Woo-verzoek inzake datadiefstal CoronIT – deelbesluit 2

Op 15 februari 2022 kreeg elke GGD een Wob-verzoek (vanaf 1 mei 2022 heet dit een Wet Open Overheid-verzoek) naar aanleiding van de datadiefstal uit CoronIT. Veiligheidsregio Limburg-Noord heeft dit Wob-verzoek eveneens ontvangen.

In dit bestand zijn vanaf 6 juli 2022 de documenten behorende tot 'deelbesluit 2' in te zien.

veiligheidsregio
limburg-noord

Postbus 11
5900 AA Venlo
088 - 11 90 000
info@vrln.nl
www.vrln.nl

SOLV Advocaten
[redacted]

datum	5 juli 2022	**behandeld door**	[redacted]
uw kenmerk		**telefoonnummer**	[redacted]
ons kenmerk	[redacted]	**bijlage(n)**	9

onderwerp Tweede deelbesluit inzake wob/woo-verzoek namens [redacted]

Geachte [redacted]

Veiligheidsregio Limburg-Noord (namens GGD Limburg-Noord) heeft, in reactie op uw brief van 15 februari 2022, namens uw cliënt, [redacted] op 1 juni 2022 een deelbesluit genomen en daarbij horende documenten openbaar gemaakt. In aanvulling op de reeds openbaar gemaakte documenten, verstrekt Veiligheidsregio Limburg-Noord u hierbij, middels dit tweede en tevens laatste deelbesluit, ook de documenten inzake "GGD Contact". Veiligheidsregio Limburg-Noord verwijst u naar de inventarislijst als bedoeld in "bijlage 1" horende bij dit tweede deelbesluit voor het overzicht van de documenten inzake "GGD Contact".

Voor de goede orde merken wij op dat wij u per e-mail van 7 april 2022 en middels het besluit van 1 juni 2022 kenbaar hebben gemaakt dat de correspondentie, naar aanleiding van uw brief van 15 februari 2022, namens de GGD Limburg-Noord wordt behandeld door de publiekrechtelijke rechtspersoon waar de GGD Limburg-Noord integraal onderdeel van uitmaakt, te weten: Veiligheidsregio Limburg-Noord.

1. Wettelijk kader

Op 1 mei 2022 is de Wet open overheid in werking getreden. Op diezelfde datum is de Wob ingetrokken. Voor de passieve openbaarmakingsplicht, zoals aan de orde in het onderhavige geval, bevat de Woo geen overgangsrecht. Het verzoek van [redacted] en de behandeling daarvan vallen daarmee onder de reikwijdte van de Woo. Het wettelijk kader van de Woo is te raadplegen via:
https://wetten.overheid.nl/BWBR0045754/2022-05-01

2. Inventarisatie documenten

Bij dit deelbesluit worden 8 documenten (gedeeltelijk) openbaar gemaakt. Deze documenten staan in de inventarislijst die wij als "bijlage 1" bij dit besluit hebben

gevoegd. Voor zover wij besloten hebben om delen van documenten niet of gedeeltelijk openbaar te maken, hebben wij in de inventarislijst aangegeven wat daarvoor de toepasselijke uitzonderingsgrond uit de Woo is.

3. Zienswijzen

U bent op 7 april 2022 per e-mail en in het besluit van 1 juni 2022 geïnformeerd dat er derde-belanghebbenden zijn bij de openbaarmaking van de documenten en dat deze in de gelegenheid zijn gesteld hierop hun zienswijze te geven. De zienswijze van deze partijen hebben wij meegenomen in onze belangenafweging. Zie het onderdeel 'Overwegingen' onder 5. van dit besluit.

Door derde-belanghebbenden zijn voor het overige geen bedenkingen ingediend.

4. Besluit

Wij hebben besloten om de documenten waar u, namens [redacted] om heeft verzocht, (gedeeltelijk) openbaar te maken. Wij verwijzen hiertoe kortheidshalve naar de inventarislijst (bijlage 1), waarop per document is aangegeven of informatie openbaar of gedeeltelijk openbaar is gemaakt. Voor zover informatie niet of niet volledig openbaar is gemaakt, is in de inventarislijst aangegeven welke uitzonderingsgrond van toepassing is.

Voor de motivering van het besluit verwijzen wij naar het onderdeel 'Overwegingen' onder 5. van het besluit.

5. Overwegingen

Op basis van artikel 4.1, zevende lid van de Woo wordt een verzoek om informatie ingewilligd met toepassing van het bepaalde in hoofdstuk 5 van de Woo, waaronder artikel 5.1.

Het recht op openbaarmaking op grond van de Woo dient het publieke belang van een goede en democratische bestuursvoering. Het komt een ieder in gelijke mate toe. Ten aanzien van de openbaarheid kan derhalve geen onderscheid worden gemaakt naar gelang de persoon, bedoeling of belangen van de verzoeker. Bij de in dit besluit verrichte belangenafwegingen worden dan ook slechts het algemeen belang bij openbaarmaking van de gevraagde informatie en de door de weigeringsgronden te beschermen belangen betrokken.

In het algemeen willen wij nog opmerken dat wij in het kader van de Woo referentie- en kenmerknummers uit documenten hebben verwijderd om misbruik hiervan te voorkomen.

5.1 Economische en financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen (artikel 5.1 lid 2 sub b)

Op grond van artikel 5.1, tweede lid, aanhef en onder b, van de Woo blijft verstrekking van informatie achterwege voor zover het belang daarvan niet opweegt tegen de economische of financiële belangen van de Staat. Bij een passage uit het document met nummer 1.1 is het financiële/economische belang van de Staat in het geding. Deze passsage is gelakt. Wij zijn van oordeel dat dit belang zwaarder moet wegen dan het

belang van openbaarheid, aangezien dit inzicht geeft in de wijze waarop de Staat economisch opereert. De financiële belangen van de Staat worden geschaad als bijvoorbeeld bekend wordt op welke wijze de Staat invulling geeft aan de wijze waarop wordt omgegaan met aansprakelijkheid in een overeenkomst en welke bedragen daarbij van toepassing zijn. Het belang van openbaarmaking van dergelijke bepalingen weegt niet op tegen deze belangen.

Openbaarmaking van de betreffende financiële gegevens zou de onderhandelingspositie van de Staat in de toekomst ernstig verslechteren, omdat marktpartijen hierop hun prijzen en onderhandelingsstrategie in toekomstige projecten en aanbestedingen zouden kunnen aanpassen. Daarnaast leidt inzicht in dergelijke bepalingen ertoe dat (potentiële) contractpartners exact zullen weten onder welke omstandigheden de Staat bereid is contracten aan te gaan.
Wij zijn van oordeel dat voornoemde belangen zwaarder wegen dan het belang van openbaarmaking en besluiten daarom de desbetreffende informatie niet openbaar te maken.

5.2 Eerbiediging van de persoonlijke levenssfeer (artikel 5.1 lid 2 sub e)

Op grond van artikel 5.2, tweede lid, aanhef en onder e van de Woo blijft verstrekking van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang dat de persoonlijke levenssfeer wordt geëerbiedigd. In vrijwel alle documenten staan persoonsgegevens. Hiervoor verwijzen wij naar hetgeen vermeld op de inventarislijst. Het betreft gegevens zoals namen, initialen, emailadressen, telefoonnummers, functieomschrijvingen en datum in dienst- en uitdiensttreding en andere tot personen herleidbare informatie. Wij zijn van oordeel dat ten aanzien van deze gegevens het belang dat de persoonlijke levenssfeer wordt geëerbiedigd, zwaarder moet wegen dan het belang van openbaarheid. Daarom hebben wij de persoonsgegevens verwijderd uit deze documenten.

In veel documenten staan tevens persoonsgegevens van ambtenaren die uit hoofde van hun functie niet in de openbaarheid treden. In het kader van goed werkgeverschap is Veiligheidsregio Limburg-Noord van oordeel dat ten aanzien van deze gegevens het belang dat de persoonlijke levenssfeer wordt geëerbiedigd, zwaarder moet wegen dan het belang van openbaarheid. Dit ter bescherming van de persoonlijke levenssfeer van de betrokken ambtenaar. Daarbij is van belang dat het hier niet gaat om het opgeven van een naam aan een individuele burger die met een ambtenaar in contact treedt, maar om openbaarmaking van de naam in de zin van de Woo. Deze gegevens hebben wij daarom ook uit de documenten verwijderd.

6. Wijze van openbaarmaking

Alle documenten, met uitzondering van de reeds openbaar gemaakte en de niet openbaar gemaakte documenten, worden tezamen met dit besluit (geanonimiseerd) en bijbehorende bijlagen op onze website geplaatst. De documenten zijn te raadplegen via de volgende link: https://vrln.nl/over/beleid en kunnen worden gedownload.

veiligheidsregio
limburg-noord

7. Contactpersoon

Op grond van artikel 4.7 Woo dient een contactpersoon te worden aangewezen aan wie vragen over de beschikbaarheid van publieke informatie kan worden gesteld. Binnen onze organisatie is de heer [redacted] aangewezen als contactpersoon, die bereikbaar is via de onderstaande contactgegevens:

[redacted]

Wij hebben uw verzoek, namens [redacted] van 15 februari 2022 met de grootst mogelijke zorgvuldigheid uitgevoerd. Mocht [redacted] desondanks menen dat er documenten ontbreken, dan vernemen wij dat graag. U kunt daartoe contact opnemen met onze contactpersoon door middel van bovengenoemde contactgegevens.

8. Bezwaar

Op grond van de Algemene wet bestuursrecht kan een belanghebbende tegen dit besluit binnen zes weken na de dag waarop dit is bekendgemaakt een bezwaarschrift indienen. Het bezwaarschrift moet worden gericht aan het dagelijks bestuur van Veiligheidsregio Limburg-Noord, postbus 11, 5900 AA Venlo. Het bezwaarschrift dient te zijn ondertekend en ten minste te bevatten:

a. naam en adres van de indiener;
b. de dagtekening;
c. een omschrijving van het besluit waartegen het bezwaarschrift zich richt (datum en nummer of kenmerk);
d. een opgave van de redenen waarom indiener het niet eens is met het besluit.

Met vriendelijke groet,

Namens het dagelijks bestuur van de Veiligheidsregio Limburg-Noord.

[redacted]

Bijlage 1 Inventarislijst

Nummer document	Naam document	Document verstrekt: ja / nee / gedeeltelijk.	Indien niet verstrekt: Uitzonderingsgrond uit de Woo Indien reeds verstrekt: Wijze van openbaarmaking
1.0	DVO GGD Contact – GGD Limburg Noord	Gedeeltelijk	Artikel 5.1 lid 2 sub e Woo
1.1	Verwerkersovereenkomst – GGD Limburg Noord – de Staat	Gedeeltelijk	Artikel 5.1 lid 2 sub b Woo Artikel 5.1 lid 2 sub e Woo
2.0	DVO GGD GHOR Nederland – GGD generieke ICT-diensten t.b.v. GGD Contact	Gedeeltelijk	Artikel 5.1 lid 2 sub e Woo
2.1	Dienstbeschrijving GGD GHOR Nederland – GGD Generieke ICT-diensten t.b.v. van GGD Contact	Gedeeltelijk	Artikel 5.1 lid 2 sub e Woo
2.2	Service Level Agreement GGD GHOR Nederland – GGD Generieke ICT-diensten ten behoeve van GGD Contact	Gedeeltelijk	Artikel 5.1 lid 2 sub e Woo
2.3	Dossier Afspraken en Procedures GGD GHOR Nederland – GGD generieke ICT-diensten ten behoeve van GGD Contact Versie: 1.1	Gedeeltelijk	Artikel 5.1 lid 2 sub e Woo
2.4	Verwerkersovereenkomst GGD Limburg-Noord – GGD GHOR Nederland	Gedeeltelijk	Artikel 5.1 lid 2 sub e Woo
2.5	Checklist Onboarding Applicaties	Gedeeltelijk	Artikel 5.1 lid 2 sub e Woo

Dienstverleningsovereenkomst Ministerie van Volksgezondheid, Welzijn en Sport en GGD Limburg Noord

Betreft: Dienstverlening GGD Contact

Datum: 07 09 2021
Status: Definitief

Colofon

Afzendgegevens: Ministerie van Volksgezondheid, Welzijn en Sport

[redacted]

Contactpersoon: [redacted]

Inhoudsopgave

Versiebeheer 5

1 Algemeen 6

1.1 Dienstverlening 6

1.2 Looptijd 6

1.3 Wijzigingen document 6

1.4 Gerelateerde documenten 6

1.5 Beëindiging 6

2 Dienstverlening 7

2.1 Algemene beschrijving dienstverlening 7

2.2 Niveau van dienstverlening 7

A. Rolverdeling AVG 7

B. Bereikbaarheid 7

C. Beschikbaarheid 7

D. Correctief onderhoud 8

E. Incidentmanagement 8

F. Change- en releasemanagement 9

G. Continuïteitsmanagement 9

3 Beveiliging 11

3.1 Van toepassing zijnde kaders 11

3.2 Logging en monitoring 11

3.3 Beveiliging afnemer 11

4 Verantwoordelijkheden 12

4.1 Verantwoordelijkheden VWS 12

4.2 Verantwoordelijkheden GGD 12

5 Communicatie 13

5.1 Rapporteren 13

5.2 Overlegvormen 13

6 Tekenblad 14

De ondergetekenden

1. de publiekrechtelijke rechtspersoon: **de Staat der Nederlanden (Ministerie van Volksgezondheid, Welzijn en Sport)**, hierna te noemen: VWS,

en

2. de **Gemeentelijke Gezondheidsdienst GGD Limburg-Noord**, gevestigd te Blerick aan de Drie Decembersingel 50, ingeschreven in het handelsregister onder KvK nummer [redacted], hierna eveneens te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted]

De partijen bij deze dienstverleningsovereenkomst ("**DVO**") worden hierna gezamenlijk ook aangeduid als "**de Partijen**" en ieder als een "**Partij**".

Versiebeheer

Versie	Datum	Auteur	Omschrijving
0.1	26-05-2021	[redacted]	Initiële versie
0.2	28-05-2021	[redacted]	Eerste review RDO verwerkt
0.3	04-06-2021	[redacted]	Aanvullingen en review verwerkt
0.4	09-06-2021	[redacted]	Aanvullingen en review van GGD GHOR verwerkt
0.5	14-06-2021	[redacted]	Aanvullingen en review [redacted] verwerkt
0.6	15-06-2021	[redacted]	Review
0.9	15-06-2021	[redacted]	Review verwerkt
0.99	23-06-2021	[redacted]	Review Stuurgroep verwerkt
1.0	23-06-2021	[redacted]	Final Review

1 Algemeen

In deze Dienstverleningsovereenkomst (DVO) komen VWS en GGD de mate van dienstverlening van GGD Contact overeen.

