

Projectstartarchitectuur

Digitaal Dossier JGZ ten behoeve van GGD
Zuid-Limburg

PROJECTSTARTARCHITECTUUR

Status
Versie
Datum

Definitief
V 20251128-1
28 november
2025

1

INLEIDING

1.1	Vraagstelling	3
1.1.1	Aanleiding, doelstelling en opdracht	3
1.1.2	Opdrachtgever	3
1.2	Aanpak, werkwijze	4
1.2.1	Betrokkenen bij de totstandkoming	4
1.2.2	Relaties met andere projecten	4

2

TOEKOMSTIGE SITUATIE

2.1	Scope	5
2.2	Stakeholders	5
2.3	Oplossingsrichting	6
2.3.1	Algemene principes	6
2.3.2	Specifieke principes rond informatiebeveiliging	11
2.3.3	Koppelingen	14
2.3.4	Specifieke functionele componenten	18
2.3.5	Training gebruikers en beheerders	21
2.3.6	Uitgangspunten ten aanzien van beheer	22
2.3.7	Datamanagement	23
2.3.8	Dataconversie/-migratie	24
2.3.9	Technische werkomgeving	25

1

INLEIDING

1.1	Vraagstelling	3
1.2	Aanpak, werkwijze	4

Inleiding

1.1 VRAAGSTELLING

1.1.1 AANLEIDING, DOELSTELLING EN OPDRACHT

GGD Zuid-Limburg beoogt door middel van een aanbestedingsprocedure één Opdracht aan één Inschrijver te verstrekken waarbinnen de behoeftestellingen van de JGZ-afdeling van GGD Zuid-Limburg de basis vormt. De Opdracht betreft, samengevat, het op basis van gebruiksrechten ter beschikking stellen, de implementatie (inclusief conversie) en het onderhoud c.q. beheer van een nieuw Digitaal Dossier JGZ. Voor GGD Zuid-Limburg betreft het de vervanging van het huidige systeem KD+ van leverancier Topicus. Verdere informatie over aanleiding, doelstelling en de opdracht is beschreven in hoofdstuk 2 van het Beschrijvend Document.

Deze projectstartarchitectuur (PSA) schetst de kaders waarbinnen de applicatie/de informatievoorziening moet passen dat door middel van de Aanbesteding wordt verkregen. Let wel: de (versie van de) PSA die bij het Beschrijvend Document is gevoegd, is maatgevend voor de Inschrijvingen en gunning van de Opdracht.

1.1.2 OPDRACHTGEVER

Opdrachtgever GGD Zuid-Limburg. Uitvoering van het project vindt plaats door een projectteam van GGD Zuid-Limburg.

1.2 AANPAK, WERKWIJZE

1.2.1 BETROKKENEN BIJ DE TOTSTANDKOMING

Bij het opstellen van deze projectstartarchitectuur is het projectteam, bestaande uit vertegenwoordigers van JGZ en de ondersteunende diensten, van GGD Zuid-Limburg betrokken.

1.2.2 RELATIES MET ANDERE PROJECTEN

Binnen GGD Zuid-Limburg spelen een aantal ICT-gerelateerde projecten die mogelijk een relatie hebben met het project voor het nieuwe Digitaal Dossier JGZ:

- Project rond de migratie van het organisatie brede data warehouse.
- Organisatieontwikkeling gerelateerd aan project Canvas.

2

TOEKOMSTIGE SITUATIE

2.1	Scope	5
2.2	Stakeholders	5
2.3	Oplossingsrichting	6

Toekomstige situatie

2.1 SCOPE

De scope van het project is beschreven in hoofdstuk 2 van het Beschrijvend Document.

2.2 STAKEHOLDERS

De stakeholders van deze PSA zijn:

Stakeholder	Belang
Opdrachtgever	De Opdrachtgever kan bepalen of de functionele behoefte die in deze projectstartarchitectuur is beschreven correspondeert met de beoogde functionaliteit.
Inschrijver	De Inschrijver kan aan de hand van de projectstartarchitectuur een goed te beoordelen functionele beschrijving geven van de oplossing die door de Inschrijver wordt aangeboden.
Leverancier	De Inschrijver die door de Opdrachtgever is geselecteerd, is in staat binnen de kaders van deze projectstartarchitectuur de oplossing te implementeren en onderhouden.

TABEL 1: STAKEHOLDERS

2.3 OPLOSSINGSRICHTING

2.3.1 ALGEMENE PRINCIPES

Voor het nieuwe Digitaal Dossier JGZ zijn de volgende algemene principes van toepassing.

De inschrijver levert een gebruiksklaar – na functioneel inhoudelijke inrichting - direct in productie te nemen Digitaal Dossier JGZ. Dit Digitaal Dossier is reeds aantoonbaar in gebruik bij meerdere JGZ-organisaties binnen Nederland voor meer dan zes maanden.

Het Digitaal Dossier JGZ biedt een volledig geïntegreerde logisch geheel aan functionaliteit waarmee alle wettelijke JGZ-taken (basistakenpakket) voor de doelgroep -9 maanden tot en met 23 jaar - zoals beschreven in [Wettelijk kader Basispakket JGZ - NCJ](#) - efficiënt, gebruiksvriendelijk en veilig kunnen worden uitgevoerd.

De gebruikersinteractie binnen het Digitaal Dossier JGZ is volledig Nederlandstalig en afgestemd op de werkprocessen van de JGZ-professionals.

Het Digitaal Dossier JGZ ondersteunt de actuele, landelijk vastgestelde standaarden waaronder de [Basis Dataset JGZ](#) (BDS). Het Digitaal Dossier JGZ voldoet aantoonbaar aan de [actuele eisen van een Goed Beheerd Zorgsysteem](#) (GBZ).

Kind- en ouderdossiers

Het Digitaal Dossier JGZ ondersteunt dossiervorming voor ouder en kind. Beide soorten dossiers kennen een gelijksoortige opbouw van de menustructuur, schermen en knoppen, zijn echter visueel duidelijk te onderscheiden van elkaar. Dossiers moeten voldoen aan de basis dataset (BDS, BDS-V).

Tussen dossiers moeten - in de applicatie voor de gebruiker, niet in het dossier zelf – links gelegd kunnen worden om de gezinsrelaties (broer(s), zus(sen), ouder(s)) te kunnen zien en te kunnen wisselen tussen de betreffende dossiers tijdens het werken hiermee.

Zorgtrajecten

Het Digitaal Dossier JGZ voorziet zowel in registratiemogelijkheden voor de 'standaard' JGZ-dienstverlening, als voor afwijkende, additionele zorgtrajecten. Denk aan een project als 'Keigezond Limburg', een initiatief in het kader van de regionale ketenaanpak overgewicht. Omwille van goede, overzichtelijke en volledige dossiervorming is het wenselijk om de registratie van additionele trajecten te kunnen borgen in het dossier van een cliënt. Cliënten kunnen meerdere trajecten gelijktijdig doorlopen. In een overzicht moet duidelijk te zien zijn welke trajecten en lopen en liepen. Vanuit dit overzicht willen we direct kunnen doorklikken naar een traject.

Zorg op maat

JGZ gaat steeds meer over op een aanbod waarin er geen vast schema van contactmomenten aangeboden wordt. Idealiter ondersteunt het Digitaal Dossier JGZ een zorgverlener bij het plannen van een volgend contactmoment door aan te geven wat de uiterlijke datum voor een volgend te plannen contactmoment is in verband met vaccinaties of wettelijk verplichte onderzoeken.

