastgestelde bewaartermijn volledig en onomkeerbaar te vernietigen conform de geldende vernietigingsprocedure. Voor het bepalen van de van toepassing zijnde bewaartermijnen worden de door de VNG vastgestelde selectielijsten (vanaf 2027 het Selectiebesluit) gehanteerd. De bewaartermijnen zijn hierin per proces, op resultaatniveau, vastgelegd.

-
- Eis 127** Het moet mogelijk zijn om een vernietigingsprocedure in te kunnen passen in de Oplossing
Toelichting: Volgens de Archiefwet 2020 hebben we als gemeente een vernietigingsplicht. Na het verstrijken van de bewaartermijn moet de informatie vernietigd worden. Voor het bepalen van de bewaartermijnen hanteren we de Gemeentelijke selectielijst 2020 van de VNG
-
- Eis 128** Het is mogelijk om een vernietigingslijst in .xlsx of .csv te kunnen uitdraaien met de vereiste informatie die nodig is om te kunnen vernietigen. De lijst moet op te bouwen zijn met de verplichte metadata: een id-nummer, omschrijving, startdatum, einddatum, bewaartermijn, en vernietigingsdatum
Toelichting: Om te kunnen vernietigen, moet een vernietigingslijst uitgedraaid kunnen worden waaruit blijkt welke informatie op welke grondslag vernietigd kan worden. De lijst wordt voorgelegd aan de archivaris en moet door hem beoordeeld kunnen worden. Hiervoor moet de lijst specifieke metadata bevatten
-
- Eis 129** De Oplossing geeft de mogelijkheid zoekopdrachten uit te kunnen voeren op ofwel Vernietigingsdatum ofwel Bewaartermijn in combinatie met de einddatum en ondersteunt het vernietigen in bulk-acties
Toelichting: Om het proces vernietiging te vergemakkelijken, willen we in bulk kunnen vernietigen op basis van zoekopdrachten op vernietigingsdatum of bewaartermijn in combinatie met een einddatum
-
- Eis 130** Aan elke casus/aanpak/werkproces kunnen, op basis van resultaat, specifieke bewaartermijnen toegekend worden. De bewaartermijn wordt geactiveerd na afhandeling.
Toelichting: Pas na afhandeling kan de wettelijke bewaartermijn gaan lopen.
-
- Eis 131** Signalen en casussen kunnen aan elkaar gekoppeld worden om de samenhang van het dossier te behouden. Hierbij wordt de bewaartermijn van de casus overgeërfd door de onderliggende signalen
-
- Eis 132** Bewaartermijnen kunnen achteraf handmatig aangepast worden
Toelichting: In geval van foutieve inrichting of afhandeling, moeten we in staat zijn om bewaartermijnen aan te passen. Ook bij wijzigingen van de wettelijke bewaartermijnen is dit nodig. Dit is van belang voor het kunnen uitdraaien van zuivere vernietigingslijsten
-
- Eis 133** Elke casus/aanpak/werkproces kan volledig en onomkeerbaar volgens de eigen bewaartermijn vernietigd worden, ook als er sprake is van een onderlinge relatie
Toelichting: Als een gezinslid binnen een gezinsgerichte aanpak een individueel traject krijgt, dan moet dit afzonderlijk van elkaar vernietigd kunnen worden. Dit betekent dat binnen de gezinsgerichte aanpak niet meer te zien mag zijn dat een persoon een persoonsgerichte traject heeft gelopen wanneer die vernietigd is. En andersom.
-
- Eis 134** Extern gecreëerde documenten moet kunnen worden opgenomen en handmatig en geautomatiseerd worden voorzien van metadata
Toelichting: Denk bijvoorbeeld aan e-mails en bijlagen die vanuit Outlook worden toegevoegd aan de aanpak
-

Eis 135	Bij een migratie naar een andere applicatie moet de volledigheid, authenticiteit en integriteit van de informatie gewaarborgd zijn <i>Toelichting: Dit kan bijvoorbeeld aan de hand van een controlegetal (checksum), waarmee de integriteit van informatie gecontroleerd kan worden.</i>
Eis 136	Alleen de Gemeente Zwolle mag toestemming geven tot het vernietigen van data.