1.1 Dienstverlening

Het doel van de dienstverlening is de GGD te ondersteunen in het Bron- en Contact Onderzoek (BCO) met het leveren, beheren en door ontwikkelen van de applicatie GGD Contact. Dit is de voorziening die het Bron- en Contact Onderzoek voor COVID-19 gerelateerd ondersteunt.

1.2 Looptijd

Deze DVO treedt in werking op 2 september 2021 en wordt aangegaan voor onbepaalde tijd.

1.3 Wijzigingen document

Het actueel houden van dit document is belegd bij [redacted] van het ministerie VWS. Bij partijen kan de wens ontstaan om dit document te wijzigen. In gezamenlijk overleg wordt de wijziging vervolgens bepaald.

- Overeengekomen wijzigingen worden vastgelegd in een wijzigingsblad;
- Dit wijzigingsblad wordt door beide partijen formeel ondertekend en als addendum toegevoegd;
- De in het addendum opgenomen afspraken worden in de eerstvolgende geactualiseerde versie van de DVO opgenomen.
- De bijlagen in dit document kunnen na en in onderling overleg tussentijds worden geactualiseerd. Het tast de rechtmatigheid van de afspraken in dit document niet aan.

1.4 Gerelateerde documenten

De volgende documenten zijn gerelateerd aan deze DVO:

- Procedurebeschrijving beheer GGD Contact (bijlage 1)
- Verwerkersovereenkomst VWS – GGD (bijlage 2)
- Beveiliging GGD Contact release X (bijlage x) wordt vertrouwelijk gedeeld onder TLP:Amber classificatie (need to know basis).
- Landelijke Referentie DPIA GGD Contact
- Lijst Overeenkomsten GGD Contact

Van de gerelateerde documenten kunnen in de loop van de tijd nieuwe versies bestaan. Sommige documenten worden zelfs elke release geüpdatet. Dit heeft geen gevolgen voor de geldigheid van deze DVO.

1.5 Beëindiging

Het verzoek van een van de partijen om de DVO te beëindigen vindt schriftelijk plaats met opgave van de reden. Partijen hanteren een opzegtermijn van drie maanden en treden met elkaar in overleg over de wijze van beëindiging.

2 Dienstverlening

2.1 Algemene beschrijving dienstverlening

De te leveren dienstverlening omvat GGD Contact: het leveren, doorontwikkelen en beheren van de voorziening die de behandeling voor COVID-19 gerelateerd Bron- en Contact Onderzoek (BCO) ondersteunt.

2.2 Niveau van dienstverlening

Deze paragraaf beschrijft de specifieke afspraken voor de dienstverlening die door het ministerie wordt geleverd aan de GGD. Voor de dienstverlening levert het ministerie Applicatie- en Technisch beheer.

Aangezien de omvang en inzet van het Bron- en Contact Onderzoek (BCO) varieert op basis van het aantal COVID-19 besmettingen, kan de gewenste dienstverlening ook fluctueren. VWS zal driemaandelijks beoordelen of de dienstverlening nog past bij het gebruik van de applicatie en waar opportuun een voorstel doen voor aanpassing van de dienstverlening om zo kosteneffectief GGD Contact aan te kunnen bieden.

A. Rolverdeling AVG

De feitelijke rolverdeling tussen GGD en VWS is bepalend voor de verantwoordelijkheden van GGD en VWS zoals die volgen uit de Algemene Verordening Gegevensbescherming (AVG). De rolverdeling is vastgesteld in de referentie DPIA GGD Contact behorend bij de release. De referentie DPIA is afgestemd met de GGD en VWS.

GGD stemt in met alle (sub)verwerkers die VWS voor haar dienstverlening inschakelt, waarbij VWS zorgdraagt voor de verwerkersovereenkomsten. De lijst met (sub)verwerkers is beschreven in Lijst Overeenkomsten GGD Contact. Deze is opgenomen als bijlage bij deze DVO.

B. Bereikbaarheid

De servicedesk GGD GHOR is het centrale loket voor alle verzoeken en meldingen rondom GGD Contact. De GGD sluit een overeenkomst die ingaat op het moment van ingebruikname van GGD Contact.

C. Beschikbaarheid

Beschikbaarheid is de tijd dat de dienstverlening onder verantwoordelijkheid van VWS, voor eindgebruikers beschikbaar is. Gepland onderhoud valt buiten de berekening van de gerealiseerde beschikbaarheid. Ook de uitval van een tussenliggende component die niet onder verantwoordelijkheid van VWS valt, zoals generieke ICT-diensten geleverd door GGD (o.a. IdentityHub en een VPN - verbinding), waardoor de systemen voor gebruikers niet beschikbaar zijn, valt hierbuiten.

Per incident (dat leidt tot onbeschikbaarheid) gelden bovendien maximale hersteltijden. Deze zijn opgenomen onder de paragraaf incidentmanagement.

Onderwerp	Toelichting	Norm
Beschikbaarheid	De mate waarin de eindgebruikers GGD Contact functioneel kunnen gebruiken binnen het servicevenster. Onbeschikbaarheid wordt gemeten vanaf het moment van melden door servicedesk aan de Incidentmanager VWS.	Minimaal 99,8% binnen het servicevenster

D. Correctief onderhoud

Correctief onderhoud aan GGD Contact (geplande onbeschikbaarheid) wordt enkel uitgevoerd buiten het servicevenster als opgenomen in paragraaf E van deze DVO. Correctief onderhoud wordt bij voorkeur drie weken van tevoren en uiterlijk drie dagen van tevoren gemeld aan de servicedesk. De servicedesk is vervolgens verantwoordelijk voor de communicatie naar de eindgebruikers en afnemers toe. Bij een dreigende verstoring moet er soms direct ingegrepen worden, daarvoor geldt onderstaande norm.

Onderwerp	Toelichting	Norm
Onderhoud	Het benodigde onderhoud om de beschikbaarheid te kunnen garanderen.	90% buiten het Servicevenster

E. Incidentmanagement

Het incidentmanagementproces heeft als doel het zo snel mogelijk verhelpen van incidenten. De doelstelling is het terugbrengen van de dienstverlening naar het normale niveau, met zo min mogelijk gevolgen in de vorm van impact, benodigde mensen, middelen (financieel & materieel) en tijd. Het incidentmanagementproces staat uitgebreid beschreven in Bijlage 1 Procedurebeschrijving beheer GGD Contact. Onderstaand een overzicht van de gehanteerde normen.

Onderwerp	Toelichting	Norm[1]
Incidentmelding (storing)	De afhandeling van aangemelde verstoringen tijdens het servicevenster. Toewijzing prioriteit vindt plaats op basis van de prioriteitenmatrix (zie hiervoor de procedurebeschrijving). NB Responstijd en doorlooptijd 1ste lijn zijn onderdeel van de afspraken GGD GHOR SD met de GGD.De hersteltijd 2e lijn start na ontvangst van het incident van de Servicedesk door de tweede lijn	P1 Hersteltijd 2e lijn: 4 uur Servicevenster: 7*16u** P2 Hersteltijd 2e lijn: 1 dag Servicevenster: 7*16u** P3 Hersteltijd 2e lijn: 1 week Servicevenster: 7*16u** P4 Hersteltijd 2e lijn: 2 weken Servicevenster: 7*16**

[1] Dit is conform de standaardnormen van de GGD GHOR servicedesk

	Afhandeling buiten servicevenster	Alleen bij P1

** Ten tijde van een hoge infectiedruk wordt het servicewindow opgerekt van 5 x 9 (8.00 – 17.00 uur) naar 7 x 16 (7.00 – 23.00 uur).

Prioriteitenmatrix

Tijdens het aannemen van een incidentmelding door de servicedesk, wordt met de aanmelder een inschatting van de ernst (impact en urgentie) van het incident gemaakt. Op basis daarvan wordt door de servicedeskmedewerker de prioriteit vastgesteld, geregistreerd en afgehandeld.

In de Procedurebeschrijving beheer GGD Contact (bijlage 1) is de prioriteitenmatrix opgenomen.

F. Change- en releasemanagement

Change- en releasemanagement is het proces rondom het gecontroleerd afhandelen van verzoeken tot wijziging van de functionele of technische werking van GGD Contact. Het proces van change- en releasemanagement is uitvoerig beschreven in Bijlage 1 Procedurebeschrijving beheer GGD Contact.

Onderwerp	Toelichting	Norm
Afhandelen wijzigingsverzoeken	De afhandeling van geaccordeerde wijzigingen	Minimaal 95% van de goedgekeurde wijzigingen wordt gerealiseerd conform afspraak
Implementeren releases	Afhandelen van een verzameling van wijzigingen in een release voor GGD Contact	Minimaal 95% van de releases wordt gerealiseerd op de overeengekomen implementatiedatum

G. Continuïteitsmanagement

Continuïteitsmanagement is het proces dat zorgt voor afdoende technische voorzieningen om de continuïteit van de dienstverlening te borgen. De borging van de continuïteit wordt gerealiseerd conform onderstaande normen.

Onderwerp	Toelichting	Norm
Back-up en restore	Het veiligstellen van mail en volledig herstel GGD Contact (inclusief database) op de productieomgeving en het terugzetten hiervan.	- 24x per uur, RPO[2] maximaal 1 uur, RTO[3] maximaal 2 uur. Reactietijd: 15 minuten (met best effort voor sneller binnen kantooruren) - 30 x per maand[4], RPO maximaal 1 dag, RTO maximaal 4 uur.

[2] Recovery Point Objective of herstelpuntdoelstelling
[3] Recovery Time Objective of hersteltijddoelstelling
[4] Voor de back-ups die tot 1 maand teruggaan, is de RTO alleen haalbaar op basis van disaster recovery. Dat betekent dat alle databases van een omgeving in één keer terug worden gezet. Bij een lagere RPO en lagere RTO (bijv. bij back-ups die verder dan 1 maand teruggaan) wordt de data in een geïsoleerde omgeving (sandbox) beschikbaar gesteld waar een extract van wordt gemaakt.

		- 12 x per jaar, RPO maximaal 1 maand, RTO maximaal 2 (werk)dagen
Bewaartermijn	Periode dat de veiliggestelde gegevens worden bewaard.	Retentie van 7 jaar
Uitwijk	De mogelijkheid om, na een calamiteit, de dienstverlening te hervatten op een andere wijze of andere locatie.	Het datacentrum van de hostingpartij is dubbel uitgevoerd. Uitwijk bij uitval van het datacenter zal automatisch plaatsvinden. Specifieke uitval wordt opgepakt binnen incidentproces, waarbij back-up en uitrolplan van de specifieke release leidend zijn.

3 Beveiliging

In GGD Contact wordt gevoelige informatie verwerkt zoals medische gegevens (bijzondere persoonsgegevens en informatie over de persoonlijke levenssfeer (o.a. persoonlijke contacten). Informatiebeveiliging is daarmee een belangrijke randvoorwaarde voor een goede en vooral betrouwbare dienstverlening. De ontwikkeling van GGD Contact en het beheer gebeurt conform hoge informatiebeveiligings- en privacybeschermingseisen.

3.1 Van toepassing zijnde kaders

Aan de basis van de inrichting, bestendiging en verbetering van beveiliging liggen primair de volgende kader stellende documenten.

- AVG
- NEN 7510-1 en NEN 7510-2 voor zover relevant voor de ontwikkeling van de applicatie.
- NEN 7512 – als subset van beheersmaatregelen uit de NEN 7510-2 voor de vertrouwensbasis voor gegevensuitwisseling.
- NEN 7513 – als ontwerpvoorwaarde voor de applicatielogging.
- DPIA GGD Contact

Deze normen zijn door VWS omgezet in concrete maatregelen die zijn genomen bij de ontwikkeling en het beheer van GGD Contact. In het document Beveiliging GGD Contact is de toelichting en concrete invulling van bovenstaande normen opgenomen. Dit document wordt elke release van GGD Contact geüpdatet en beschikbaar gesteld aan de CISO van de GGD en de kwaliteitsmanager GGD GHOR.

3.2 Logging en monitoring

Applicatielogging is ingericht conform NEN7513. RDO geeft inzicht in een selectie van de logging ten behoeve van het herkennen van afwijkende handelingen in de applicatie om misbruik op te sporen. Dit deelt RDO met een partij die door de GGD is aangewezen om de monitoring uit te voeren. Daarnaast is (infrastructuur) logging - en monitoring onderdeel van de dienstverlening van RDO – dit wordt onder eigen beheer uitgevoerd. Afwijkingen worden gemeld aan GGD-GHOR SOC. Waar nodig deelt VWS logbestanden op verzoek van de GGD voor de uitvoering van verzoeken door toezichthouders of wettelijke verplichting in het kader van opsporing.

3.3 Beveiliging afnemer

Zowel dienstverlener als afnemer dienen invulling te geven aan de ministeriële regeling voor infectieziektebestrijding[5]. Met het tekenen van deze DVO bevestigen beide partijen hieraan te voldoen.

De wijze waarop de beveiliging van de informatie-uitwisseling met externe bronnen is ingericht moet worden vastgelegd conform de eisen uit de NEN 7512. De uitwisseling wordt pas gestart als deze maatregelen zijn vastgelegd.

[5] Regeling van de Minister van Volksgezondheid, Welzijn en Sport van 18 november 2008, nr. PG/ZP-2.892.655, houdende nieuwe eisen inzake de publieke gezondheid (Regeling publieke gezondheid)

4 Verantwoordelijkheden

Zowel de GGD als VWS zijn verantwoordelijk voor het niveau van dienstverlening, GGD in de rol van afnemer en VWS in de rol van leverancier. De verantwoordelijkheden zijn hieronder beschreven.

4.1 Verantwoordelijkheden VWS

- Het leveren van de diensten conform het dienstenniveau zoals in dit document beschreven.
- Het uitvoeren van de noodzakelijke patches en updates indien dit vanuit beheer en/of beveiliging noodzakelijk blijkt om de bestaande functionaliteit van de diensten in stand te houden.
- Het uitvoeren van applicatie-, en technisch beheer.
- Het contractueel vastleggen van afspraken met externe leveranciers.
- Signaleren en melden van risico's in de keten die invloed hebben op het functioneren van de applicatie, zoals beschreven in Bijlage 1 Procedurebeschrijving beheer GGD Contact.