Toestemmingen

Toestemming van cliënten en ouders zijn op een centrale plek in het dossier van een cliënt te zien en aan te vullen door functioneel beheer. Deze toestemmingen (zoals onder BDS R010: Informatie over werkwijze JGZ staan vermeld) denk bijvoorbeeld aan toestemming voor het delen van informatie met andere zorgverleners of toestemming voor gebruik van gegevens voor wetenschappelijk onderzoek, moeten ook in de data export beschikbaar zijn. Toestemmingen kennen een ingangsdatum en wijzigingsdatums, toestemmingen kunnen immers ingetrokken worden.

Ouderlijk gezag

In het Digitaal Dossier JGZ willen we onderscheid kunnen maken tussen ouders die gezag hebben en ouders die geen gezag hebben en dossiers (tijdelijk) kunnen afschermen voor ouders.

De eerste categorie, gezaghebbende ouder(s) – hiermee bedoelen we hier aanstaande ouders, ouders en andere personen (waaronder adoptiefouder en stiefouders) die een jeugdige als behorend tot het gezin verzorgen en opvoeden, niet zijnde pleegouders, met het ouderlijk gezag - hebben recht op inzage in het dossier van hun kind(eren).

De tweede categorie, ouders die geen gezag hebben over hun kind(eren), hebben geen recht op inzage in het dossier van hun kind(eren). Desgevraagd hebben ze wel recht op om belangrijke feiten en omstandigheden die de persoon van het kind of diens verzorging en opvoeding betreffen te weten (conform artikel 1:377c BW).

Ook zijn er soms andere omstandigheden denkbaar waardoor het wenselijk is dat om een kinddossier, al dan niet tijdelijk, te kunnen afschermen voor ouders.

Het Digitaal Dossier JGZ voorziet in de mogelijkheid om dossiers te kunnen afschermen voor ouders en baseert de basisinstellingen hiervoor op gegevens ten aanzien van ouderlijk gezag uit de BRP of - bij voorkeur - het Gezagsregister.

Voldoen aan wettelijke kaders

Het Digitaal Dossier JGZ dient te voldoen aan geldende wettelijke kaders, waaronder bovengenoemd wettelijk kader Basispakket JGZ, de AVG, de Wet publieke gezondheid (Wpg), de Jeugdwet en de WGBO. De volgende kaders zijn relevant:

- Gebruik van A-nummer en BSN voor vaststelling van identiteit, mits bekend (bijv. asielzoekers, dan V-nummer).
- De applicatie ondersteunt de wettelijke identificatieplicht door het mogelijk te maken om bij het eerste contact de identiteit van de cliënt (jeugdige en/of gezaghebbende ouder) te controleren aan de hand van een geldig identiteitsbewijs en deze controle vast te leggen in het dossier, inclusief het type en nummer van het ID-bewijs en het BSN-nummer.

- De applicatie legt gezinsrelaties, met name gezagsrelaties, gestructureerd en eenduidig vast, zodat de juiste personen toegang hebben en de zorg optimaal kan worden afgestemd op de gezinscontext, conform de informatiestandaard JGZ van Nictiz.
- Alleen personen die direct betrokken zijn bij de zorg mogen toegang hebben tot het dossier, tenzij er uitdrukkelijke toestemming is verleend door de cliënt of zijn wettelijke vertegenwoordiger.
- Het Digitaal Dossier JGZ voorziet in logging conform NEN 7513.
- Gegevens enkel zijn opgeslagen conform AVG binnen landen binnen de Europese Economische Ruimte (EER).
- Cliënten kunnen verzoeken doen om hun dossier in te zien, te corrigeren en aan te vullen en – na afloop van de bewaartermijn - te laten verwijderen.
- Cliënten krijgen op verzoek een afschrift van hun dossier en kunnen het laten overdragen aan een derde partij (bijvoorbeeld een andere GGD in geval van verhuizing), via het Landelijk Schakel Punt (LSP). Indien beide organisaties dezelfde applicatie gebruiken en de betreffende applicatie een onderlinge overdracht op een andere manier ondersteund, is dit een goed alternatief.
- Het moet met een beperkt aantal handelingen mogelijk zijn om een client inzage in zijn of haar dossier te verschaffen en om het dossier in een gangbare elektronische vorm conform de AVG over te dragen.
- Per client een dossier.
- Dossiers in beginsel 20 jaar bewaren, na einde behandelrelatie.
- Herkent wanneer een jeugdige zelfstandig of mede kan tekenen c.q. toestemming kan geven (16 respectievelijk 12 jaar).
- Respecteren van de regeling rond ouderlijk gezag. In dit geval betekent ouderlijk gezag het recht en de plicht om een minderjarig kind te vertegenwoordigen bij medische handelingen. Ouderlijk gezag ligt bij de gezaghebbende ouder(s), adoptiefouder(s), stiefouder(s) of een ander(en) die een jeugdige als behorend tot het gezin verzorgen en opvoeden, niet zijnde pleegouder. Alle personen met ouderlijk gezag dienen toestemming te geven voor behandeling bij kinderen jonger dan 12 jaar. Bij kinderen van 12 tot 16 jaar is de toestemming nodig van zowel kind, als de personen met ouderlijk gezag. Gezagsverhoudingen kunnen worden gecontroleerd in het Centraal Gezagsregister, via de gezagsmodule (GM) van de BRP.
- Medewerkers moeten signalen van kindermishandeling of huiselijk geweld kunnen melden en passende maatregelen nemen (toepassen Meldcode).
- Gegevensverwerking conform Hoofdstuk 7 van de Jeugdwet.
- Het verstrekken van gegevens voor statistiek, informatievoorziening en beleidsvorming met betrekking tot de uitvoering van de Jeugdwet.

Gebruiksgemak

Het Digitaal Dossier JGZ volgt het werk(proces) en ondersteunt dat op een flexibele en gebruiksvriendelijke manier voor zowel client als medewerker. Dit betekent in ieder geval (en niet limitatief):

- De applicatie vereist zo min mogelijk overbodige handelingen en heeft een intuïtieve bediening.

- De applicatie beschikt over instelbare invoermaskers om incorrecte invoer waar mogelijk te voorkomen.
- De applicatie biedt gebruikers overzicht en signaleert actief op het proces (werkvoorraad en openstaande acties), voor medewerkers en cliënten.
- De applicatie ondersteunt de UTF8-tekenset en geeft diakritische tekens correct weer, zowel op het scherm, als op afdrukken. Ook in eventuele uitvoerbestanden en bij digitale gegevensuitwisseling is dit correct doorgevoerd. In zoekfuncties worden diakritische tekens daarentegen juist genegeerd in eerste instantie.
- Zoekfuncties zoeken bij het zoeken op namen automatisch ook naar namen die lijken op of klinken als de gezochte naam, maar anders worden gespeld, ook zonder wildcards te gebruiken.
- Zoekfuncties geven automatisch suggesties voor zoektermen zodra een gebruiker begint met het tikken van een zoekterm, gebaseerd op mogelijke overeenkomstige items uit de totale verzameling van items waarbinnen gezocht wordt.
- Het afdrukken en delen van dossiers met cliënten en ouders moet eenvoudig kunnen en qua opmaak hier ook geschikt voor zijn.

Archivering en vernietiging van dossiers

Na afloop van de behandelrelatie, omwille van leeftijd of verhuizing of anderszins, moet het mogelijk zijn om een dossier te archiveren. Een gearcheveerd dossier moet ook weer geopend/geactiveerd kunnen worden mocht daar noodzaak voor zijn.

Een speciale casus zijn overleden cliënten, zodra er via BRP een melding van overlijden binnen komt of deze handmatig door een medewerker wordt geregistreerd, dient een notificatie te worden gegeven aan de aan het dossier gekoppelde behandelaar(s). Daarnaast krijgt het dossier bij voorkeur een speciale status die aangeeft dat het dossier gearcheveerd moet worden ('te archiveren'). Dit is aan een medewerker die na het volgen van het protocol bij het overlijden van een cliënt het dossier archiveert.