5 Functioneel beheer

Eis 137	Opdrachtnemer levert gebruikershandleidingen.
Eis 138	U verzorgt, per functionaliteit en module een Nederlandstalige gebruikerstraining/instructie op de locatie van de gemeente Zwolle, afgestemd op de verschillende typen gebruikers (onderscheid functioneel beheer, key-users, overige gebruikers).
Eis 139	U stelt het opleidingsmateriaal zodanig samen dat de getrainde en opgeleide beheerders en key-users deze kunnen gebruiken én aanpassen om derden op te leiden en te trainen.
Eis 140	Alle documentatie, voor het gebruik en het beheer van de Oplossing is volledig Nederlandstalig en op taalniveau B1.
Eis 141	Opdrachtnemer verplicht zich de documentatie actueel te houden.
Eis 142	Per release, update en patch wordt een volledig overzicht meegeleverd van de inhoud van de release, update en patch. Een beschrijving van de nieuwe functionaliteiten, een opsomming van opgeloste fouten (beschrijving van de fout en de Oplossing) en instructies voor de functioneel beheerder.
Eis 143	Opdrachtnemer levert een lijst met bekende beperkingen (zowel technisch als functioneel) van de Oplossing, met betrekking tot de bij de gemeente Zwolle opgeleverde release bij implementatie.
Eis 144	Uw Oplossing biedt naast een productie omgeving een acceptatieomgeving waarin de Opdrachtgever kan testen. Op de acceptatieomgeving moeten dezelfde koppelingen gelegd worden als in productie maar dan met de acceptatie-/testomgevingen van deze systemen, voor zover deze beschikbaar zijn.
Eis 145	Het functioneel beheer van de OOV-Oplossing kan volledig door de Opdrachtgever worden uitgevoerd.
Eis 146	Op basis van het afgesloten contract garandeert de Opdrachtnemer dat de Oplossing, gedurende de contractperiode, doorontwikkeld zal worden zonder additionele kosten. Onder deze doorontwikkeling wordt, naast additief, correctief en preventief, ook verstaan dat op de Oplossing adaptief onderhoud wordt uitgevoerd om als opdrachtgever te blijven voldoen aan in de contractperiode geldende wet- en regelgeving en inspeelt op ontwikkelingen in de markt. Nieuwe ontwikkelingen op grond van specifieke wensen van de Opdrachtgever vallen hierbuiten.
Eis 147	Nieuwe releases, updates en patches mogen de basisfunctionaliteit uit dit PvE niet verstoren. Tenzij na akkoord van de Opdrachtgever.
Eis 148	De Oplossing houdt in geval van aanpassingen aan inrichtingsparameters rekening met historische content.

6 Service level agreement (SLA)

We verwachten een SLA waarin in ieder geval de volgende eisen zijn opgenomen.

Eis 149 De Inschrijver levert maandelijks een rapportage aan bij gemeente Zwolle over de volgende onderwerpen:

- Incidenten en de afhandeling daarvan
- Beschikbaarheid van de Oplossing
- Onderhoudsrapportages / releaseplanning
- Beveiligingscontroles
- Wijzigingsaanvragen en de afhandeling daarvan
- Klachtenrapportages

Daarnaast wordt jaarlijks de voortgang van (eventuele) verbeterrapportages (bv toegankelijkheidsverklaring WCAG 2.2) besproken

Eis 150 Opdrachtnemer stelt een Single point of Contact voor de Opdrachtgever.

De volgende drie communicatie en escalatie niveaus worden minimaal onderkend:

1. Operationeel (serviceniveau: procescoördinatie en 1e escalatie);
 2. Tactisch (service/contract management en vertegenwoordiger gebruikersorganisatie);
 3. Strategisch (directie/afdelingsmanagement).
-

Eis 151 Opdrachtgever krijgt periodiek een rapportage (SLR) met daarin een overzicht van de behaalde servicelevels, afgehandelde storingen/wijzigingen en eventuele beveiligingsincidenten. Deze rapportage wordt in een periodiek overleg tussen Opdrachtnemer en Opdrachtgever besproken.

Eis 152 Voor een goede organisatie van het beheer en onderhoud van de Oplossing is een eenduidige en efficiënte overlegstructuur noodzakelijk. De overlegstructuur is zodanig opgezet dat communicatie zo simpel en efficiënt mogelijk verloopt. Op strategisch (richten), tactisch (inrichten) en operationeel (verrichten) niveau is er communicatie tussen aanbestede dienst en inschrijver. De periodiciteit van de overleggen is als volgt:

- Strategisch 1 x per 12 maanden
 - Tactisch 1 x per 6 maanden
 - Operationeel 1 x per kwartaal
-

Eis 153 De Oplossing is op de volgende wijze beschikbaar:

- Beschikbaarheid tijdens kantoor tijden, ma t/m vr van 07:00-21:00: 99,9% (min.)
 - Beschikbaarheid buiten kantoor tijden: 99% (min.)
 - MTBF (Mean time between failure): 100 dagen (min.)
 - MTTR (Mean time to repair): Voor storingen langer dan 3 minuten: 4 uur (max.)
 - Maximaal dataverlies 24 uur
 - Maximale hersteltijd in geval van incidenten is binnen 16 werkuren (2 dagen van 8 uur).
-

Eis 154 De Inschrijver verzorgt een Nederlandstalige helpdesk voor zowel technische als functionele ondersteuning.