4.2 Verantwoordelijkheden GGD

- Het melden van wijzigingen in de koppeling van eigen systemen, die op enige wijze relevant zijn voor de werking van de afgenomen diensten.
- Het melden van (beveiligings-)technische en functionele onvolkomenheden in de werking van de diensten en de gegevensuitwisseling.
- Het uitvoeren van functioneel beheer.
- Het bewaken van de kwaliteit van de (door de afnemer zelf) vast te leggen gegevens met betrekking tot tijdigheid, juistheid en volledigheid en het gebruik van deze gegevens.
- Het signaleren en melden van beveiligingsrisico's die effect hebben op de veiligheid/beveiliging van GGD Contact.
- Het gestructureerd en geprioriteerd melden van wensen voor doorontwikkeling, conform het wijzigingsproces als gespecificeerd in Bijlage 1 Procedurebeschrijving beheer GGD Contact.
- Afstemming over toevoeging van koppelingen (of wijzigingen hierop).

5 Communicatie

5.1 Rapporteren

Rapportage over de dienstverlening worden in afstemming met GGD GHOR vastgesteld en zijn onderdeel van het document Procedurebeschrijving beheer GGD Contact.

5.2 Overlegvormen

Overleggen ten behoeve van de te leveren dienstverlening zijn omschreven in de Bijlage 1 Procedurebeschrijving beheer GGD Contact.

6 Tekenblad

Door de ondertekening stemt ondergetekende in met de overeenkomst voor het gebruik van GGD Contact, als gevolg waarvan een overeenkomst ontstaat tussen VWS en de GGD.

Voor akkoord:

[redacted]

Partij: Staat der Nederlanden (Ministerie VWS)
Datum: [redacted] 1/11/2021
Voor deze: [redacted]

Tekenblad

Door de ondertekening stemt ondergetekende in met de overeenkomst voor het gebruik van GGD Contact, als gevolg waarvan een overeenkomst ontstaat tussen VWS en de GGD.

Voor akkoord:

[redacted]

Partij: GGD Limburg Noord
Datum: 23-09-2021
Voor deze: [redacted]

Inhoud

Artikel 1. Begrippen 2
Artikel 2. Voorwerp van deze Verwerkersovereenkomst 3
Artikel 3. Inwerkingtreding en duur 3
Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer 3
Artikel 5. Beveiliging van de Verwerking 4
Artikel 6. Geheimhouding door Personeel van Opdrachtnemer 4
Artikel 7. Subverwerker 4
Artikel 8. Bijstand vanwege rechten van Betrokkene 5
Artikel 9. Inbreuk in verband met Persoonsgegevens 5
Artikel 10. Terugbezorgen of wissen Persoonsgegevens 5
Artikel 11. Informatieverplichting en audit 5
Artikel 12. Aansprakelijkheid 5
Bijlage 1. De Verwerking van Persoonsgegevens 7
Bijlage 2. Passende technische en organisatorische maatregelen 8
Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens 9

Verwerkersovereenkomst ARVODI-2018

De ondergetekenden:

1. De Gemeentelijke Gezondheidsdienst GGD Limburg-Noord, gevestigd te Blerick aan de Drie Decembersingel 50, ingeschreven in het handelsregister onder KvK nummer [redacted] rechtsgeldig vertegenwoordigd door [redacted] hierna te noemen: Opdrachtgever,

en

2. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag, te dezen vertegenwoordigd door de Minister van Volksgezondheid, Welzijn en Sport, namens deze, [redacted], hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in artikel 1 van de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten 2018 (ARVODI-2018). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

1.3 Overeenkomst: de overeenkomst tussen Opdrachtgever en Opdrachtnemer OVEREENKOMST HOSTING EN BEHEER 'GGD CONTACT' van /datum/.

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven. Opdrachtgever garandeert dat de opdracht van de Verwerking in overeenstemming is met de door Opdrachtgever uitgevoerde data protection impact assessment (DPIA).

2.3 Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen zoals bedoeld in Bijlage 2 , opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens zoals Opdrachtgever die heeft gecommuniceerd en vertaald zijn naar requirements.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Opdrachtnemer alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 In aanvulling op artikel 15 van de ARVODI-2018 en onverminderd artikel 2.3 treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtgever garandeert Opdrachtnemer zo spoedig mogelijk op de hoogte te brengen van aanvullende of aangescherpte beveiligingseisen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens. Indien deze aanvullende maatregelen het beveiligingsniveau van Opdrachtnemer overstijgen en meerwerk oplevert dan komen de kosten voor deze aanvullende maatregelen voor rekening van Opdrachtgever.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening. De redelijke kosten die hierbij gemoeid zijn kunnen door Opdrachtnemer bij Opdrachtgever in rekening gebracht worden.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 13.1 van de ARVODI-2018.

6.2 Opdrachtnemer toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 13.2 van de ARVODI-2018.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 8 van de ARVODI-2018, een andere verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

Opdrachtnemer verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden. De redelijke kosten die hierbij gemoeid zijn worden door Opdrachtnemer bij Opdrachtgever in rekening gebracht.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

10.2 Zodra de Overeenkomst is beëindigd, zal Opdrachtnemer – naar keuze van Opdrachtgever – alle persoonsgegevens die bij haar aanwezig zijn in originele of kopievorm retourneren aan Opdrachtgever, en/of deze persoonsgegevens en eventuele kopieën daarvan verwijderen en/of vernietigen op instructie van Opdrachtgever.

Artikel 11. Informatieverplichting en audit

11.1 Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Opdrachtnemer verleent op basis van nacalculatie alle benodigde medewerking aan audits. De bedoelde audit vindt plaatst nadat Opdrachtgever de bij Opdrachtnemer aanwezige soortgelijke auditrapportages heeft opgevraagd, beoordeeld en zij redelijke argumenten ziet om een audit te doen.

11.3 Opdrachtnemer verstrekt met een frequentie van eenmaal per jaar, uiterlijk op 1 maart aan Opdrachtgever een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de genoemde naleving.

Artikel 12. Aansprakelijkheid

[redacted]

[redacted]

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Blerick, datum: 23-09-2021 GGD Limburg Noord namens deze, [redacted]	Den Haag, datum: 1/11/2021 DE MINISTER/STAATSSECRETARIS Volksgezondheid, Welzijn en Sport namens deze, [redacted]

Bijlage 1. De Verwerking van Persoonsgegevens

Het onderwerp/aard en doel van de Verwerking	De verwerking door opdrachtnemer betreft het hosten van app, sluis en webportal van 'GGD Contact'. Het doel van GGD Contact is op een goede, veilige en efficiënte manier uitvoeren van bronnen- en contactonderzoek.
Het soort Persoonsgegevens	• Bijzondere categorieën van gegevens als bedoeld in artikel 9 AVG • Wettelijk voorgeschreven identificatienummers • Overige persoonsgegevens.
Beschrijving categorieën Persoonsgegevens	• Gegevens die de Opdrachtgever nodig heeft voor bron- en contactopsporing. Dit zijn gezondheidsgegevens. Bijvoorbeeld: netwerk/relatie-gegevens, gegevens over contacten van index, contactgegevens, besmettingsrisico, klachten, door de index in een open veld zelf ingevulde gegevens • Gegevens van medewerkers die het bronnen- en contactonderzoek uitvoeren, waaronder ook de logging van het gebruik van de applicatie.
Beschrijving categorieën Betrokkenen	• Met infectieziekte besmette personen ('index') • Contacten die mogelijk besmet zijn ('contacten') • Medewerkers die bronnen en contactonderzoek uitvoeren
Beschrijving categorieën ontvangers van Persoonsgegevens	Medewerkers van Opdrachtnemer en door Opdrachtnemer ingeschakelde (sub)verwerkers die vanuit hun rol bij de verwerking betrokken zijn.

Bijlage 2. Passende technische en organisatorische maatregelen

Het vereiste beveiligingsniveau is vastgelegd in de DVO in hoofdstuk 3 (Beveiliging) en in de daarbij behorende bijlage Beveiliging GGD Contact (zie de verwijzing in artikel 1.3 van de DVO).

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Inbreuken in verband met Persoonsgegevens moeten worden gemeld bij de servicedesk van GGD GHOR en worden afgewikkeld volgens het door GGD GHOR gehanteerde incidentproces.

Betreft het een incident dat zich voordoet bij Opdrachtnemer, dan worden bij de melding van het incident alleen die persoonsgegevens verstrekt die noodzakelijk zijn voor de afwikkeling van het incident, waaronder een beschrijving van

Aard van de Inbreuk in verband met Persoonsgegevens
De Persoonsgegevens en Betrokkene (voor zover noodzakelijk)
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

De wijze waarop incidenten kunnen worden aangemeld zal door GGD GHOR aan Opdrachtgever en Opdrachtnemer worden gecommuniceerd. Partijen zijn hierbij zelf verantwoordelijk voor de beveiliging van de henzelf verzonden berichten.

Op verzoek van de Privacy Lead van GGD GHOR of de FG van de GGD kan bij de opvolging van incidenten ondersteuning gevraagd worden van Opdrachtnemer. In dat geval wordt in een intake bepaald welke gegevens Opdrachtnemer hiervoor nodig heeft.

Dienstverleningsovereenkomst
GGD GHOR Nederland – GGD
generieke ICT-diensten ten behoeve van GGD Contact

Versie:	1.1
Datum:	8 juni 2021

Versiehistorie

Versie	Datum	Auteur	Status document
0.1	31 mei 2021	[redacted]	Nieuwe overeenkomst
0.3	3 juni 2021		Review commentaar verwerkt
0.98	4 juni 2021		Review commentaar/context informatie verwerkt
0.99	7 juni 2021		Review commentaar JS en Vendor Mgt verwerkt
1.0	8 juni 2021		Review EY programma
1.1	21 juni 2021		Review commentaren stuurgroep verwerkt.

De ondergetekenden:

De Stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland, gevestigd te [redacted] aan het adres [redacted] ingeschreven in het handelsregister onder KvK nummer [redacted] hierna eveneens te noemen **"GGD GHOR Nederland"** rechtsgeldig vertegenwoordigd door [redacted]

En

De Gemeentelijke Gezondheidsdienst GGD Limburg-Noord, gevestigd te Blerick aan de Drie Decembersingel 50, ingeschreven in het handelsregister onder KvK nummer [redacted] hierna eveneens te noemen **"GGD"**, rechtsgeldig vertegenwoordigd door [redacted] eveneens te noemen **"GGD"**.

Hierna gezamenlijk aangeduid als **"de Partijen"** en ieder als een **"Partij"**.

Overwegende dat:

- De Vereniging GGD GHOR Nederland heeft statutair onder meer ten doel het inhoudelijk functioneren van de GGD organisaties te bevorderen, deskundige en innoverende bijdrages te leveren aan het beleid van de GGD organisaties en de belangen van haar leden te behartigen. In de kern vormt de Vereniging het samenwerkingsverband van de GGD-en;
- De algemene ledenvergadering van GGD GHOR Nederland (**"de DPG-raad"**) bestaat uit de directeuren publieke gezondheid (**"DPG'en"**) van alle GGD'en. De DPG-en zijn belast met de leiding van de GGD-en (art. 14 lid 3 Wet Publieke Gezondheid);
- Contractspartij Stichting Projectenbureau (**"Stichting"**) heeft statutair ten doel de Vereniging GGD GHOR Nederland in haar doelstellingen te ondersteunen en taken te verrichten in opdracht van het bestuur van de Vereniging (**"Presidium"**). De Stichting kan namens en op verzoek van de Vereniging verplichtingen aangaan ten laste van haar leden of rechten bedingen ten behoeve van haar leden;
- In de DPG-raad van 12 februari is door de leden besloten om zo spoedig als juridisch verantwoord mogelijk is, een alternatief voor het systeem (**"HPzone (Lite)"** dat gebruikt wordt in het bron- en contactonderzoek (**"BCO"**) te ontwikkelen en VWS als stelsel-verantwoordelijke te verzoeken als opdrachtgever op te treden. In de DPG-raad van 15 april 2021 is besloten om over te gaan tot de installatie van een projectstuurgroep Fase 1 die zich richt op de zo spoedig als mogelijk en verantwoorde uitrol bij de GGD'en van dit alternatieve systeem (**"GGD Contact"**). Deze overeenkomst en de daarin benoemde dienstverlening vloeit voort uit deze besluiten;
- Het ministerie van Volksgezondheid, Welzijn en Sport (**"VWS"**) heeft in haar rol als opdrachtgever, indachtig de besluiten van de DPG-raad, aan GGD GHOR Nederland de opdracht gegeven om de vervanging van HPzone (Lite) door GGD Contact ten behoeve van BCO in het kader van de bestrijding van covid-19 bij de GGD'en te coördineren en een deel van de dienstverlening rondom GGD Contact aan de GGD'en na implementatie op zich te nemen;
- Met de in gebruik name van GGD Contact zal GGD gebruik gaan maken van een aantal generieke ICT-diensten van GGD GHOR Nederland. Hierover wensen partijen middels deze overeenkomst nadere afspraken te maken;
- Deze Dienstverleningsovereenkomst inclusief haar bijlagen is door de projectstuurgroep Fase 1 d.d. op 25 juni 2021 vastgelegd als de standaard overeenkomst voor alle GGD'en die

gebruik gaan maken van GGD Contact en de hiervoor benodigde generieke ICT-diensten van GGD GHOR Nederland;

- In geval van strijdigheid tussen de Dienstverleningsovereenkomst en de bijlagen prevaleert het bepaalde in de Dienstverleningsovereenkomst.

Partijen verklaren als volgt te zijn overeengekomen

1. Doel

1.1. Het doel van partijen is zich gezamenlijk in te spannen voor een optimale invoering en gebruik van GGD Contact;

1.2. GGD GHOR Nederland zal diensten aan GGD leveren inzake GGD Contact en GGD zal deze diensten van GGD GHOR Nederland afnemen gedurende de looptijd van deze overeenkomst. Deze diensten zijn vermeld in bijlage I welke integraal deel uit maakt van deze overeenkomst;

1.3. Deze diensten worden conform de kwaliteitsstandaarden als vermeld in de Service Level Agreement die bijgevoegd is in bijlage II;

1.4. De benoemde diensten als genoemd in artikel 1.2. betreffen collectieve diensten die aangeboden worden aan iedere GGD die gebruik maakt van GGD Contact;

1.5. Partijen zullen elkaar ten behoeve van de samenwerking telkens tijdig alle relevante gegevens en inlichtingen verschaffen.