Het moet met een beperkt aantal handelingen mogelijk zijn om dossier een geheel of gedeeltelijk te verwijderen met bewijs dat de gegevens daadwerkelijk verwijderd zijn, na afloop van de wettelijke bewaarplicht, al dan niet op verzoek van een client.

Het vernietigen van informatie in het Digitaal Dossier JGZ is slechts voorbehouden aan de daartoe geautoriseerde personen. Deze kunnen een selectie maken van dossiers die voor vernietiging in aanmerking komen en op basis van deze selectie een overzicht maken.

In een dossier kan een geautoriseerde gebruiker, onder vermelding van een reden, aangeven dat dit dossier niet vernietigd mag worden.

Leverancier levert een verklaring van vernietiging op over de dossiers die definitief vernietigd zijn volgens de standaard van Opdrachtgever. Vernietigde dossiers mogen nooit op een later moment, bijvoorbeeld bij het restoren van een back-up alsnog teruggeplaatst worden. Leverancier voert zelf vernietiging van gegevens in het Digitaal Dossier JGZ enkel en uitsluitend uit in opdracht van Opdrachtgever.

Overig

Het Van Wiechenonderzoek en de D-score - een door TNO ontwikkelde maat die de resultaten van het Van Wiechenonderzoek samenvat in één getal, waarmee de sociale, cognitieve en motorische ontwikkeling van jonge kinderen (0-4 jaar) objectief en universeel kan worden weergegeven – kan worden opgenomen als van een dossier van een cliënt.

Ten behoeve van rapportages en onderzoeken willen we doelgroepen onder de cliënten kunnen labelen. Dat wil zeggen dat we een kenmerk aan een dossier van een cliënt kunnen toevoegen op basis van een vooraf samengestelde keuzelijst. Denk aan nieuwkomers, PGA enzovoort.

Het Digitaal Dossier JGZ ondersteunt de geheimhouding van adressen die als zodanig in de BRP zijn gekenmerkt en verwijdt deze of voegt deze toe aan de betreffende cliëntdossier(s) zodra er een wijziging in de BRP binnenkomt.

Software as a Service

Het Digitaal Dossier JGZ wordt als webapplicatie afgenomen via het Software as a Service (SaaS) leveringsmodel. Vanuit GGD Zuid-Limburg gelden een aantal aansluitvoorwaarden. Uitgangspunt is dat deze aansluitvoorwaarden van toepassing zijn voor deze Opdracht. De richtlijnen zijn als bijlage bij deze PSA bijgevoegd.

Alle eindgebruikers en (functioneel) beheerders moeten gebruik kunnen maken van een webbrowser om de applicatie te benaderen. Dit moet onafhankelijk zijn van het soort device (pc/laptop/smartphone/tablet) waarmee de medewerker dit wil doen.

Gescheiden gegevensopslag

Leverancier draagt zorg voor een technisch logisch gescheiden gegevensopslag (o.a. databases en bestandssystemen) van de specifieke data GGD Zuid-Limburg binnen de 'generieke' SaaS-applicatie (pakketoplossing).

Beperken van maatwerk

Uitgangspunt is dat zoveel als mogelijk gebruik gemaakt wordt van standaardfunctionaliteiten die in het Digitaal Dossier JGZ beschikbaar zijn, waarbij deze functionaliteiten door inrichting/configuratie wel op de specifieke processen kunnen worden aangepast. Maatwerk wordt zoveel mogelijk beperkt, maar nadrukkelijk niet onmogelijk. Achtergrond hiervan zijn de kosten die gemoeid zijn met maatwerk, zowel voor het ontwikkelen, als het beheren ervan.

Toekomstbestendigheid

Leverancier volgt proactief de ontwikkelingen binnen de publieke (jeugd)gezondheidszorg en de ontwikkelingen in het sociaal domein en acteert hierin samen met Opdrachtgever door middel van doorontwikkelingstrajecten. Doorontwikkeling ten gevolge van wijzigende wet- en regelgeving (bijvoorbeeld op het gebied van privacy of gegevensbescherming) komen ten laste van Leverancier die

zorgt dat zijn Digitaal Dossier JGZ up-to-date blijft. Evenals toekomstige doorontwikkelingen van functionaliteiten die in het basispakket zitten.

Nieuwe versies van de BDS-JGZ (kinderen en volwassenen) dienen zo snel mogelijk, in ieder geval uiterlijk binnen zes maanden na publicatie ondersteund te worden door het Digitaal Dossier JGZ.

Na wijzigingen, zoals bijvoorbeeld de genoemde wijzigingen in de BDS, blijven eenmaal gedefinieerde rapportages, dossiers en dossieroverdrachten beschikbaar en operationeel.

2.3.2 SPECIFIEKE PRINCIPES ROND INFORMATIEBEVEILIGING

Specifiek op het gebied van informatiebeveiliging gelden de volgende principes:

Leverancier voldoet aan de [NEN 7510](#) norm, (inclusief naleving van [NEN 7512](#) en [NEN 7513](#)) en de BIO2 richtlijn. Eventuele partners en leveranciers (subverwerkers) voldoen eveneens aan NEN 7510 of [ISO 27001](#) en BIO2 of NIS-2 richtlijnen. Leverancier is in staat certificaten hiervan, uitgegeven door een geaccrediteerde auditor, inclusief de verklaring van toepasselijkheid (jaarlijks) te overleggen ten behoeve van een controle door een onafhankelijke auditor.

Informatiebeveiliging op niveau passend bij medische gegevens

De applicatie inclusief de onderliggende hosting en housing dient beveiligd te zijn op het niveau dat past bij een systeem waar medische gegevens in worden verwerkt en zijn opgeslagen. De toepasselijke norm voor informatiebeveiliging is NEN 7510 (bovenop ISO 27001), rekening houdend met de AVG.

Toegang en logging

Op het gebied van toegang en logging voor het Digitaal Dossier JGZ gelden de volgende punten:

- De toegang tot de applicatie geschiedt met multifactor authenticatie (MFA), conform NEN 7510, met de toevoeging dat de *authentication strength* minimaal op het niveau van een *authenticator-app* (TOTP) ligt en SMS niet is toegestaan.
- Het Digitaal Dossier JGZ dwingt het gebruik van sterke wachtwoorden - bestaande uit minimaal 15 tekens, bestaande uit een combinatie van hoofdletters, kleine letters, cijfers en speciale tekens, zonder spaties - af. Gebruikers worden bovendien verplicht om hun wachtwoord regelmatig - minimaal tweemaal per jaar - te wijzigen. Minimaal de laatste 12 gebruikte wachtwoorden mogen niet worden hergebruikt.
- Wanneer een medewerker al met MFA op de portal/werkplekomgeving is ingelogd, dan kan bij voorkeur al direct van de applicatie gebruik gemaakt worden (Single Sign On). Hiervoor is een koppeling met Entra ID van GGD Zuid-Limburg noodzakelijk.
- De applicatie voorziet in logging conform NEN 7513. Deze logging is voor functioneel beheerders te allen tijde inzichtelijk en is het mogelijk om hier rapportages van te maken.

- Leverancier houdt een audit trail bij van iedereen die toegang heeft gekregen tot het Digitaal Dossier JGZ. GGD Zuid-Limburg krijgt toegang tot deze audit trail ten behoeve van probleemanalyse en om te gebruiken als bewijsmateriaal bij overtreding van wet- en regelgeving.
- Logmutaties worden zodanig vastgelegd en ontsloten dat ze eenvoudig gesorteerd en gefilterd kunnen worden op relevante kenmerken, zodat achteraf controle, verantwoording en inzage mogelijk zijn voor cliënten, zorginstellingen en toezichthouders.
- De autorisatie van de loggegevens is dusdanig dat deze nooit gewijzigd kunnen worden.
- Inzage in de volledige audit logs is beperkt tot bevoegde functionarissen (zoals beheerders, security officers of privacy officers).
- Medewerkers mogen alleen inzage krijgen in logging voor zover dat noodzakelijk is voor hun functie.
- Idealiter voorziet Leverancier in monitoring van deze logging gekoppeld aan real-time analyse en dreigingsdetectie.
- Patiënten hebben wettelijk recht op een overzicht van wie hun dossier heeft ingezien en met welk doel.
- Sessie time-out: de applicatie dient de gebruiker automatisch uit te loggen na een vast te stellen periode van inactiviteit.