De helpdesk is het centrale punt voor het melden van incidenten, het stellen van vragen, indienen van wijzigingsvoorstellen en geeft informatie/ inzicht in de afhandeling daarvan.

Daarnaast geeft de Inschrijver inzicht in veelvoorkomende meldingen van andere klanten. De helpdesk van de Inschrijver levert zowel telefonische ondersteuning als ondersteuning via e-mail en/of een webportaal. De helpdesk is telefonisch bereikbaar tijdens kantooruren tussen 08.30 en 17.00 uur (CET). Voor ondersteuning door de helpdesk van de Inschrijver worden geen aanvullende kosten in rekening gebracht.

Voor incidenten buiten de openingstijden van de helpdesk is er voor 100% van de resterende tijd een storingsdienst/noodnummer beschikbaar.

- Eis 155** De helpdesk van de Opdrachtnemer is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de Oplossing volgens de procedure zoals vastgelegd in de SLA. De Opdrachtgever bepaalt de initiële prioriteit van incidenten. Ten aanzien van de ondersteuning wordt de volgende prioriteitsbepaling gehanteerd:

Categorie	Omschrijving
1	De Oplossing is volledig niet bruikbaar (naar mening van de Opdrachtgever een Critical Problem)
2	De Oplossing is deels niet bruikbaar of deels niet bruikbaar voor meer dan 10% van de gebruikers (naar mening van de Opdrachtgever een Major Problem).
3	Kleine verstoringen (naar mening van de Opdrachtgever een Minor Problem) Dit gaat om bijvoorbeeld om foutmeldingen zonder verdere consequenties.
4	Gebruikers/ beheerdersvraag.

De helpdesk draagt ook zorg voor relateren van incidenten aan al bekende problemen m.b.t. de Oplossing. De Opdrachtnemer maakt voor de Opdrachtgever inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is.

De Opdrachtnemer is eindverantwoordelijk voor het beheren van incidenten.

Opdrachtnemer geeft bij het niet behalen van de afgesproken dienstverlening (servicelevels) dit gemotiveerd per e-mail door aan de Opdrachtgever.

Categorie	Reactietijd	Oplossing binnen
1	0-0,5 uur beantwoorden (24/7)	Work-around binnen 4 uur. Oplossing binnen 8 uur
2	1 uur (tijdens kantooruren)	Work-around binnen 8 uur tijdens kantooruren. Oplossing binnen 48 uur tijdens kantooruren
3	24 uur (tijdens kantooruren)	Work-around binnen 2 werkdagen Oplossing in volgende reguliere versie maar uiterlijk binnen 1 maand.
4	24 uur (Tijdens kantooruren tussen 8.00 en 18.00)	Antwoord binnen 1 week

Opdrachtnemer dient bij iedere categorie een minimale KPI aan te geven.

De SLA wordt bij aanvang van de overeenkomst in onderling overleg specifiek en definitief gemaakt.

- Eis 156** De Opdrachtnemer is verantwoordelijk voor de gehele afhandeling van wijzigingsvoorstellen m.b.t. de Oplossing.
- De Opdrachtnemer is verantwoordelijk voor het inbrengen van wijzigingsvoorstellen ten behoeve van het oplossen van al geïdentificeerde problemen. Elk wijzigingsvoorstel ondergaat een intakeprocedure. De releasementen worden minimaal 2 weken van tevoren vastgesteld en beschikbaar gesteld in de acceptatie-omgeving waarbij releasenotes minimaal 3 werkdagen van tevoren worden opgeleverd. De Opdrachtnemer hanteert een vooraf afgestemde planning (met o.a. jaarplan van de releases) voor het uitbrengen van nieuwe releases.
- De Opdrachtgever heeft de mogelijkheid om nieuwe releases tegen te houden, dan wel een bezwaar in te dienen, als dit een risico vormt voor bedrijfskritische processen. Voor het oplossen van urgente productieverstoringen kunnen ad hoc crash releases worden ingepland.