2. Looptijd en beëindiging

2.1. Deze overeenkomst treedt in werking op de datum waarop Partijen deze ondertekenen ("Ondertekendatum");

2.2. De overeenkomst eindigt van rechtswege wanneer de tijdelijke dienstverlenings-overeenkomst tussen VWS en GGD GHOR Nederland betreffende GGD Contact stopt. GGD GHOR Nederland informeert GGD hier onverwijld over;

2.3. Mocht een wijziging in de bestuurlijke verhoudingen en positionering van GGD GHOR Nederland hier om vragen, dan verplichten partijen zich over en weer mee te werken aan een eventuele overdracht van de rechten en verplichtingen uit hoofde van onderhavige overeenkomst;

2.4. In geval van beëindiging van deze overeenkomst zal in gezamenlijk overleg een exit plan worden opgesteld.

3. Transitie

3.1. De uitrol van GGD Contact zal in iteraties verlopen. In de eerste iteratie wordt GGD Contact naast HPZone (Lite) in gebruik genomen. GGD draagt zorg voor het parallelle gebruik. GGD GHOR Nederland houdt de dienstverlening rondom HPzone (Lite) in stand gedurende de transitieperiode;

3.2. De ontwikkeling van de dienst "GGD Contact" wordt uitgevoerd door en onder verantwoordelijkheid van VWS RDO. De projectstuurgroep fase I besluit over de snelheid en wijze van implementatie van GGD Contact. Partijen volgen de besluiten van de projectstuurgroep;

3.3. VWS is op het moment van aangaan van deze overeenkomst eigenaar van GGD Contact en verantwoordelijk voor het beheer van deze toepassing;

3.4. De afspraken over het gebruik van GGD Contact door GGD en de tijdelijke dienstverlening door VWS in dit kader, zijn onderwerp voor een aparte 'dienstverleningsovereenkomst GGD Contact' tussen GGD en VWS.

3.5. GGD GHOR Nederland draagt zorg voor de afstemming met VWS tussen de dienstverlening als benoemd in deze overeenkomst en de dienstverlening als benoemd in 3.4.

4. Kosten

4.1. De kosten voor benoemde diensten worden voorlopig gedekt door VWS. GGD GHOR Nederland zal de kosten voor de dienstverlening aan GGD bij VWS in rekening brengen;

4.2. Indien de dekking van de kosten door VWS wegvalt, treedt GGD GHOR Nederland in overleg met de DPG-Raad om tot een alternatieve financiering te komen. Partijen zullen in dat geval meewerken aan het vinden van een passende oplossing.

5. Verplichtingen GGD GHOR Nederland

5.1. GGD GHOR Nederland spant zich in om de dienstverlening als gesteld in bijlage I te leveren conform het vastgestelde kwaliteitsniveau als gesteld in bijlage II;

5.2. GGD GHOR Nederland tracht om waar mogelijk personeel met kennis van de organisatie en bedrijfsprocessen van de GGD in de te leveren dienstverlening in te zetten;

5.3. GGD GHOR Nederland wijst een vertegenwoordiger aan die als single point of entry, het aanspreekpunt is voor GGD en bevoegd is om beslissingen op het operationele vlak te nemen en maakt deze persoon aan GGD kenbaar;

5.4. GGD GHOR Nederland voorziet GGD van rapportages zoals vastgelegd in bijlage III. De rapportages voorzien in een periodieke performance evaluatie van de geleverde services.

5.5. GGD GHOR Nederland spant zich in om de door haar geleverde diensten continu te verbeteren. Verbeteringen vinden met vooraanmelding bij GGD plaats.

6. Verplichtingen GGD

6.1. GGD maakt bij het in gebruik nemen van GGD Contact gebruik van de daarbij behorende diensten die aangeboden worden door GGD GHOR Nederland.

6.2. GGD maakt gebruik van de opstelde werkinstructies en procedures die verstrekt worden door GGD GHOR Nederland waaronder de checklist onboarding applicaties zoals beschreven in bijlage V.

6.3. GGD wijst een vertegenwoordiger aan die als, single point of entry, het aanspreekpunt is voor GGD GHOR Nederland n bevoegd is om beslissingen op het operationele vlak te nemen en maakt deze persoon aan GGD kenbaar.

7. Gegevensbescherming

7.1. De Algemene Verordening Gegevensbescherming (AVG) is van toepassing op de in deze overeenkomst benoemde dienstverlening;

7.2. Partijen hebben bepaald dat GGD GHOR Nederland voor bedoelde ICT diensten verwerker is in het kader van de AVG;

7.3. Partijen hebben een verwerkersovereenkomst gesloten zoals opgenomen in bijlage IV;

7.4. Conform het bepaalde in de verwerkersovereenkomst zal GGD GHOR Nederland op een zorgvuldige wijze, in overeenstemming met de AVG gegevens en documentatie van GGD verwerken.

8. Klachtafhandeling

8.1. De klachtenprocedure van GGD GHOR Nederland is van toepassing op de in deze overeenkomst benoemde dienstverlening;

8.2. In geval dat GGD een klacht indient bij GGD GHOR Nederland, zal laatstgenoemde zo spoedig mogelijk in overleg treden met de indiener van de klacht om tot een correcte oplossing te komen.

9. Aansprakelijkheid

9.1. Partijen vrijwaren elkaar tegen alle aanspraken van derden die betrekking hebben op hetgeen is overeengekomen in deze overeenkomst en evenals tegen alle aanspraken die betrekking hebben op hun eigen verrichtingen.

9.2. Partijen dragen zorg voor een eigen dekkende verzekering voor het vergoeden van eventuele schade.

10. Wijzigingen in de overeenkomst

10.1. Partijen zijn gemachtigd om een verzoek tot wijziging van de Dienstverleningsovereenkomst voor te stellen, evenals wijzigingen op de geleverde diensten als benoemd in bijlage I.

10.2. Partijen zullen binnen een maand na een verzoek als gesteld in artikel 3.1. met elkaar in overleg treden om de gewenste wijzigingen en de daaruit voortvloeiende consequenties te bespreken conform hetgeen gesteld is in bijlage III;

10.3. Partijen nemen bij wijzigingsverzoeken de collectiviteit van de dienstverlening in ogenschouw.

11. Geheimhouding

11.1. Partijen zullen over en weer geheimhouding betrachten ten aanzien van alle gegevens, documentatie en know how die hen bekend zijn geworden in het kader van deze Dienstverleningsovereenkomst en alle van de wederpartij ontvangen gegevens waarvan men weet of redelijkerwijs behoort te weten dat deze van vertrouwelijke aard zijn;

11.2. Het verbod als benoemd in artikel 11.1. geldt niet indien en voor zover verstrekking van de betreffende gegevens of informatie aan een derde noodzakelijk is ingevolge een rechtelijke uitspraak, een wettelijk voorschrift of op basis van een wettelijk bevel.

11.3. De geheimhouding zal Partijen blijvend binden ook na beëindiging of ontbinding van deze Dienstverleningsovereenkomst tot 2 jaar na beëindiging.

Deze Dienstverleningsovereenkomst zal worden uitgelegd in overeenstemming met en worden beheerst door Nederlands recht.

Toepasbaarheid

- Verwijzingen naar wettelijke bepalingen worden zo opgevat als verwijzingen naar wettelijke bepalingen zoals deze luiden bij het aangaan van de Dienstverleningsovereenkomst
- De bijlagen vormen een integraal onderdeel van deze Dienstverleningsovereenkomst
- Hetgeen in de Dienstverleningsovereenkomst overeengekomen is, prevaleert boven de bijlagen in geval van strijdigheid en/of onverenigbaarheid
- In geval van strijdigheid en/of onverenigbaarheid tussen de bijlagen geldt de rangregeling waarbij het hoger gerangschikte document prevaleert boven het lagere gerangschikte:
    - Bijlage I; Dienstbeschrijving
    - Bijlage II; Service Level Agreement
    - Bijlage III; Dossier Afspraken en Procedures

- Bijlage IV; Verwerkersovereenkomst
- Bijlage V; Checklist onboarding applicaties

GGD GHOR Nederland

[redacted]

GGD Limburg Noord

[redacted]

Dienstbeschrijving
GGD GHOR Nederland – GGD
Generieke ICT-diensten ten behoeve van
GGD Contact

Versie: 1.1
Datum: 23 juni 2021

Versiehistorie

Versie	Datum	Auteur	Status document
0.1	31 mei 2021	[redacted]	Concept dienstbeschrijving
0.2	3 juni	[redacted]	IAM en SIEM SOC benoemd
0.3	3 juni	[redacted]	Review commentaar verwerkt
0.98	4 juni	[redacted]	Review commentaar verwerkt
0.99	7 juni	[redacted]	Review Vendor Mgt en FB
1.0	8 juni	[redacted]	Review EY programma
1.1	23 juni	[redacted]	Nieuwe reviews verwerkt

Inhoudsopgave

Versiehistorie 2
Inhoudsopgave 3
1. Dienstbeschrijving 4
1.1 Inleiding 4
1.2 Dienstbeschrijving Service Desk 4
1.3 Dienstbeschrijving ggdcontact.nl 5
1.4 Dienstbeschrijving E-mail toegang Webhelp 5
1.5 Dienstbeschrijving Identity & Access Management 6
1.6 Dienstbeschrijving SIEM SOC 6
1.7 Dienstbeschrijving VPN Verbinding 7

1. Dienstbeschrijving

1.1 Inleiding

Deze Dienstbeschrijving maakt onderdeel uit van de 'Dienstverleningsovereenkomst GGD GHOR Nederland – GGD generieke ICT-diensten' ten behoeve van GGD Contact (te noemen 'Dienstverleningsovereenkomst'). De inhoud heeft betrekking op de te leveren diensten door GGD GHOR (nader te noemen Leverancier) te [redacted]

In het kader van GGD Contact zal GGD GHOR Nederland ten behoeve van het gebruik van GGD Contact een aantal generieke ICT-diensten leveren (ook wel: Diensten), te weten:

Hieronder een nadere specificatie per generieke ICT-dienst.

- Service Desk
- Beheer van de website ggcontact.nl
- Beheer van de VPN verbinding t.b.v. GGD Contact
- Beheer E-mail toegang webhelp (GGD Contact helpdesk voor burgers)
- Beheer The Identity Hunb (TIH)
- Beheer SIEM / SOC oplossing

1.2 Dienstbeschrijving Service Desk

Voor GGD Contact voert GGD GHOR Nederland een aantal Service management processen uit voor alle GGD's, te weten de Service Desk, Incident Management en Change Management.

GGD GHOR Nederland biedt GGD een Servicedesk welke voor GGD medewerkers benaderbaar is ingeval van vragen, incidenten of wijzigingen (alleen key-users).

Eenheden en opties

- Er worden door de Servicedesk een drietal processen ondersteund, te weten: Informatie aanvraag, Incident Management en Change Management.
- De processen zijn Ingericht op basis van ITIL Service Management.
- Er wordt hierbij maximaal gebruik gemaakt van de standaardprocessen van GGD GHOR ten aanzien van Regievoering, Problem Management, Identity & Access management, Security Management etc.
- Voor ondersteuning van deze processen wordt gebruik gemaakt van de Service Management Tool: TopDesk.

Verplichtingen GGD GHOR Nederland

- Het aanbieden van de processen Informatie aanvraag, Incident Management en Change Management.
- Het doorvoeren van verbeteringen in de processen en het eventueel uitbreiden met extra diensten.
- Opleveren van rapportages.

Verplichting GGD

- Aanleveren wijzigingsverzoeken ten aanzien van processen en/ of diensten (alleen door key-users).), waarbij duidelijk omschreven wat de wens is en met welk doel.
- Veranderingen in werkprocessen, aan GGD Contact gerelateerde zaken en alles wat van invloed kan zijn op de juiste werking van GGD Contact na constatering binnen een dag doorgeven aan GGD GHOR Nederland.

- Alle mogelijke datalekken na constatering binnen maximaal 30 minuten doorgeven aan GGD GHOR Nederland.

Beheeractiviteiten GGD GHOR Nederland

- Alle meldingen worden gedaan bij de Service Desk (SD) van GGD GHOR. Dit kan per mail [redacted]@ggdghor.nl) of telefonisch ([redacted].
- De Service Desk is dagelijks geopend van 7:00 uur tot 23:00 uur.
- Alle meldingen worden geregistreerd, voorzien van een eerste prioriteit op basis van de formule impact x urgentie.

1.3 Dienstbeschrijving ggdcontact.nl

Voor de dienst GGD Contact is een website (ggdcontact.nl) voor burgers ontwikkeld voor informatievoorziening over deze dienst. Deze site wordt functioneel beheerd door GGD GHOR Communicatie (content). Applicatie beheer en hosting is in handen van Bizway BV.

Eenheden en opties

- De website ggdcontact.nl is primair bedoeld voor burgers die informatie wensen over BCO.
- De website kan ook gebruikt worden door alle GGD medewerkers.

Verplichtingen GGD GHOR Nederland

- GGD GHOR Nederland (Communicatie) is verantwoordelijk voor het actueel en volledig houden van de content op de website.
- GGD Contact is 24* 7 beschikbaar (99,9%).
- Goede performance ten aanzien van het gebruik van de website: Pagina's worden in < 0,5 sec opgebouwd.

Verplichting GGD

- Aanleveren van goed omschreven wijzigingsverzoeken.

Beheeractiviteiten GGD GHOR Nederland

- GGD Contact 24* 7 monitoren op gebied van beschikbaarheid door hosting partij.
- Performance monitoring en treffen van maatregelen wanneer deze te gering is door.
- Alle meldingen worden geregistreerd, voorzien van prioriteit op basis van de formule impact x urgentie. De classificatiematrix is een leidraad.

1.4 Dienstbeschrijving E-mail toegang Webhelp

Het GGD Contact Callcenter voor eindgebruikers (burgers) is uitbesteed aan Webhelp. Er is ook een e-mailadres beschikbaar voor burgers: [redacted]@ggdcontact.nl.

Omdat Webhelp wegens privacy regelgeving geen persoonsgegevens in mag zien wordt er gebruik gemaakt van een E-mailforwarder van Freedom Internet. Hierdoor kan Webhelp veilig mails verwerken.

Eenheden en opties

- E-mail toegang tot Webhelp.
- Koppeling tussen Webhelp en GGD GHOR Service Management.

Verplichtingen GGD GHOR Nederland

- E-mail is 24* 7 beschikbaar (99,9%).
- Goede performance (geen congestie); aflevertijd < 10 minuten.

Verplichting VWS (Webhelp)

- Aanleveren van goed omschreven wijzigingsverzoeken.
- Burgers informeren over wijzigingen via haar bestaande kanalen.

Beheeractiviteiten GGD GHOR Nederland

- GGD Contact 24* 7 monitoren.
- Performance monitoring en treffen van maatregelen.
- Alle meldingen worden geregistreerd, voorzien van prioriteit op basis van de formule impact x urgentie.

1.5 Dienstbeschrijving Identity & Access Management

Om toegang te krijgen tot de GGD Contact omgeving moet men gebruik maken van de GGD GHOR Identity Hub. Hierdoor is een gecontroleerde en beveiligde toegang gewaarborgd. De Identity Hub wordt reeds gebruikt voor toegang tot een aantal GGD GHOR Nederland systemen als CoronIT, Kennisnet etc.