Autorisaties

Het Digitaal Dossier JGZ ondersteunt restrictie op toegang tot functionaliteiten en gegevens op basis van autorisaties van medewerkers. Uitgangspunt hierbij is de rol of zijn de rollen die de betreffende medewerker heeft (role based access control, RBAC).

Per rol kunnen autorisaties worden toegekend: raadpleeg-, wijzigings- en/of verwijderrechten. Deze autorisaties moeten per rol en per dossieronderdeel of functionaliteit kunnen worden toegekend.

'Breaking the Glass'

Het Digitaal Dossier JGZ ondersteunt 'Breaking the Glass'-rechten conform NEN 7510, waarbij een behandelaar in (spoed- of nood)situaties waarin normale authenticatiemethoden onwerkbaar zijn tijdelijk en gecontroleerd toegang kan krijgen tot dossiers die normaal gesproken niet toegankelijk zijn. De applicatie logt en monitort het gebruik van deze functionaliteit en zorgt voor een proactieve melding richting een privacy officer die kan controleren of het gebruik gerechtvaardigd was.

'Privacy by design', 'Privacy by default', 'Security by design' en 'Security by default'

Het Digitaal Dossier JGZ is ontworpen en ingericht volgens de principes 'Privacy by design', 'Privacy by default', 'Security by design' en 'Security by default'.

Privacy by design houdt in dat in het ontwerp van de applicatie al aandacht is voor privacy-aspect. Onderdeel hiervan is Privacy by default: dit betekent dat standaardinstellingen van de applicatie zo privacy-vriendelijk als mogelijk zijn.

Security by Design betekent dat beveiliging vanaf het allereerste ontwerp van de applicatie wordt meegenomen. Het is een proactieve benadering waarbij veiligheid geïntegreerd wordt in elke fase van de ontwikkeling. Security by Default betekent dat een systeem standaard veilig is geconfigureerd, zonder dat de gebruiker extra stappen hiervoor hoeft te nemen.

Data integriteit

Het Digitaal Dossier JGZ is zo ontworpen en opgebouwd dat de data-integriteit te allen tijde gewaarborgd is. Zo staat de applicatie het gelijktijdig muteren van hetzelfde veld door verschillende gebruikers niet toe. Bovendien dienen in de browser ingevoerde gegevens bewaard te blijven. In het geval van bijvoorbeeld inactiviteit of het tijdelijk wegvallen van de internetverbinding moet de hoeveelheid invoer die verloren gaat zo beperkt mogelijk zijn. Deze gegevens mogen niet in lokale bestanden of anderszins niet-vluchtige cache worden opgeslagen.

Gegevensuitwisseling

Het is cruciaal dat het Digitaal Dossier JGZ een veilige en betrouwbare uitwisseling van (medische) gegevens conform NEN 7512 waarborgt tussen ketenpartners en Opdrachtgever. Voor veilig e-mailverkeer is de norm [NTA 7516](#) van toepassing.

Back-up en recovery

Leverancier draagt zorg voor een periodieke (minimaal dagelijks) back-up van alle data en de mogelijkheid om deze in geval van calamiteiten te herstellen. Van belang is daarbij dat dit restoren op regelmatige basis (minimaal jaarlijks) aantoonbaar getest wordt. Back-ups moeten niet te wijzigen of te verwijderen zijn (immutable/WORM), zodat ransomware geen back-ups kan versleutelen of wissen. Back-ups dienen op meerdere, fysiek gescheiden locaties opgeslagen te worden (3-2-1-regel: drie kopieën, twee media, één offsite).

Disaster recovery

Leverancier moet een actueel en getest disaster recovery-plan hebben, inclusief procedures voor failover en failback, dat periodiek (minimaal jaarlijks) aantoonbaar getest wordt. Daarbij zijn er heldere afspraken gemaakt over maximale hersteltijd (RTO) en maximaal acceptabel dataverlies (RPO).

SaaS-beveiliging

In het kader van een veilige exploitatie van het nieuwe Digitaal Dossier JGZ als SaaS-oplossing zijn een aantal kritieke cybersecurityvoorzieningen gewenst:

- **Continue monitoring van gebruikers- en beheerdersactiviteiten:**
Alle relevante activiteiten, zoals inlogpogingen (succesvol en mislukt), wijzigingen in rechten, aanmaken/verwijderen van accounts, en verdachte downloads of dataverplaatsingen, moeten 24/7 worden gemonitord.
- **Real-time meldingen bij verdachte of risicovolle gebeurtenissen:**

De applicatiemonitoring genereert direct waarschuwingen bij bijvoorbeeld ongebruikelijke inloglocaties of -tijden, meerdere mislukte inlogpogingen gevolgd door een succesvolle login, onverwachte wijzigingen in toegangsrechten of configuraties, grote hoeveelheden data-export of -verwijdering, aanmaken van open of gedeelde links naar gevoelige data.

- **Automatische incidentrespons:**
Waar mogelijk moet het systeem automatisch kunnen reageren op kritieke incidenten, bijvoorbeeld door verdachte accounts tijdelijk te blokkeren of verdachte sessies te beëindigen.
- **Gedetailleerde logging en audit trails:**
Alle relevante gebeurtenissen moeten worden vastgelegd in logbestanden die minimaal 12 maanden bewaard blijven, zodat forensisch onderzoek mogelijk is.
- **Dashboards en rapportages:**
Opdrachtgever krijgt via dashboards of rapportages inzicht in de status en ontwikkeling van monitoring, incidenten en trends.
- **Integratie met SIEM/SOC-oplossing:**
Monitoring en meldingen zijn gekoppeld aan centrale security monitoring (SIEM/SOC) voor een geïntegreerd overzicht en snelle opvolging. Idealiter kan er gekoppeld worden met de SIEM/SOC-oplossing van Opdrachtgever voor een integrale beveiliging.
- **Regelmatige evaluatie en testen van monitoringprocessen:**
De effectiviteit van monitoring en meldingen moet periodiek worden getest en geëvalueerd, bijvoorbeeld via penetratietests of incident response-oefeningen.

2.3.3 KOPPELINGEN

Voor het Digitaal Dossier JGZ zijn op dit moment de volgende koppelingen/integraties voorzien. In de toekomst zullen mogelijk nog aanvullende koppelingen aan de orde zijn.

Koppeling	Type (koppeling, import, export)	Omschrijving
Basisregistratie Personen (BRP)	Import of koppeling	Minimaal noodzakelijk importmogelijkheden voor: • VO107 voor inlezen noodzakelijke BRP-gegevens • VO105 voor uitsturen terugmelding Wenselijk: koppeling voor inlezen noodzakelijke BPR-gegevens en uitsturen terugmeldingen.
Sectorale Berichtenvoorziening in de Zorg (SBV-Z)	Koppeling	Verificatie van het BSN en de adresgegevens.
MULTIsignaal	Koppeling	Inzicht in welke professionals bij een cliënt of gezin betrokken zijn, zodat zij beter kunnen samenwerken aan passende hulp en ondersteuning.
Vektis	Import of koppeling	Vektis beheert het AGB-register, een koppeling is wenselijk om AGB-register te kunnen gebruiken bij verwijzingen.
DUO Register Onderwijsdeelnemers	Import	Inlezen van ROD lijsten (scholen-/leerlingenlijsten) van DUO uit het Databuffet GGD GHOR t.b.v. het beheren en uitwisselen van onderwijsgegevens
Kadaster Landelijke Voorziening Basisregistratie Adressen en Gebouwen (LV BAG)	Koppeling	Stamtabel postcodes die actueel gehouden wordt, bij voorkeur beheerd door Leverancier
Centraal orgaan Opvang Asielzoekers	Import	Inlezen van COA-lijsten uit het Databuffet GGD GHOR t.b.v. het beheren en uitwisselen van gegevens over vluchtelingen/asielzoekers
ZorgMail	Koppeling	Minimaal: berichten ontvangen via ZorgMail. Wenselijk: berichten ontvangen en versturen via ZorgMail.