Eenheden en opties

- Aanmaken en afmelden van gebruikers (GGD Medewerkers).
- Ondersteunen bij het gebruik van de Identity Hub (TIH) .

Verplichtingen GGD GHOR Nederland

- Juiste werking van de Identity Hub.
- Ondersteuning ingeval de Identity Hub niet juist werkt.
- Goede performance van de Identity Hub (geen congestie).

Verplichting GGD

- Aanleveren van goed omschreven wijzigingsverzoeken.

Beheeractiviteiten GGD GHOR Nederland

- Performance monitoring van de Identity Hub en het treffen van maatregelen in geval van congestie.
- Alle meldingen worden geregistreerd, voorzien van prioriteit op basis van de formule impact x urgentie.

1.6 Dienstbeschrijving SIEM SOC

GGD GHOR Nederland maakt (direct of indirect) gebruik van een SIEM SOC systeem om verdacht gedrag van medewerkers te achterhalen en zo nodig te rapporteren / in te grijpen. SIEM staat voor “Security Information and Event Management”. Wanneer verdacht gedrag geconstateerd wordt, zal contact opgenomen worden met de FG van de betreffende GGD. Dit is identiek aan de wijze hoe dit voor andere toepassingen van GGD GHOR Nederland is ingericht.

1.7 Dienstbeschrijving VPN Verbinding

Voor GGD medewerkers die niet op locatie zijn (en dus niet zijn aangesloten op het AMzX netwerk), is GGD Contact te benaderen via een VPN verbinding. GGD GHOR Nederland biedt GGD'en de mogelijkheid gebruik te maken van een door haar beheerde VPN-oplossing.

In tegenstelling tot de hierboven beschreven diensten is de VPN-oplossing een optionele dienst. Van de 6 'praktijktestregio's zal (voorlopig) alleen GGD West-Brabant gebruik gaan maken van de VPN-oplossing.

Eenheden en opties

- Ondersteunen bij installatie van de VPN client door medewerkers.
- Ondersteuning bij incidenten m.bt. de VPN verbinding.

Verplichtingen GGD GHOR Nederland

- Juiste werking van de VPN verbinding.
- Ondersteuning ingeval de VPN verbinding niet juist werkt.
- Goede performance van de VPN Verbinding.

Verplichting GGD

- Aanleveren van goed omschreven wijzigingsverzoeken.

Beheeractiviteiten GGD GHOR Nederland

- Performance monitoring van de VPN verbinding en het treffen van maatregelen in geval van congestie.
- Alle meldingen worden geregistreerd, voorzien van prioriteit op basis van de formule: impact x urgentie.

Service Level Agreement
GGD GHOR Nederland – GGD

Generieke ICT-diensten
ten behoeve van GGD Contact

Versie: 1.1
Datum: 23 juni 2021

Versiehistorie

Versie	Datum	Auteur	Status document
0.1	3 juni 2021	[redacted]	Concept SLA
0.2	3 juni 2021	[redacted]	Review commentaar verwerkt
0.90	4 juni 2021	[redacted]	Service levels ingevuld
0.99	7 juni	[redacted]	Review Vendor Mgt en FB
1.0	8 juni	[redacted]	Review EY programma
1.1	23 juni	[redacted]	Nieuwe reviews verwerkt

Inhoudsopgave

Versiehistorie 2
Inhoudsopgave 3
1. Doel en wijzigingen 4
1.1 Inleiding 4
1.2 Doel 4
1.3 Uitbreidingen of wijzigingen 4
2. Verplichtingen en verantwoordelijkheden 4
2.1 Verplichtingen GGD GHOR Nederland 4
2.2 Verantwoordelijkheden GGD GHOR Nederland 5
2.3 Verantwoordelijkheden GGD 5
2 Aard en prestaties dienstverlening 6
3.1 Incidentproces 6
3.1.1. Doel 6
3.1.2. Definitie 6
3.1.3 Uitgangspunten 6
3.1.4 Classificatie 6
3.1.5 Urgentie 6
3.1.6 Impact 6
3.1.7 Communicatie en rapportage 6
3.2 Wijzigingsproces 7
3.2.1. Definitie 7
3.2.2 Classificatie 8
3.3 Patch management 8
Bijlage A: Classificatie matrix 9
Bijlage B: Service management proces 10
Bijlage C: Functieomschrijving GGD key-user 11

1. Doel en wijzigingen

1.1 Inleiding

Deze Service Level Agreement, hierna te noemen 'SLA', en de daarbij behorende bijlagen maken onderdeel uit van de contractenset onder de 'Dienstverleningsovereenkomst GGD GHOR Nederland – GGD generieke ICT-diensten' ten behoeve van GGD Contact (te noemen 'Dienstverleningsovereenkomst'). De inhoud heeft betrekking op de te leveren diensten door GGD GHOR Nederland te Utrecht.

1.2 Doel

Het doel van deze SLA is het vastleggen van de condities en niveaus van de dienstverlening die nodig zijn om invulling te geven aan de overeengekomen generieke ICT-diensten van GGD GHOR Nederland aan de GGD zoals beschreven in de Dienstbeschrijving ("**Diensten**").

De beschrijving van de SLA bestaat uit een definitie van indicatoren (de Servicelevels) die voor GGD van belang zijn met het oog op (de kwaliteit van) haar bedrijfsvoering. De betreffende indicatoren zijn meetbaar en beïnvloedbaar door GGD GHOR Nederland. Per indicator is de bijbehorende norm opgenomen. Deze normen zijn de meetbare criteria waarvan GGD GHOR Nederland moet voldoen om de Servicelevels richting GGD te garanderen.

Deze SLA is een gemeenschappelijk referentiekader voor de verwachtingen van de Service Levels en vormt een normstelling voor prestatiemetingen. Zowel GGD GHOR Nederland als de GGD zullen de benodigde inspanningen leveren om de afspraken genoemd in dit document, tezamen met die in de Dienstverleningsovereenkomst, Dienstbeschrijving, DAP en overige bijlagen vastgestelde afspraken te realiseren.

1.3 Uitbreidingen of wijzigingen

Uitbreidingen of wijzigingen in scope van de dienstverlening en/of servicelevels zijn mogelijk gedurende de looptijd van de Diensten, waar deze SLA op van toepassing is. Betreffende aanpassingen worden in onderling overleg vastgesteld en schriftelijk vastgelegd zoals bepaald in het DAP. Deze uitbreidingen en/of wijzigingen zullen waar mogelijk in een Addendum worden vastgelegd en waar noodzakelijk in een nieuwe versie van de SLA worden verwerkt.

2. Verplichtingen en verantwoordelijkheden

2.1 Verplichtingen GGD GHOR Nederland

GGD GHOR Nederland zal gedurende de looptijd trachten storingen die het gebruik van GGD Contact belemmeren te verhelpen en bovendien ondersteuning op afstand bieden. Indien GGD GHOR Nederland de storing niet zelf kan verhelpen of indien GGD GHOR Nederland niet gemachtigd is tot het verhelpen van storingen in een product van een derde, zal GGD GHOR Nederland zo spoedig mogelijk de productleverancier op de hoogte stellen van de storing en eventuele (door GGD GHOR Nederland gevalideerde) oplossingen die de productleverancier aandraagt doorvoeren.

GGD GHOR Nederland onderneemt al het nodige om de door de GGD duidelijk en schriftelijk kenbaar gemaakte veiligheidsrichtlijnen na te leven.

2.2 Verantwoordelijkheden GGD GHOR Nederland

Iedere dienst is schaalbaar en op verzoek aan te passen aan veranderede wensen en behoefte van de GGD. Aanpassingen verwerkt GGD GHOR Nederland in de DAP conform overeengekomen wijzigingsprocedure.

Hieronder een overzicht van de verantwoordelijkheden voor GGD GHOR Nederland:

- Levering van de dienst conform de contractuele Dienstbeschrijving.
- Beschikbaar stellen en houden van de functionaliteit voor zover vastgelegd in het DAP.
- Beheer van de ICT Infrastructuur waar deze GGD Contact direct of indirect ondersteund.
- Monitoring van de beheerde componenten.
- Telefonisch ondersteuning binnen het afgesproken service window.
- Single point of contact. GGD GHOR Nederland zet meldingen, die buiten het domein van de door GGD GHOR Nederland geleverde diensten, door naar derde partijen. Na doorzetting van de melding beperkt de verantwoordelijkheid zich tot het rapporteren van de status.
- Registratie van alle meldingen.
- GGD GHOR Nederland zorgt voor tijdige informatie over geplande werkzaamheden wanneer deze de dienstverlening zoals beschreven in de Dienstbeschrijving beïnvloeden.
- Maandelijkse SLA reporting aan en opstellen van Risk Letters voor GGD
- Informatieplicht bij storingen.
- Afstemming VWS.

2.3 Verantwoordelijkheden GGD

Hieronder een overzicht van de verantwoordelijkheden voor GGD:

- Regierol richting GGD gebruikersorganisatie.
- Eerste lijns gebruiksondersteuning (Key users).
- Devices (desktop, laptop, tablet) en (mobiele) telefonie.
- Beheer van technische IT-voorzieningen op de GGD locaties.
- Verbindingen (inclusief monitoring).
- Printers.

Daarnaast heeft GGD de verantwoordelijkheid en meldingsplicht richting GGD GHOR Nederland aangaande infrastructuur wijzigingen en andere wijzigingen die betrekking hebben en/of invloed kunnen hebben op de afgenomen dienstverlening. Alle wijzigingsverzoeken en wijzigingen die betrekking hebben op – of een relatie met GGD Contact hebben moeten onderling afgestemd en collectief geaccepteerd zijn voordat ze richting GGD GHOR Nederland gecommuniceerd mogen worden. Bij nalatigheid is GGD GHOR Nederland niet verantwoordelijk voor het nakomen van de servicelevels zoals vermeld in deze SLA.

2 Aard en prestaties dienstverlening

In dit hoofdstuk worden de service specificatie van de verschillende beheerprocessen die deel uitmaken van het GGD Contact beheer beschreven. In bijlage B is het Service Management proces grafisch weergegeven.

3.1 Incidentproces

3.1.1. Doel

Het incidentproces heeft als doel het zo snel mogelijk verhelpen van incidenten. De doelstelling is het terugbrengen van de dienstverlening naar het normale niveau, met zo min mogelijk gevolgen in de vorm van impact, benodigde mensen, middelen (financieel & materieel) en tijd.

3.1.2. Definitie

Een incident is een afwijking van de afgesproken norm (servicelevel) ten aanzien van geleverde (ICT) diensten. Denk hierbij aan niet beschikbaar zijn van een dienst, foutieve werking of vertraagde werking.

3.1.3 Uitgangspunten

Voor de incidentprocedure geldt:

- Alle key-users van de dienst GGD Contact kunnen een incident melden.
- Alle meldingen worden gemeld bij de Servicedesk (SD) van GGD GHOR Nederland. Dit kan per mail [redacted]@ggdghor.nl) of telefonisch [redacted].
- De Servicedesk is dagelijks geopend van 7:00 uur tot 23:00 uur.
- Meldingen met de prioriteit P1 (Hoog) worden telefonisch gemeld bij [redacted].
- Alle meldingen worden geregistreerd, voorzien van prioriteit op basis van de formule impact x urgentie. De classificatiematrix is een leidraad.
- De GGD'en hebben inzage mogelijkheden in registratie en status van incidenten.

3.1.4 Classificatie

De classificatie van een incident gebeurt o.b.v. het bepalen van de urgentie en de impact. Hiervoor is de classificatiematrix de leidraad (zie Bijlage A). Hierin is ook de definitie opgenomen van prioriteit van incidenten.

3.1.5 Urgentie

De urgentie wordt bepaald door het incident en de mate waarop het betrekking heeft op continuïteit van infra, netwerk, applicaties (ketens) en betrekking heeft op beschikbaarheid, integriteit en/of vertrouwelijkheid. Gesignaleerde kwetsbaarheden, misbruik door medewerkers en/of externen vallen hier ook onder.

3.1.6 Impact

De impact wordt bepaald door de gevolgen voor gebruikers, voldoen aan wet-regelgeving, reputatieschade en/of politieke verantwoording.

3.1.7 Communicatie en rapportage

Afhankelijk van de classificatie van het incident communiceert de SD medewerker/ incidentmanager over de voortgang van de oplossing met de melder en betreffende stakeholders. In het geval van een P1 wordt onder verantwoordelijkheid van de incidentmanager nadat de oplossing gerealiseerd is, altijd een MIR (major Incident Report) en / of een RCA (Root Cause Analysis) opgesteld en gedeeld met betrokkenen.

Een MIR omvat in ieder geval:

- Komt het incident vaker voor
- Beschrijving van het incident
- Prioriteit en impact (a.d.h.v. classificatie)
- Getroffen gebruikers in %
- Consequenties incident
- Beschrijving workaround (indien relevant)
- Verder informatie indien relevant

Een RCA omvat in ieder geval:

- Korte omschrijving van het incident
- Korte omschrijving van de geschiedenis
- Hoe heft GGD GHOR Nederland het opgelost
- Wat is de hoofdoorzaak (5 * "waarom")
- Activiteiten om dit in de toekomst te voorkomen
- Overige acties
- en aanbevelingen

3.2 Wijzigingsproces

Het wijzigingsproces wordt gebruikt om op een adequate manier antwoord te geven op en invulling te geven aan een wijzigingsverzoek van GGD. Dit proces voorziet in registratie, classificatie en terugkoppeling (passief) van verwachte duur (en inspanning) van wijzigingsverzoeken.

Er worden drie soorten wijzigingsverzoeken (changes) onderscheiden:

1. Standaard change
2. Niet-standaard change

In onderstaande tabel is een verdere specificatie van de changes gegeven:

Type change	Aanmelder	Autorisatie	Voor gedefinieerd
Standaard change	• GGD key – user • GGD GHOR Nederland • VWS RDO	Nee	Zie Dienstbeschrijving
Niet standaard change	• GGD key – user • GGD GHOR Nederland • VWS RDO	Ja, het CAB	Nee, impact analyse opstellen

In Bijlage C is de functieomschrijving van een GGD key-user opgenomen.

3.2.1. Definitie

De definities van de verschillende changes zijn:

Type change	Omschrijving
Standaard change	Die is een vooraf goedgekeurde change met laag risico, relatief veelvoorkomend, en volgens een vooraf bepaalde procedure of werkinstructie af te handelen (opvoeren, verwijderen van een medewerker)
Niet-standaard change	Dit is een wijziging die geen standaardwijziging of spoedwijziging is

3.2.2 Classificatie

De classificatie van de changes is als volgt:

- Standaard change: Een wijziging die via een vooraf opgestelde standaardinstructie op afstand uitgevoerd kan worden binnen kantoortijd en minder dan 8 uur kost, met een lage impact / risico (aanmaken gebruiker, autorisatie verlening etc.).
- Minor change: een wijziging die minder dan 5 werkdagen tijd kost, op afstand uitgevoerd kan worden, binnen kantoortijd (9.00 – 17.00 uur) zonder downtime, met lage impact / laag risico.
- Major change: een wijziging die meer dan 5 werkdagen tijd kost en / of hoge impact / hoog risico en downtime met zich meebrengt en / of onsite en / of buiten kantoortijd uitgevoerd dient te worden.

3.3 Patch management

Periodiek gepland onderhoud ten behoeve van het volgens het DAP bepaalde systeem applicaties of netwerk componenten vindt afgestemd met de GGD plaats. Dit gebeurt zoveel mogelijk buiten reguliere kantooruren. Ieder jaar geeft GGD GHOR Nederland een planning van de patch momenten zodat de GGD hierop kunnen anticiperen.

Eventuele uitzonderingen op de patch management methodiek stent GGD GHOR Nederland met de GGD af en worden vermeld in het DAP.

Indien GGD zelf (periodiek) gepland onderhoud heeft aan haar applicaties, dan dient GGD GHOR Nederland dit ten minste 5 werkdagen van tevoren door te geven aan de Service Desk van GGD GHOR Nederland.

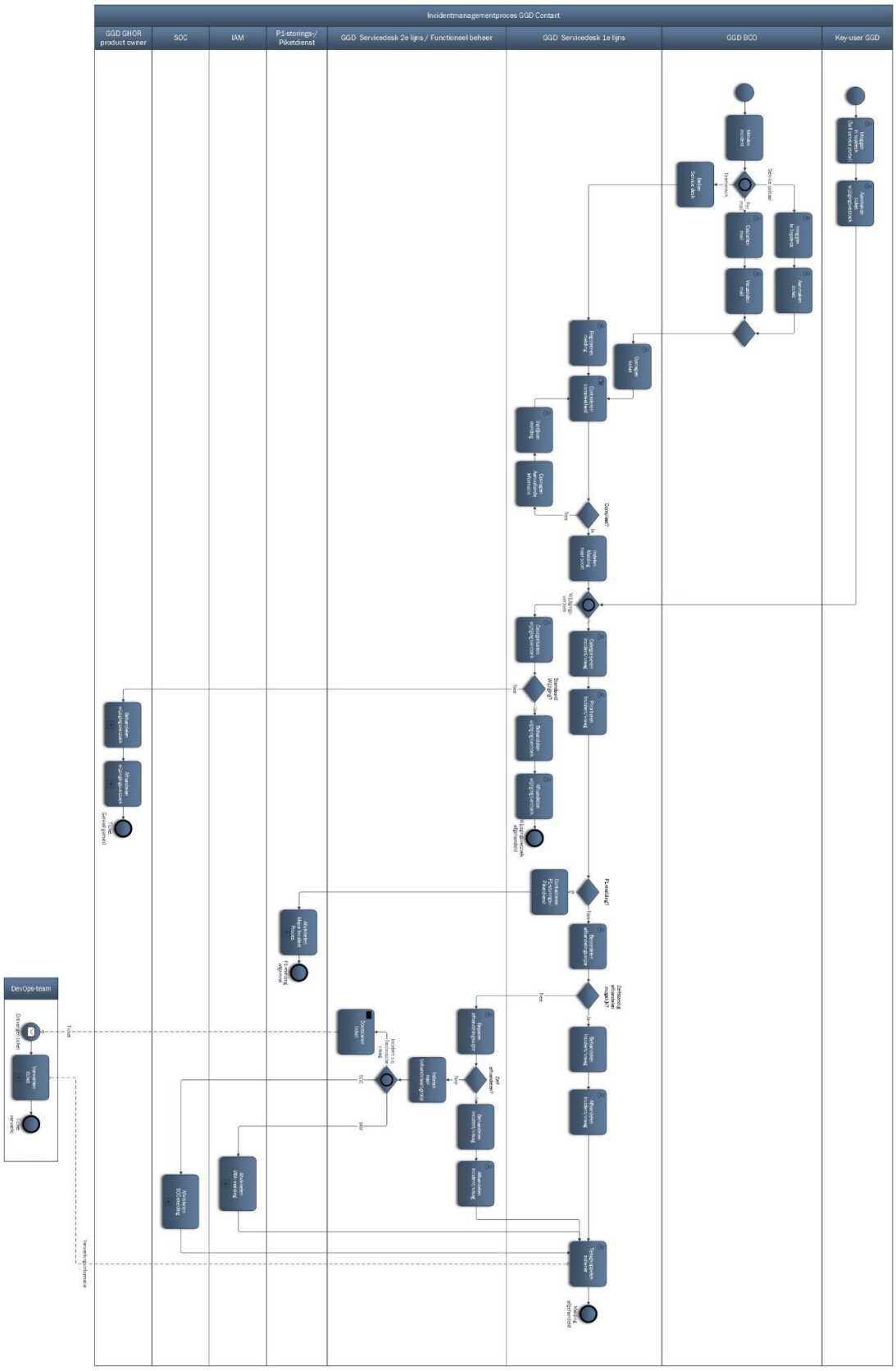
Bijlage A: Classificatie matrix

Prioriteitenmatrix

Urgentie ↓ Impact →	> 20 gebruikers	2 tot 20 gebruikers	1 gebruiker
Geen uitstel mogelijk	**P1**	**P2**	**P3**
Responstijd	[redacted]		
Doorlooptijd eerste lijn			
Doorlooptijd tweede lijn			
Servicewindow			
Kan enige uitstel verdragen	**P2**	**P3**	**P3**
Responstijd	[redacted]		
Doorlooptijd eerste lijn			
Doorlooptijd tweede lijn			
Servicewindow			
Uitstel mogelijk	**P3**	**P3**	**P4**
Responstijd	[redacted]		
Doorlooptijd eerste lijn			
Doorlooptijd tweede lijn			
Servicewindow			

[1] Ten tijde van hoge infectiedruk wordt het servicewindow opgerekt van [redacted] naar [redacted]

Bijlage B: Service management proces



Bijlage C: Functieomschrijving GGD key-user

Beheer	Key-user GGD Contact
Rolbeschrijving	De key-user is een toekomstig eindgebruiker van GGD Contact met een bovenmatige interesse & affiniteit voor digitalisering. Key-users staan er bij collega's om bekend dat ze thuis zijn in de betreffende applicatie en graag anderen ondersteunen bij het gebruik ervan. Is er issue of verbetermogelijkheid? De key-user inventariseert, verzamelt en communiceert punten richting Service Desk. De key-user is hiermee naast coach van collega's ook een 'vooruitgeschoven post' van de Service Desk. Tijdens de introductie én nieuwe release van GGD Contact speelt een key-user letterlijk en figuurlijk een sleutelrol. Proactieve ondersteuning van collega's t.b.v. een plezierige en snelle adoptie maar ook het tijdig opmerken, inventariseren, categoriseren en melden van issues en verbeteringen zijn belangrijke en primaire taken van een key-user. Key-users zijn de eersten die opleidingsmateriaal doorlopen en kennismaken met de applicatie. Zij worden voorafgaand en tijdens de transitie ondersteunt door een landelijke coach. De landelijk coach begeleid key-users ook in de wijze waarop verbeter voorstellen, bugs en issues kunnen worden geïnventariseerd, beoordeeld, gecategoriseerd en gemeld kunnen worden bij de Service Desk. Voor GGD Contact gaat de voorkeur uit naar minimaal 8 key-users per organisatie, desgewenst / naar eigen inzicht uit te breiden naar bijvoorbeeld 1 key-user per 25 medewerkers. Daarnaast heeft het de voorkeur om 1 key-user per organisatie als aanspreekpunt te laten fungeren voor de huidige projectorganisatie van GGD Contact.
Verantwoorde Lijkheden	Een key-user is op <u>afdelingsniveau</u> / <u>teamniveau</u> verantwoordelijk voor: o Draagvlak creëren voor gebruik van de applicatie onder collega's o Verspreiden release notes en workarounds o Vraagbaak voor collega's o Inventariseren & verzamelen functionele gebruikerswensen o Inventariseren & verzamelen van bugs / issues o Melden van verzamelde gebruikerswensen, bugs & issues bij Service Desk o Aanspreekpunt voor servicedesk o Aanspreekpunt voor (ondersteuners van) Product Owner i.g.v. vragen o Informeren eindgebruikers over inhoud nieuwe releases o Informeren eindgebruikers over actuele incidenten / verstoringen en oplossingen o Signaleren & terugkoppelen van procesverbeteringen o Signaleren & terugkoppelen van aanvullende opleidingsbehoefte o Afstemming en kennisdeling key-users eigen organisatie o Afstemming en kennisdeling key-users andere organisaties
Tijd besteding	De key-user kent verschillende verantwoordelijkheden. Afhankelijk van organisatiegrootte en aantal key-users, verdeling van taken/verantwoordelijkheden, aantal én impact van releases wordt een gemiddelde tijdsbesteding per week voorgesteld van 1 a 2 uur.

	Tijdens de introductie van de eerste release van GGD Contact wordt kortstondig een hogere inzet verwacht om tegemoet te komen aan gebruikersvragen en mogelijke issues / bugs en overige aandachtspunten. Key-users ontvangen telkens ruim van te voren informatie over nieuwe release zodat tijdig kan worden geanticipeerd op de mogelijke impact op processen. Ook tijdens volgende release wordt kortstondig een hogere inzet verwacht van key-users.
Competenties	Een key-user: o Heeft een meer dan brede interesse in digitaal werken o Beschikt over coachende vaardigheden om individuele collega's of groepen te ondersteunen in het gebruik van applicaties o Beschikt over algemene en/of specifieke proceskennis aangaande Bron- & Contact Onderzoek (BCO) o Beschikt over analytisch vermogen om applicaties en de processen die zij ondersteunen te doorgronden o Is in staat functionele gebruikerswensen en/of eisen te inventariseren, te beoordelen en te kunnen koppelen aan processen o Is in staat bugs en issues zich te inventariseren en te beoordelen, zodanig dat duidelijk wordt of deze al dan niet blokkerend of proces verstorend zijn o Beschikt over kwaliteiten die nodig zijn om opgehaalde wensen, eisen, bugs en issues helder te verwoorden en over te dragen aan de Service Desk o Beschikt over kwaliteit die nodig zijn om individuele of collectieve weerstanden bij collega's als gevolg van oneigenlijke bezwaren te doorbreken o Neemt initiatieven en doet concrete voorstellen t.b.v. verbetering van applicaties o Is in staat om het leren en ontwikkelen van collega's te ondersteunen o Draagt bij aan het optimaliseren van werkprocessen / workarounds
Communicatie & Contact	Key-users spelen een sleutelrol in het blijvende succes van een applicatie. Communicatie met verschillende stakeholders is hierbij van essentieel belang o De key-user onderhoudt tijdens de introductie van GGD Contact intensief contact met de landelijke coach vanuit het projectteam o De key- user onderhoudt op operationeel niveau contact met eindgebruikers van eigen organisatie o De key-user fungeert als 'vooruitgeschoven post' van de Service Desk naar de eindgebruikers en communiceert (intensief) met collega's van de Service Desk o De key-user neemt deel aan overleggen met key-users van de eigen organisatie én andere gelieerde organisaties o De key-user kan als aanspreekpunt dienen voor (ondersteuners van) Product Owner
Werkervaring	Bij voorkeur > ¾ jaar werkzaam binnen organisatie en onderdeel Bron- en Contact Onderzoek Pre: eerdere werkervaring als key-user of soortgelijke functie

Dossier Afspraken en Procedures
GGD GHOR Nederland – GGD generieke ICT-diensten
ten behoeve van
GGD Contact

Versie: 1.1
Datum: 23 juni 2021

Versiehistorie

Versie	Datum	Auteur	Status document
0.1	31 mei 2021	[redacted]	Concept DAP
0.2	3 juni 2021	[redacted]	Change proces aangevuld
0.3	3 juni 2021	[redacted]	Review commentaar verwerkt. Update van Change proces.
0.98	4 juni	[redacted]	Review Commentaar verwerkt
0.99	7 juni	[redacted]	Review Vendor Mgt en FB
1.0	8 juni	[redacted]	Review EY programma
1.1	23 juni	[redacted]	Nieuwe reviews verwerkt

Inhoudsopgave

Versiehistorie 2
Inhoudsopgave 3
1. Doel en wijzigingen 4
1.1 Inleiding 4
1.2 Doel 4
2. Contract Change Management 4
2.1 Veranderingen in onderliggende documenten 4
2.2 Niet standaard changes 4
2.3 Standaard changes 4
3. Verplichten en verantwoordelijkheden 5
3.1 Vastgestelde afspraken en procedures 5
3.1.1 Verantwoordelijkheden 5
3.1.2 Procedure 5
3.1.3 Change Advisory Board 5
3.2 Uitsluitingen 6
3.3 Verantwoordelijkheden GGD GHOR Nederland 6
3.4 Verantwoordelijkheden GGD 6
4. Vastgestelde afspraken en procedures 6
5.5 Contactgegevens 7
5.1 Aanmelden incidenten en changes 7
5.2 Aanmelden incidenten en changes 7
Bijlage A: Wijzigingsproces GGD Contact 8
Bijlage B: Service management proces 9
Bijlage C: Functieomschrijving GGD key-user 10

1. Doel en wijzigingen

1.1 Inleiding

Dit Dossier Afspraken en Procedures (hierna te noemen '**DAP**') en de daarbij behorende bijlagen, hebben betrekking op de te leveren diensten door GGD GHOR Nederland te Utrecht en maakt onderdeel uit van de 'Dienstverleningsovereenkomst GGD GHOR Nederland – GGD generieke ICT-diensten' (hierna te noemen '**Dienstverleningsovereenkomst**').

1.2 Doel

Het doel van dit DAP is het vastleggen van de verdeling van de operationele verantwoordelijkheden tussen GGD GHOR Nederland en de GGD. De focus ligt op de onderdelen die betrekking hebben op het raakvlak tussen GGD GHOR Nederland en de GGD en het vastleggen en beschrijven van de overlappende onderdelen.

2. Contract Change Management

Een contractchange is een wijziging in de overkoepelende contractvoorwaarden in de Dienstverleningsovereenkomst, SLA, DAP of dienstbeschrijving. Deze staat dus los van het in de SLA bepaalde Change Management.

Een wijzigingsverzoek van een van deze bovenstaande onderdelen dient voorgelegd te worden aan het MT Service management van GGD GHOR Nederland. Alle partijen dienen akkoord te gaan met de wijziging.