TABEL 2A: KOPPELVLAKKEN

Koppeling	Type (koppeling, import, export)	Omschrijving
ZorgDomein	Koppeling	Rechtstreeks verwijzen naar medisch specialisten via ZorgDomein en verwijzingen ontvangen vanuit ketenpartners via ZorgDomein.
NSDSK Centraal Administratiesysteem Neonatale Gehoorscreening (CANG)	Export, koppeling	Minimaal: dagelijkse export van nieuwgeborenen door Opdrachtgever die wordt ingelezen in CANG.
Het Landelijk Schakelpunt (LSP)	Koppeling	Aansluiting op LSP voor de uitwisseling van DOB-berichten voor dossieroverdracht en uitwisseling van rijksvaccinatieprogrammegegevens (RVP) en hieprikscreeningsgegevens (NHS) met RIVM.
TNO	Koppeling	Minimaal een koppeling met het I-JGZ-platform voor de groeidiagrammen. Wenselijk: daarnaast een koppeling met de slimme richtlijnmodule (SRM) voor beslissingsondersteuning van JGZ-professionals.
CareCodex Babyconnect	Koppeling	Veilige digitale uitwisseling van gegevens in keten van de geboortezorg ondersteunen zodra dit beschikbaar is.
I-JGZ	Koppeling	Mogelijkheid om aan te sluiten op het I-JGZ ICT-platform om eHealthmodules te kunnen gebruiken op het moment dat dit beschikbaar is.
Gezagsregister	Koppeling	Updates van gewijzigde gezagsverhoudingen ten aanzien van kinderen, zodat dossiers bijgewerkt kunnen worden en dossier al dan niet afgeschermd kunnen worden.
Zorgverzekeraars/intermediairs	Export, koppeling	Mogelijkheid om relevante kenmerken te kunnen toevoegen aan zorgtrajecten in dossiers en aan de hand hiervan exports te kunnen draaien of een koppeling te leggen met zorgverzekeraars en/of intermediairs (bijvoorbeeld Promeetec) ten einde zorg te kunnen declareren.

TABEL 2B: KOPPELVLAKKEN

Speelse dataverzameling	Koppeling	Ondersteuning voor andere manieren van dataverzameling náást handmatige invoer en vragenlijsten door bijvoorbeeld (serious) gaming.
-------------------------	-----------	---

TABEL 2C: KOPPELVLAKKEN

Het Digitaal Dossier JGZ voor GGD Zuid-Limburg, staat niet op zichzelf, maar ondersteunt professionals in een context van diverse uitvoeringsprocessen. De komende jaren zullen deze gegevensuitwisselingen steeds meer volgens standaarden worden ontwikkeld. Het Digitaal Dossier JGZ is zodanig voorbereid dat ketenpartners kunnen worden aangesloten via gestandaardiseerde gegevensuitwisseling. Het onderhouden van bestaande koppelingen met landelijke systemen en het doorvoeren van aanpassingen om nieuwe versies hiervan te ondersteunen valt onder de verantwoordelijkheid van Leverancier en brengen geen extra kosten voor Opdrachtgever met zich mee.

Zo is op termijn, na de implementatie, een integratie met bedrijfsvoeringsapplicaties, zoals financiële en tijdsregistratiesystemen of een ERP, te verwachten.

2.3.4 SPECIFIEKE FUNCTIONELE COMPONENTEN

Documenten

Het Digitaal Dossier JGZ beschikt over specifieke functionaliteiten rond documenten als uitnodigingen en verwijzingen. Denk aan documentbeheer, genereren output (digitaal of schriftelijk) aan de hand van een gestandaardiseerde opzet met sjablonen en het digitaal kunnen ondertekenen van documenten. Deze functionaliteiten kunnen middels een koppeling tot stand komen of geïntegreerd in de applicatie verweven zitten. Hier zijn enkele voorwaarden aan verbonden:

- Correspondentie over afspraken wordt zowel naar ouders en cliënt verstuurd als de cliënt jonger dan 16 is. Correspondentie wordt uitsluitend naar het adres van de cliënt verstuurd als deze 16 jaar of ouder is.
- Documenten kunnen centraal (bijvoorbeeld door de planning van het bedrijfsbureau) of decentraal (individuele medewerker) gegenereerd en verstuurd of geprint worden.
- Het is mogelijk om tussen verschillende in het Digitaal Dossier JGZ opgeslagen adressen te kiezen, er kan echter een standaardadres ingesteld worden.
- Het is mogelijk om variabelen/samenvoegvelden te gebruiken waarbij gegevens uit het Digitaal Dossier JGZ worden opgehaald en opgenomen in het document. Zo moeten ook documenten op basis van sjablonen automatisch gegenereerd kunnen worden met in het Digitaal Dossier JGZ beschikbare gegevens.
- Een verpleegkundige dient vanuit een arts gedelegeerd te kunnen verwijzen in het Digitaal Dossier JGZ.
- In sjablonen voor documenten kunnen het logo, correspondentieadres en handtekening van de locatie/medewerker die het document verstuurd worden opgenomen in combinatie met tekstenblokken die automatisch met de juiste data uit het Digitaal Dossier JGZ gevuld.
- Het aanmaken en opslaan van documenten moet direct vanuit de applicatie kunnen, met opslag terug in de applicatie, zonder tussentijdse lokale opslag of het downloaden door andere applicaties of de gebruiker. Dit geldt ook voor het invullen van formulieren en het ondertekenen.
- Een individueel document kan door een gebruiker op lay-out en inhoud gewijzigd worden, behoudens de huisstijl die in het betreffende sjabloon is vastgelegd.
- Bijlagen toevoegen moet mogelijk zijn.
- Ondertekenen moet digitaal mogelijk zijn naast handmatige handtekening in geval van een schriftelijke variant van een document.
- Verstuurde documenten kunnen, ook automatisch, aan een dossier worden toegevoegd.
- Gekoppelde documenten moet gelabeld kunnen worden om ze in een overzicht elders terug te kunnen zien, bijvoorbeeld in het kindbeeld.
- Titels van gekoppelde documenten moeten te wijzigen zijn.

Clïëntportaal

Clïënten - jeugdigen, volwassenen (ouders en aanstaande ouders)* - worden actief betrokken bij het proces en hun dossier. Via een cliëntportaal hebben cliënten toegang tot (delen van) het dossier, die zij zelf kunnen inzien. Het cliëntportaal is

beveiligde internetomgeving waar cliënten (kinderen en ouders) deels toegang krijgen tot het Digitaal Dossier JGZ. Dit cliëntportaal maakt logisch gezien onderdeel uit van het Digitaal Dossier JGZ. Het cliëntportaal biedt functionaliteit voor cliënten (kinderen), ouders en aanstaande ouders.