2.1 Veranderingen in onderliggende documenten

Gedurende de contractperiode zal er behoeft bestaan om onderliggende documenten aan te passen. Er ontstaan wijzigingen in de werkprocedures of afspraken die vastgelegd zijn in de SLA, DAP of dienstbeschrijving.

De FB coördinatoren van GGD GHOR Nederland zijn gemachtigd om wijzigingen voor te stellen en in onderling overleg de wijzigingen goed te keuren.

2.2 Niet standaard changes

Wijzigingen met financiële gevolgen worden door GGD GHOR Nederland opgesteld, gecoördineerd en gefiatteerd.

2.3 Standaard changes

De autorisatie voor goedkeuring en de uitvoering van de standaard changes, afwijkend van de SLA, is indien van toepassing verder gedefinieerd in dit DAP.

3. Verplichten en verantwoordelijkheden

3.1 Vastgestelde afspraken en procedures

De onderstaande afspraken en procedures zijn in onderling overleg vastgesteld.

3.1.1 Verantwoordelijkheden

GGD GHOR Nederland is verantwoordelijk voor de in dienstbeschrijving en opdrachtverstrekking vastgelegde dienstverlening, in overeenstemming met de Dienstverleningsovereenkomst en haar Bijlagen..

De verantwoordelijkheden voor de GGD'en zijn als volgt:

- Aanleveren wijzigingsverzoeken conform een afgesproken formaat, zodat het juiste detail niveau beschreven staat.

Een verdere specificering van de verantwoordelijkheden is opgenomen in de Dienstbeschrijving. De Dienstbeschrijving is leidend. Als GGD niet aan haar verantwoordelijkheid voorkomend uit de Dienstverleningsovereenkomst en hetgeen genoemd in paragraaf 3.4 voldoet, kan GGD GHOR Nederland niet gehouden worden aan nakoming van de overeengekomen servicelevels zoals opgenomen in de SLA. Uitgangspunt is dat beide partijen zich gezamenlijk maximaal inspannen om een optimale dienstverlening te leveren.

3.1.2 Procedure

Voor de wijzigingsprocedure geldt:

- Alle key-users van de dienst GGD Contact kunnen een change aanmelden.
- Alle Changes worden gemeld bij de Service Desk (SD) van GGD GHOR. Dit kan via de Topdesk Self Service Portal (SSP).
- Changes worden geclassificeerd door een Service Desk medewerker.
- Alle wijzigingen worden geregistreerd. De process owner houdt de status van een wijziging bij.
- GGD heeft inzage mogelijkheden in registratie en status van wijzigingsverzoeken.

3.1.3 Change Advisory Board

Het Change Advisory Board (CAB) is het besluit / adviesorgaan voor de niet-standaard en spoedwijzigingen. Tijdens dit overleg wordt de geïnitieerde change besproken en een besluit tot uitvoer genomen. Waar nodig sluiten naast GGD GHOR Nederland en vertegenwoordiging vanuit de eindgebruikers ook een derde partijen (bijvoorbeeld VWS) aan.

Tijdens het CAB komen de volgende onderwerpen aan de orde. Afhankelijk van de complexiteit en de impact worden de onderwerpen bepaald:

- Vaststellen doel van de change.
- Concretiseren van de change.
- Bepalen welke middelen nodig zijn bij de uitvoer van de change.
- Randvoorwaarden bepalen m.b.t. de uit te voeren change.
- Vaststellen impact van de change op de gebruikersorganisatie.
- Communicatieplan.
- Tijdstip van uitvoer.
- Accorderen plan van aanpak.
- Accorderen roll-back plan.

De volgende rollen dienen minimaal in een CAB aanwezig te zijn:

Functie	Rol	Partij
Product owner	Voorzitter	GGD
Process owner(s)	Besluit	GGD
Lead engineer consultant	Techniek	VWS (DevOps)
Change uitvoerder	Techniek	VWS (DevOps)
Service Desk	Beheer	GGD GHOR Nederland

3.2 Uitsluitingen

In de verplichtingen van GGD GHOR Nederland zijn werkzaamheden voorkomend als gevolg van de onderstaande factoren niet inbegrepen, tenzij anders vermeld:

- Storingen die worden veroorzaakt door het gebruik door GGD van het onderhoudsobject in combinatie met apparatuur, accessoires of software die niet zijn goedgekeurd door GGD GHOR Nederland, op een manier die afbreuk doet aan de functionaliteit van het onderhoudsobject.
- Storingen die worden veroorzaakt door wijzigingen die door GGD / VWS worden aangebracht of werkzaamheden aan het onderhoudsobject die zonder afstemming met GGD GHOR Nederland worden aangebracht.
- Storingen die worden veroorzaakt door virussen of andere externe invloeden, tenzij deze door onachtzaamheid van GGD GHOR Nederland worden veroorzaakt, of storingen die door derden worden veroorzaakt op andere manieren of via omstandigheden die buiten de invloedsfeer van GGD GHOR Nederland liggen.

3.3 Verantwoordelijkheden GGD GHOR Nederland

- GGD GHOR Nederland verricht geen werkzaamheden aan de GGD Contact omgeving die buiten de dienstverlening valt. Deze werkzaamheden worden, indien nodig, alleen in overleg met de GGD ingevuld.
- Indien GGD GHOR Nederland onverplicht overgaat tot het verrichten van werkzaamheden die redelijkerwijs dienstig zijn aan het goed functioneren van de GGD Contact omgeving en die geen uitstel kunnen leiden, dan wordt de GGD hier tijdig over geïnformeerd.

3.4 Verantwoordelijkheden GGD

- Ondersteuning van de eindgebruikers
- Training en communicatie van nieuwe functionaliteit in combinatie met GGD GHOR
- Wijzigingsproces: van Wens naar Requirement (JIRA melding)
- Fysiek beheren van lokale systeem- en patchruimtes van GGD (SER's en MER's) m.b.t. aspecten als koeling, bekabeling en gecontroleerde toegang.
- Hardware werkplek
- (Mobiele) telefonie
- Lokale verbindingen
- Beheer van randapparatuur

4. Vastgestelde afspraken en procedures

In een bijlage B worden de afspraken en procedures schematisch weergegeven.

5.5 Contactgegevens

5.1 Aanmelden incidenten en changes

Onderstaande operationele contactpersonen zijn bevoegd tot het aanmelden van incidenten en changes door de GGD.

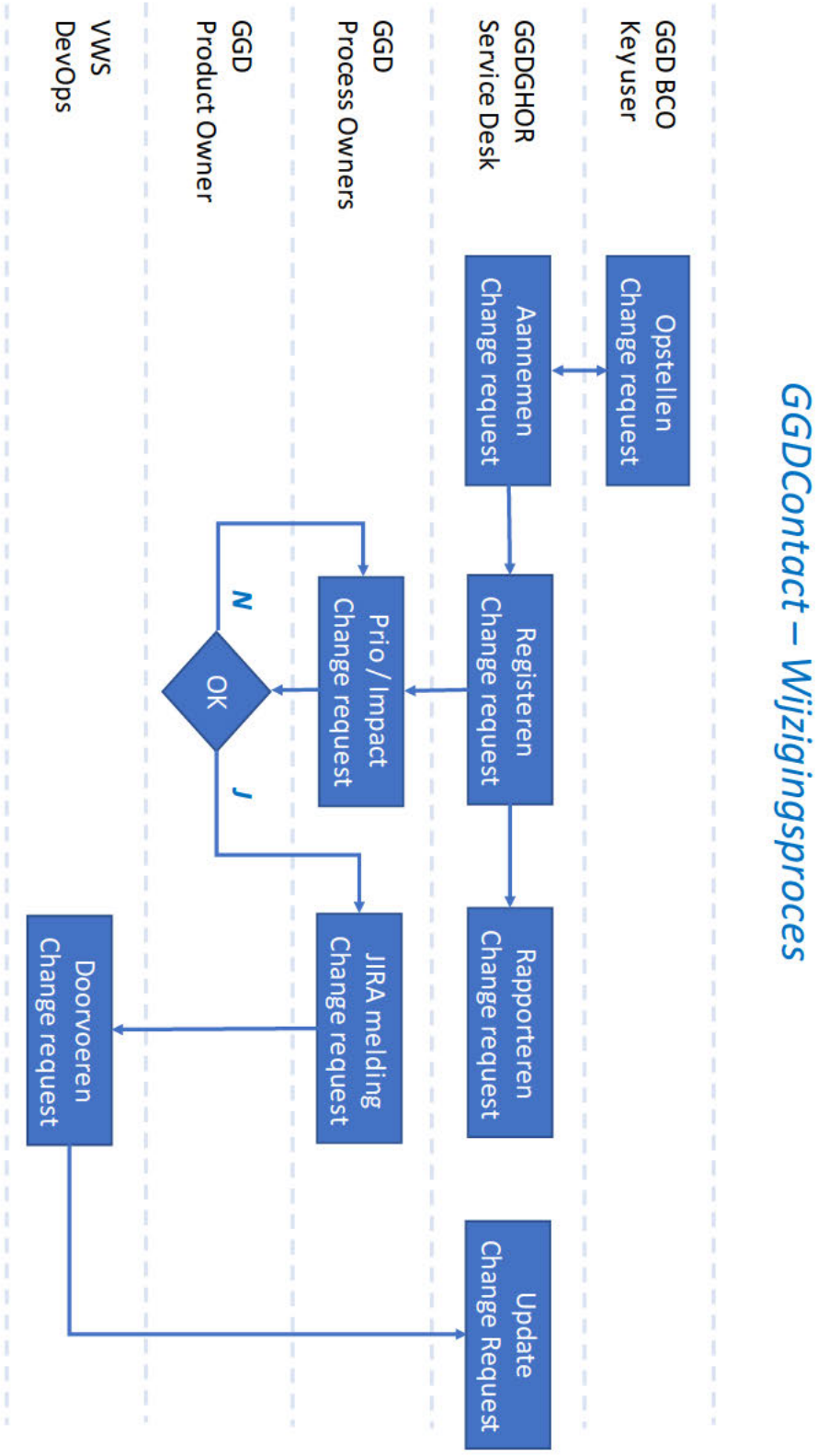
Incidenten en Wijzigingsverzoeken kunnen enkel door de key-users van een GGD (zie bijlage C) aangemeld worden. Het accorderen van een wijziging verloopt volgens de Change Management procedure (bijlage A).

5.2 Aanmelden incidenten en changes

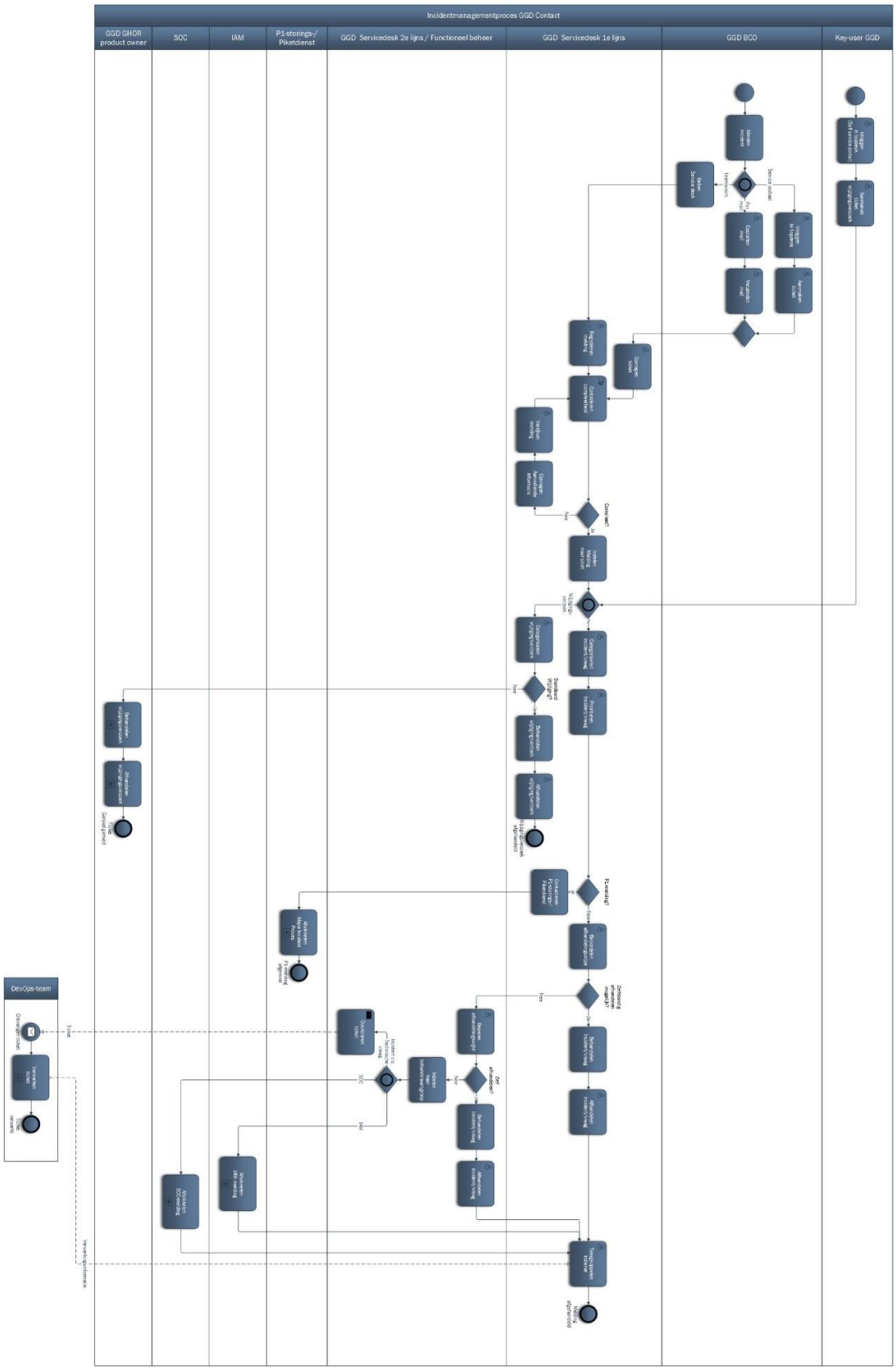
Ter ondersteuning van de dienst GGD Contact heeft GGD GHOR Nederland een Service Desk ingericht. De Service Desk is dagelijks geopend van 7:00 uur tot 23:00 uur. Het aanmelden van incidenten en / of wijzigingen kan via:

- Mail: [redacted]@ggdghor.nl
- Telefoon: [redacted]