Het cliëntportaal maakt het voor cliënten mogelijk om op een gebruiksvriendelijke wijze specifieke onderdelen van hun eigen dossier of - als ouders - dat van hun kinderen in te zien:

- Een cliënt kan in het cliëntportaal de vaccinaties bekijken die in zijn dossier zijn vastgelegd.
- Een ouder kan in het cliëntportaal de vaccinaties raadplegen die in de dossiers van zijn kind(eren) zijn vastgelegd.
- Een client kan in het cliëntportaal de geplande en uitgevoerde afspraken in het dossier bekijken
- Een ouder kan in het cliëntportaal de geplande en uitgevoerde afspraken bekijken die de dossiers van zijn kind(eren) zijn vastgelegd.

De rechten van cliënten in het cliëntportaal moeten aansluiten op actuele wetgeving (12+ en 16+). Ouders van een kind krijgen via het cliëntportaal alleen toegang tot de gegevens die zijn vastgelegd in de dossiers van hun kind(eren) voordat de kinderen 12 jaar oud zijn geworden. Alleen wanneer het kind hiervoor toestemming heeft gegeven en dat zo geconfigureerd is, kan een ouder gegevens raadplegen die zijn vastgelegd nadat een kind ouder dan 12 jaar was of is.

Het cliëntportaal maakt het voor cliënten/ouders mogelijk om op een gebruiksvriendelijke wijze afspraken in te zien en te wijzigen of annuleren. Het is voor een client/ouder mogelijk om afspraken uit het verleden en voor de toekomst in te zien. Het overzicht van afspraken biedt een client/ouder helder en gestructureerd inzicht in de afspraken. Het toont in één oogopslag: de client (kind/ouder), de datum en tijd, de locatie. Als een client een contactmoment heeft gewijzigd via het cliëntportaal, wordt een bevestiging van de wijziging gestuurd naar de client.

Functioneel beheer kan instellen welke gegevens uit het dossier getoond worden in het cliëntportaal. Functioneel beheer kan daarnaast per type contactmoment instellen of een gebruiker van het cliëntportaal hiervoor wordt uitgenodigd en het geplande contactmoment kan verzetten of annuleren. Ook kan functioneel beheer bij elk type contactmomentregistratie een toelichting toevoegen (algemene informatie over het contactmoment) die zichtbaar is voor de ouder als er een contactmoment staat gepland voor dat type contactmomentregistratie. Functioneel beheer kan verder instellen dat een ouder het dossier van een kind kan toevoegen aan het cliëntportaal, mits de ouder daarbij actief bevestigt dat hij /zij het ouderlijk gezag heeft, aangeeft of er bezwaar is dat de andere ouder het dossier kan bekijken en dat de vragen naar waarheid zijn ingevuld. Tot slot kunnen hoofdgebruikers en functioneel beheerders de toegang tot het cliëntportaal blokkeren voor bepaalde kinddossiers voor een ouder (specifiek BSN).

Het cliëntportaal is bereikbaar via een eigen organisatie specifieke URL. Het gehele cliëntportaal voldoet aantoonbaar aan de WCAG 2.1 AA richtlijnen en overige wet- en regelgeving voor digitale toegankelijkheid. Het cliëntportaal is toegankelijk, bruikbaar en goed leesbaar op pc's/laptops, tablets en smartphones. Het cliëntportaal voldoet aan de huisstijl- en communicatie-eisen van GGD Zuid-Limburg.

* Waar hier wordt gesproken over ouders bedoelen wij aanstaande ouders en personen met het ouderlijk gezag conform de registratie in het BRP.

Vragenlijsten

Het Digitaal Dossier JGZ biedt een geïntegreerde oplossing voor vragenlijsten. De applicatie biedt opdrachtgever de mogelijkheid zelf vragenlijsten samen te stellen te en beheren. Bovendien biedt de applicatie de mogelijkheid om cliënten (via e-mail) uit te nodigen om een of meerdere vragenlijsten in te vullen en te versturen in een beveiligde online omgeving. De opmaak van de vragenlijsten dient te kunnen worden aangepast aan de huisstijl van GGD Zuid-Limburg.

De door cliënten ingevulde en verstuurd vragenlijsten worden automatisch in het Digitaal Dossier JGZ verwerkt en aan het dossier van de betreffende client toegevoegd. Deze vragenlijsten zijn dan bij een contactmoment zichtbaar en kunnen worden bewerkt door een zorgverlener.

Vragenlijsten moeten ook ingevuld kunnen worden door leerlingen in het voortgezet onderwijs. Bijvoorbeeld via een openbare url die, samen met voor elke leerling een unieke code om in te loggen en de vragenlijst in te vullen, gedeeld kan worden met de betreffende leerlingen.

In het Digitaal Dossier JGZ kunnen cliënten worden uitgenodigd voor afnemen van specifieke vragenlijsten op basis van door functioneel beheer in te stellen regels: school, klas, leeftijd, enzovoorts. Vragenlijsten die door cliënten zijn ingevuld en verzonden worden automatisch door het Digitaal Dossier JGZ ingelezen en verwerkt in het dossier van de cliënt.

De vragenlijsten kennen waar mogelijk controles en validaties tijdens het invullen om misverstanden en vergissingen te voorkomen. Bij voorkeur kunnen vragen automatisch secties overslaan of juist toevoegen indien van toepassing bijvoorbeeld op basis van geslacht of eerdere antwoorden. Ook zijn de vragenlijsten gebruiksvriendelijk en is het scrollen binnen de vragenlijsten zo beperkt mogelijk.

Planning

Het Digitaal Dossier JGZ moet op verschillende niveaus (kind-, team- of organisatieniveau) kunnen tonen:

- de nog in te plannen consulten,
- de beschikbare vrije roosterplekken binnen een opgegeven periode.

Het moet mogelijk zijn om meerdere kinderen tegelijk op één spreekuurmoment in te plannen (groepsplanning). Tevens moet het mogelijk zijn om meerdere consulten in één handeling te plannen, elk op een eigen tijdstip (bulkplanning).

Om afspraken te kunnen plannen, is het noodzakelijk dat het Digitaal Dossier JGZ werkt met roosters die een duidelijke begin- en eindtijd hebben. Binnen deze roosters moeten afspraken met verschillende duur ingepland kunnen worden. De duur van een consult is opgebouwd uit vaste tijdsblokken (bijvoorbeeld van vijf minuten), zodat het systeem flexibel om kan gaan met consulten van uiteenlopende lengtes.

Er kunnen meerdere roostersjablonen bestaan, omdat niet ieder type consult op elk rooster ingepland moet kunnen worden. Zo kan er een sjabloon zijn voor een vaccinatiespreekuur, waarin uitsluitend vaccinatieafspraken kunnen worden gepland. Tegelijkertijd moet dezelfde vaccinatieafpraak óók ingepland kunnen worden op een breder roostersjabloon, zoals een consultatiebureauspreekuur of een spreekuur voor de leeftijdsgroep 4-18.

Deze flexibiliteit in roosters en sjablonen is noodzakelijk om de diversiteit aan contactmomenten binnen de JGZ te kunnen faciliteren en om te zorgen dat afspraken altijd in een passend tijdslot en op een geschikte plek in het rooster terechtkomen.

2.3.5 TRAINING GEBRUIKERS EN BEHEERDERS

De onderstaande combinatie van e-learning, praktijktraining en documentatie waarborgt dat alle medewerkers goed toegerust zijn om veilig en vertrouwd met het nieuwe Digitaal Dossier JGZ te werken.

Leverancier zorgt voor een complete opleidingsomgeving die nieuwe medewerkers stapsgewijs wegwijs gemaakt kunnen worden in het Digitaal Dossier JGZ. Deze omgeving bevat bij voorkeur e-learningmodules die zijn afgestemd op verschillende disciplines, waaronder artsen, verpleegkundigen en assistenten. Deze modules bieden dan een walkthrough door de functionaliteit en worden actueel gehouden bij aanpassingen en nieuwe versies van de applicatie. De opleidingsomgeving werkt met fictieve data en heeft geen verbinding met externe systemen, zodat medewerkers veilig kunnen oefenen met alle functionaliteiten.

Bij de implementatie leidt de leverancier functioneel beheerders en hoofdgebruikers op, waarna GGD Zuid-Limburg zelfstandig de rest van de gebruikers kan trainen. Daarnaast ondersteunt de inschrijver bij het opleiden van de volledige gebruikersorganisatie.

Minstens 6 weken voor de livegang en minstens 2 weken voor elke nieuwe release in de toekomst levert de inschrijver een actuele, Nederlandstalige digitale gebruikershandleiding aan. Deze handleiding is aanpasbaar (bijvoorbeeld Word-document in plaats van PDF) zodat hoofdgebruikers en functioneel beheerders op basis van deze handleiding specifieke documentatie voor GGD Zuid-Limburg kunnen opstellen.

2.3.6 UITGANGSPUNTEN TEN AANZIEN VAN BEHEER

Ten aanzien van het beheer van het Digitaal Dossier JGZ gelden de volgende uitgangspunten:

- Leverancier voorziet in een OTAP-omgeving, die naast elkaar operationeel zijn, voor Opleiding (speeltuin), Test (op aanvraag), Acceptatie en Productie. De nadrukkelijke wens de beschikbaarheid van zogenaamde OTAP-omgevingen waarbij de Opleidingsomgeving een periodieke, op aanvraag te verversen geanonimiseerde kopie van productie is, de Acceptatieomgeving een vaste kopie van productie is waarbij updates de bestaande inrichting niet overschrijven en de Testomgeving wordt (kosteloos) maximaal twee keer per jaar op aanvraag beschikbaar is voor doorontwikkeling en de Productieomgeving altijd actueel en volledig beschikbaar is.
- In het datamodel van het Digitaal Dossier JGZ wordt onderscheid gemaakt tussen regio's, teams, medewerker, en functies.
- Het gemakkelijk kunnen filteren van data vanuit het pakket (bijvoorbeeld snel kunnen filteren op alle openstaande contactmomenten behorende bij team X en team Y).
- Tabellen in de beheeromgeving kunnen gebruiksvriendelijk worden beheerd (middels een logische structuur; met zo min mogelijk handelingen).
- De planningsmodule moet op een intuïtieve, logische en zo eenvoudig mogelijke manier kunnen worden beheerd.
- Sjablonen voor correspondentie en contactmomenten kunnen in de beheeromgeving gebruiksvriendelijk worden beheerd (op een intuïtieve, logische en zo eenvoudig mogelijke manier; met zo min mogelijk handelingen).
- Functioneel beheerders van Opdrachtgever kunnen zelf, zonder tussenkomst van Leverancier, contactmomenten inrichten voor hun eigen organisatie: naamgeving, opbouw, inhoud, tijdsduur en autorisatie, instellingen gekoppeld aan de planmodule, op welke locaties het contactmoment gebruikt wordt en aan welk BDS-moment het gekoppeld is.
- De mogelijkheid om specifieke items te kunnen definiëren (zoals bijvoorbeeld, asielzoeker, meerlingen, Oekraïne) die zichtbaar zijn op het kindbeeld.
- Vaccinatieschema's en importformulieren kunnen in de beheeromgeving gebruiksvriendelijk worden beheerd (op een intuïtieve, logische en zo eenvoudig mogelijke manier; met zo min mogelijk handelingen).
- Archiveren van dossier in bulk is mogelijk.
- Ten behoeve van planning, autorisaties en correspondentie dient Functioneel beheer van Opdrachtgever zelf gebruikers en teams (verzameling van medewerkers) aanmaken, muteren en deactiveren en kan medewerkers (gebruikers) groeperen in teams. Een medewerker kan deel uitmaken van meerdere teams. Aan een team kunnen meerdere medewerkers van eenzelfde discipline worden gekoppeld.
- In het Digitaal Dossier JGZ is het mogelijk voor functioneel beheerders niet-Basis Data Set registratie-items in te richten die voor gebruikers te gebruiken zijn in contactmomentregistraties.
- Het functioneel applicatiebeheer van de aangeboden oplossing moet eenvoudig en zelfstandig door Opdrachtgever gedaan kunnen worden zonder verplichte

ondersteuning door Leverancier en de inrichting kan door functioneel applicatiebeheer zelf worden uitgevoerd, waar nodig in samenspraak met en ondersteund door Leverancier.

- Idealiter kan functioneel beheer kan registratie-items verplicht stellen.
- Beheerfuncties zijn aanwezig voor alle stamgegevens, zoals medewerkers, locaties, scholen, gemeenten, postcodes (landelijke postcodetabellen, up to date gehouden door leverancier), werkgebieden, zorgverleners, enz.
- Op basis van postcode worden cliënten automatisch aan een door organisatie aan te geven werkgebied/locatie gekoppeld behalve bij schoolgaande kinderen, die moeten op basis van school gekoppeld worden aan het bijbehorende team.
- Er is bij Leverancier één door Leverancier beheerd en beschikbaar gesteld incidentsysteem waar known bugs en RFC's in worden geregistreerd. Het incidentsysteem moet voor Opdrachtgever inzichtelijk zijn met minimaal de volgende velden: omschrijving, indiener (kan ook een andere organisatie zijn), classificatie, impact, status, datum van indienen en eventuele release waarop dit staat ingepland. Het incidentsysteem heeft een zoekfunctie en biedt inzicht in de historie.
- Functioneel beheer van Opdrachtgever heeft te allen tijde inzicht in uitstaande incidenten en supportaanvragen.

2.3.7 DATAMANAGEMENT

GGD Zuid-Limburg wil graag inzicht in de data in het Digitaal Dossier JGZ om op basis hiervan te kunnen sturen. Om deze data via het eigen data warehouse van Opdrachtgever te kunnen ontsluiten en verwerken verwachten we dat de data op een structurele en gestructureerde wijze wordt aangeleverd. Bij voorkeur loopt dit via een API waarbij op elk willekeurig moment een data-aanvraag gedaan kan worden. Mocht dit niet mogelijk zijn verwachten we minimaal een dagelijkse aanlevering van data in een gangbaar en voor Opdrachtgever werkbaar en acceptabel formaat. Dit betekent dat:

- Van Leverancier wordt verwacht dat alle gegevens die worden verwerkt en opgeslagen in het informatiesysteem volledig, ongefilterd en onbewerkt beschikbaar worden gesteld voor onder meer managementinformatie doeleinden met rapportagetools naar eigen keuze van Opdrachtgever.
- Deze gegevens zullen periodiek beschikbaar gesteld worden aan de Opdrachtgever met een minimaal dagelijkse frequentie. Data zal worden aangeleverd op een geautomatiseerde manier, denk hierbij aan een API, databaseconnectie, structurele exports of een dump van het bronsysteem. Het format waarin de data worden aangeleverd is in een van de volgende soorten: csv/txt, json, xml, sql.

2.3.8 DATACONVERSIE/-MIGRATIE

Leverancier verzorgt de conversie en migratie van alle dossiers, in en uit zorg, uit het huidige Digitaal Dossier JGZ naar het nieuw Digitaal Dossier JGZ conform de voorafgaand aan de implementatie gezamenlijk verder uit te werken aanpak. Hierbij hanteert Leverancier de volgende uitgangspunten:

- In de basis worden alle velden meegenomen in migratie en wordt er een mapping voorzien op veldniveau, waardoor alle items op de juiste plek in het nieuwe dossier terechtkomen. BDS-items, maar ook andere items.
- Correspondentie en documenten uit het oude dossier komen in het nieuwe dossier op de daarvoor bestemde plek terecht.
- Ook vaccinatieschema's, toestemmingen, Van Wiechen-items en items die horen onder 'Info werkwijze JGZ' worden correct gemigreerd/geconverteerd naar het nieuwe Digitaal Dossier JGZ.
- De gegevens opgeslagen in het kader van het DMO-taxatiemodel worden overgezet in de vorm van een aparte PDF die als document aan het dossier gekoppeld wordt.
- De vragenlijsten en hun antwoorden worden eveneens mee overgenomen naar op de juiste plek in het nieuwe dossier overgezet.

Leverancier is verantwoordelijk voor de kwaliteit (volledigheid, correctheid, tijdigheid en consistentie) van de dataconversie van alle dossiers. Leverancier controleert aantoonbaar de betrouwbaarheid van de gegevens in het Digitaal Dossier JGZ en stelt ook Opdrachtgever in staat om dit op een eenvoudige manier te controleren. Leverancier zet in het implementatieplan uiteen hoe de kennis en capaciteit voor de dataconversie geborgd is.

Leverancier dient daarnaast een plan in voor en werkt mee aan de overdracht van informatie en data aan een eventuele volgende leverancier aan het eind van de overeenkomst. Hierin dient o.a. te zijn beschreven hoe:

- Hoe de overdracht van het Digitaal Dossier JGZ en alle data naar een volgende leverancier gewaarborgd wordt ten einde een probleemloze voortzetting van de dienstverlening mogelijk te maken.
- Hoe de migratie van de gegevens verloopt, inclusief een uitleg over het gegevensmodel, zodat Opdrachtgever en de volgende leverancier begrijpen hoe het datamodel in elkaar zit.
- Hoe de geheimhouding ten aanzien van de privacy van gebruikers en deelnemers na overdracht van de informatie en data aan een volgende leverancier is gewaarborgd. Komen de gegevens in het bezit van GGD Zuid-Limburg na of wordt er een garantie gegeven dat deze worden vernietigd? In dat laatste geval beschrijft Leverancier hoe de vernietiging van gegevens wordt aangetoond.
- Hoe Leverancier vervolgens zorg draagt voor de vernietiging van de gegevens de gebruikte test-, acceptatie en productieomgeving en de back-ups.

2.3.9 TECHNISCHE WERKOMGEVING

Deze paragraaf beschrijft globaal de technische werkomgeving van GGD Zuid-Limburg. Deze beschrijving is bewust globaal, omdat het nieuwe Digitaal Dossier JGZ als SaaS-dienst wordt afgenomen. Dit stelt immers slechts beperkt eisen aan technische werkomgeving. Kenmerken van technische werkomgeving kunnen echter wel relevant zijn in verband met (applicatie)koppelingen.

De technische werkomgeving van GGD Zuid-Limburg ziet er als volgt uit. Medewerkers maken gebruik van HP Elitebook laptops voorzien van Microsoft Windows 11, met Microsoft Edge als standaardbrowser. De standaard GGD Zuid-Limburg heeft als beleid dat iedereen locatie-onafhankelijk moet kunnen werken en dus beschikking krijgt over een laptop en mobiele telefoon.

2.3.10 DIMENSIONERING IN KADER VAN PERFORMANCE

Bij de dimensionering van het Digitaal Dossier JGZ moet (in het kader van het borgen van een goede performance) rekening gehouden worden met de volgende kentallen:

Totaal aantal dossiers in het huidige systeem Topicus KD+: ongeveer **275.000**, waarvan ruim **105.000** actief.

Totaal aantal gebruikers: ongeveer **250**.

Bijlage

AANSLUITVOORWAARDEN GGD ZUID-LIMBURG

Authenticatie en autorisatie

- De applicatie faciliteert authenticatie door middel van de combinatie gebruikersnaam/wachtwoord + Token.
- De applicatie kan gebruik maken van Single of Same Sign On (SSO) op basis van het OIDC protocol of het OAuth2 protocol. De gebruiker authenticatieert zich hiermee conform de Identity Access Management (IAM) oplossing van GGD Zuid-Limburg. De gebruiker kan hiermee inloggen met de netwerk inlognaam en wachtwoord en token.

Transportbeveiliging

- Bij koppelingen (in- en uitgaand) biedt de applicatie een mechanisme om het datatransport te versleutelen (bijvoorbeeld SSL/TLS).
- Bij systeemkoppelingen (in- en uitgaand) vindt er wederzijds systeemauthenticatie plaats door middel van certificaten ('Two Way SSL').

Databeveiliging

- De data van de SaaS-oplossing wordt gehost in landen binnen de Europese Economische Ruimte (EER). Bij voorkeur niet (meer) in Groot-Brittannië.
- Toegang tot de SaaS-oplossing via een Internet Browser vindt versleuteld plaats ('https') met TLS1.2 of hoger voorzien van een Extended Validation (EV) SSL-certificaat.

Applicatiestandaarden

- De leverancier moet voldoen aan NCSC-beveiligingsrichtlijnen voor webapplicaties. <https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html>
- De applicatie voldoet aan de meest actuele OWASP-richtlijnen: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.
- De applicatie is benaderbaar via een zogenaamde 'Fully Qualified Domain Name (FQDN)'.
- Voor de webbrowsers dienen de twee laatste versies van de meest gebruikte desktopbrowsers (Chrome, Edge, Firefox) en mobiele browsers (Chrome, Safari) ondersteund te worden.
- Voor apps geldt dit voor de laatste twee major versies van iOS en Android.
- Het Digitaal Dossier JGZ voldoet aantoonbaar aan actuele webstandaarden en functioneert correct in de genoemde webbrowsers.
- Voor het functioneren van de webapplicatie op het client device zijn geen verdere instellingen, dan wel installaties benodigd. De webapplicatie maakt geen gebruik van plug-in componenten (zoals o.a. Microsoft Active X, Microsoft Silverlight,

Microsoft ClickOnce, Adobe Flash en Java plug-in). Dit geldt zowel voor het client device als ook in de browser.

- Afwijkingen voor wat betreft instellingen en installaties (uitgezonderd plug-in componenten) kunnen in overleg worden toegestaan voor devices van (functioneel) beheerders.
- Het is mogelijk dat alle rollen (medewerker, leidinggevende, professional en functioneel beheerder) via een Internetbrowser, zonder additionele plug-ins of andere software, gebruik kunnen maken van de SaaS-applicatie. De SaaS-applicatie is voor deze rollen een 'Zero Footprint' webapplicatie.
- De applicatie mag geen (backchannel) interactie met overige applicaties binnen de GGD-infrastructuur toestaan behalve wanneer deze internet enabled API's hanteren.

Connectiviteitsstandaarden

- Voor nieuwe koppelingen tussen de SaaS-oplossing en GGD-systemen, Richting: van de SaaS-oplossing naar een GGD-systeem / van een GGD-systeem naar de SaaS-oplossing, Batch/Realtime: Batch/Scheduled en/of Realtime, Transport/Bestandsformaat: Data uitwisseling via REST / SOAP over HTTPS of bestandsuitwisseling via SFTP, FTPS of HTTPS. XLSX, JSON, CSV, XML, Beveiliging: Gebruikersnaam + wachtwoord + Certificaat, Gebruikersnaam + wachtwoord, SAML 2.0 / Two Way SSL
- Voor koppelingen, integratie, import en export vindt data uitwisseling plaats via bestanden en protocollen die voorkomen in de lijst van open standaarden (<https://www.forumstandaardisatie.nl/open-standaarden>).
- De leverancier zorgt voor de complete implementatie (technisch en functioneel) van koppelingen met andere SaaS leveranciers. GGD Zuid-Limburg stelt daarbij de informatiebeveiligingskaders vast. Het gaat hier om de bestaande en in de toekomst nog aan te leggen koppelingen met andere SaaS-leveranciers.