Bijlage A: Wijzigingsproces GGD Contact



Bijlage B: Service management proces



Bijlage C: Functieomschrijving GGD key-user

Beheer	Key-user GGD Contact
Rolbeschrijving	De key-user is een toekomstig eindgebruiker van GGD Contact met een bovenmatige interesse & affiniteit voor digitalisering. Key-users staan er bij collega's om bekend dat ze thuis zijn in de betreffende applicatie en graag anderen ondersteunen bij het gebruik ervan. Is er issue of verbetermogelijkheid? De key-user inventariseert, verzamelt en communiceert punten richting Service Desk. De key-user is hiermee naast coach van collega's ook een 'vooruitgeschoven post' van de Service Desk. Tijdens de introductie én nieuwe release van GGD Contact speelt een key-user letterlijk en figuurlijk een sleutelrol. Proactieve ondersteuning van collega's t.b.v. een plezierige en snelle adoptie maar ook het tijdig opmerken, inventariseren, categoriseren en melden van issues en verbeteringen zijn belangrijke en primaire taken van een key-user. Key-users zijn de eersten die opleidingsmateriaal doorlopen en kennismaken met de applicatie. Zij worden voorafgaand en tijdens de transitie ondersteunt door een landelijke coach. De landelijk coach begeleid key-users ook in de wijze waarop verbeter voorstellen, bugs en issues kunnen worden geïnventariseerd, beoordeeld, gecategoriseerd en gemeld kunnen worden bij de Service Desk. Voor GGD Contact gaat de voorkeur uit naar minimaal 8 key-users per organisatie, desgewenst / naar eigen inzicht uit te breiden naar bijvoorbeeld 1 key-user per 25 medewerkers. Daarnaast heeft het de voorkeur om 1 key-user per organisatie als aanspreekpunt te laten fungeren voor de huidige projectorganisatie van GGD Contact.
Verantwoorde Lijkheden	Een key-user is op <u>afdelingsniveau</u> / <u>teamniveau</u> verantwoordelijk voor: o Draagvlak creëren voor gebruik van de applicatie onder collega's o Verspreiden release notes en workarounds o Vraagbaak voor collega's o Inventariseren & verzamelen functionele gebruikerswensen o Inventariseren & verzamelen van bugs / issues o Melden van verzamelde gebruikerswensen, bugs & issues bij Service Desk o Aanspreekpunt voor servicedesk o Aanspreekpunt voor (ondersteuners van) Productowner i.g.v. vragen o Informeren eindgebruikers over inhoud nieuwe releases o Informeren eindgebruikers over actuele incidenten / verstoringen en oplossingen o Signaleren & terugkoppelen van procesverbeteringen o Signaleren & terugkoppelen van aanvullende opleidingsbehoefte o Afstemming en kennisdeling key-users eigen organisatie o Afstemming en kennisdeling key-users andere organisaties
Tijd besteding	De key-user kent verschillende verantwoordelijkheden. Afhankelijk van organisatiegrootte en aantal key-users, verdeling van taken/verantwoordelijkheden, aantal én impact van releases wordt een gemiddelde tijdsbesteding per week voorgesteld van 1 a 2 uur.

	Tijdens de introductie van de eerste release van GGD Contact wordt kortstondig een hogere inzet verwacht om tegemoet te komen aan gebruikersvragen en mogelijke issues / bugs en overige aandachtspunten. Key-users ontvangen telkens ruim van te voren informatie over nieuwe release zodat tijdig kan worden geanticipeerd op de mogelijke impact op processen. Ook tijdens volgende release wordt kortstondig een hogere inzet verwacht van key-users.
Competenties	o Een key-user: o Heeft een meer dan brede interesse in digitaal werken o Beschikt over coachende vaardigheden om individuele collega's of groepen te ondersteunen in het gebruik van applicaties o Beschikt over algemene en/of specifieke proceskennis aangaande Bron- & Contact Onderzoek (BCO) o Beschikt over analytisch vermogen om applicaties en de processen die zij ondersteunen te doorgronden o Is in staat functionele gebruikerswensen en/of eisen te inventariseren, te beoordelen en te kunnen koppelen aan processen o Is in staat bugs en issues zich te inventariseren en te beoordelen, zodanig dat duidelijk wordt of deze al dan niet blokkerend of proces verstorend zijn o Beschikt over kwaliteiten die nodig zijn om opgehaalde wensen, eisen, bugs en issues helder te verwoorden en over te dragen aan de Service Desk o Beschikt over kwaliteit die nodig zijn om individuele of collectieve weerstanden bij collega's als gevolg van oneigenlijke bezwaren te doorbreken o Neemt initiatieven en doet concrete voorstellen t.b.v. verbetering van applicaties o Is in staat om het leren en ontwikkelen van collega's te ondersteunen o Draagt bij aan het optimaliseren van werkprocessen / workarounds
Communicatie & Contact	Key-users spelen een sleutelrol in het blijvende succes van een applicatie. Communicatie met verschillende stakeholders is hierbij van essentieel belang o De key-user onderhoudt tijdens de introductie van GGD Contact intensief contact met de landelijke coach vanuit het projectteam o De key- user onderhoudt op operationeel niveau contact met eindgebruikers van eigen organisatie o De key-user fungeert als 'vooruitgeschoven post' van de Service Desk naar de eindgebruikers en communiceert (intensief) met collega's van de Service Desk o De key-user neemt deel aan overleggen met key-users van de eigen organisatie én andere gelieerde organisaties o De key-user kan als aanspreekpunt dienen voor (ondersteuners van) productowner
Werkervaring	Bij voorkeur > ¾ jaar werkzaam binnen organisatie en onderdeel Bron- en Contact Onderzoek Pre: eerdere werkervaring als key-user of soortgelijke functie

DEZE VERWERKERSOVEREENKOMST IN DE ZIN VAN ARTIKEL 28 AVG (deze "**Verwerkersovereenkomst**") is getekend op 7 september 2021,

TUSSEN:

(1) De Gemeentelijke Gezondheidsdienst GGD Limburg-Noord, gevestigd te Blerick aan de Drie Decembersingel 50, ingeschreven in het handelsregister onder KvK nummer [redacted] hierna te noemen "**GGD**", rechtsgeldig vertegenwoordigd door [redacted] eveneens te noemen "**GGD**" (de "**Verwerkingsverantwoordelijke**"); [en]

(2) De Stichting Projectenbureau Publieke Gezondheid en Veiligheid Nederland, gevestigd te [redacted] aan het adres [redacted] ingeschreven in het handelsregister onder KvK nummer [redacted] hierna eveneens te noemen "**GGD GHOR Nederland**" rechtsgeldig vertegenwoordigd door [redacted] de "**Verwerker**").

De partijen bij deze Verwerkersovereenkomst worden hierna gezamenlijk ook aangeduid als de **Partijen** en ieder als een **Partij**.

OVERWEGENDE DAT:

(A) Verwerkingsverantwoordelijke persoonsgegevens verwerkt in de zin van de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening Gegevensbescherming) (de "**AVG**"), waaronder maar niet beperkt tot persoonsgegevens inzake haar GGD Contact waarvan zij het doel van en de middelen voor vaststelt en daarom kwalificeert als verwerkingsverantwoordelijke in de zin van artikel 4 lid 7AVG;

(B) Partijen de Dienstverleningsovereenkomst GGD GHOR – GGD generieke ICT-diensten ten behoeve van GGD Contact met ingangsdatum 7 juli 2021 hebben gesloten (de "Dienstverleningsovereenkomst").;

(C) In het kader van de uitvoering van de Dienstverleningsovereenkomst Verwerkingsverantwoordelijke aan Verwerker direct en/of indirect persoonsgegevens zal verstrekken en/of Verwerker toegang zal verkrijgen tot persoonsgegevens van Verwerkingsverantwoordelijke;

(D) Verwerker in het kader van de uitvoering van de Overeenkomst onder instructie van Verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan diens rechtstreeks gezag te zijn onderworpen en daarbij kwalificeert als verwerker in de zin van artikel 4 lid 8 AVG; en

(E) Partijen, in aanvulling op de Dienstverleningsovereenkomst, hun rechten en plichten vast wensen te leggen in deze Verwerkersovereenkomst overeenkomstig de AVG, de Uitvoeringswet AVG en eventuele overige toepasselijke Europese en nationale wet- en regelgeving op het gebied van privacy ("**Toepasselijke Data Protectie Wetgeving**").

PARTIJEN KOMEN OVEREEN als volgt:

1. DEFINITIES

Partijen hanteren in deze Verwerkersovereenkomst de onderstaande definities:

Autoriteit	De toezichthoudende autoriteit zoals bedoeld in artikel 51 AVG;

Betrokkene	De geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft;
Beveiligingsprotocollen	De door Verwerker te hanteren beveiligingsmaatregelen conform artikel 32 AVG;
Datalek	Een inbreuk op de beveiliging van Persoonsgegevens zoals bedoeld in artikel 4 lid 12 AVG;
Persoonsgegeven(s)	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon zoals bedoeld in artikel 4 lid 1 AVG, die Verwerker direct en/of indirect van Verwerkingsverantwoordelijke heeft verkregen en/of waartoe Verwerker toegang tot heeft gekregen van Verwerkingsverantwoordelijke.

2. DOEL VERWERKING PERSOONSGEGEVENS

2.1 Verwerker zal de Persoonsgegevens uitsluitend verwerken ten behoeve van Verwerkingsverantwoordelijke, overeenkomstig de instructies en onder de verantwoordelijkheid van Verwerkingsverantwoordelijke. Verwerker heeft geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens.

2.2 Gelet op het bepaalde in het vorige artikellid, zal de verwerking van Persoonsgegevens door Verwerker uitsluitend plaatsvinden in het kader van:

i. de uitvoering van de Dienstverleningsovereenkomst en deze Verwerkersovereenkomst; en
ii. een wettelijke verplichting die Verwerker tot de verwerking van Persoonsgegevens verplicht, in dat geval stelt Verwerker de Verwerkingsverantwoordelijke voorafgaand aan de verwerking in kennis van dat wettelijk voorschrift.

2.3 De Persoonsgegevens blijven eigendom van Verwerkingsverantwoordelijke dan wel de betreffende Betrokkene.

3. VERPLICHTINGEN VERWERKER

3.1 Verwerker is verplicht op eerste verzoek van Verwerkingsverantwoordelijke die medewerking te verlenen die nodig is om de Persoonsgegevens in te zien, aan Verwerkingsverantwoordelijke over te dragen, te verwijderen en/of te vernietigen.

3.2 Verwerker is verplicht haar verplichtingen onder de Verwerkersovereenkomst schriftelijk op te leggen aan degenen die handelen onder het gezag van Verwerker, waaronder maar niet beperkt tot medewerkers van Verwerker en de door haar ingeschakelde (sub)verwerker(s). Verwerker is jegens Verwerkingsverantwoordelijke volledig aansprakelijk voor (schade voortvloeiend uit) de verwerking van Persoonsgegevens door (sub)verwerkers die zij conform artikel 13 van deze Verwerkersovereenkomst heeft ingeschakeld.

3.3 Verwerker is verplicht om aan Verwerkingsverantwoordelijke redelijke medewerking te verlenen die noodzakelijk is voor het voldoen aan de rechten van de Betrokkene zoals bedoeld in artikel 12 t/m artikel 22 AVG, het uitvoeren van Gegevensbescherming-effectbeoordelingen (ook wel genoemd '*Privacy Impact Assessments*') zoals bedoeld in artikel 35 AVG en het voldoen aan de wettelijke verplichtingen van Verwerkingsverantwoordelijke in dit verband.

3.4 Verwerker is verplicht een administratie te voeren waaruit gedetailleerd blijkt op welke wijze zij voldoet aan haar verplichtingen op basis van deze Verwerkersovereenkomst en de Toepasselijke Data Protectie Wetgeving. Verwerker is verplicht Verwerkingsverantwoordelijke op eerste verzoek

inzage te verlenen in deze administratie en schriftelijk te informeren over de door haar genomen maatregelen met betrekking tot de verplichtingen onder deze Verwerkersovereenkomst en de Toepasselijke Data Protectie Wetgeving.

4. BEVEILIGINGSMAATREGELEN

4.1 Verwerker zal passende technische en organisatorische maatregelen nemen om de Persoonsgegevens te beveiligen tegen verlies en/of enige vorm van onrechtmatige verwerking, ermee rekening houdend dat de Persoonsgegevens tevens bijzondere categorieën van persoonsgegevens in de zin van artikel 9 en artikel 10 AVG, nationaal identificatienummers in de zin van artikel 87 AVG en persoonsgegevens van gevoelige aard bevatten. Verwerker zal zich daartoe in ieder geval, maar niet uitsluitend, houden aan het niveau van beveiliging zoals vastgelegd in de Beveiligingsprotocollen.

4.2 Verwerker is zich bewust van het belang van beveiligingsmaatregelen en zal op verzoek jaarlijks op een door Verwerker aan te wijzen manier kenbaar maken welke passende technische en organisatorische maatregelen Verwerker heeft getroffen ter beveiliging van de Persoonsgegevens.

5. MELDPLICHT DATALEKKEN

5.1 In het geval van een Datalek, zal Verwerker Verwerkingsverantwoordelijke onmiddellijk, maar in ieder geval binnen 48 uur na ontdekking van het Datalek, schriftelijk informeren op het volgende e-mail adres: [redacted]@ggdghor.nl.

5.2 Verwerker zal Verwerkingsverantwoordelijke binnen 48 uur na ontdekking van Datalek, indien op data moment beschikbaar, de informatie verstrekken die benodigd is voor het doen van de melding(en) zoals bedoeld in artikel 33 en 34 AVG en die ten minste betreft:

i. de categorieën en een indicatie van het aantal Persoonsgegevens die zijn getroffen;
ii. de categorieën en een indicatie van het aantal Betrokkene die zijn getroffen;
iii. de aard van het Datalek;
iv. de periode waarin het Datalek heeft plaatsgevonden;
v. de maatregelen die zijn genomen om de negatieve gevolgen van het Datalek te beperken;
vi. een beschrijving van de geconstateerde en de vermoedelijke gevolgen van het Datalek;
vii. de maatregelen die Verwerker en/of de door haar ingeschakelde (sub)verwerker(s) heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

5.3 Verwerkingsverantwoordelijke zal zelf de meldingen als bedoeld in artikel 33 AVG doen aan de Autoriteit en indien noodzakelijk aan de Betrokkene overeenkomstig artikel 34 AVG. Zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke, is Verwerker niet gerechtigd om Datalekken te melden aan de Autoriteit en/of Betrokkene.

5.4 Partijen kunnen schriftelijk overeenkomen dat en onder welke voorwaarden Verwerker meldingen in de zin van artikelen 33 en 34 AVG zal doen.

6. DOORGIFTE

6.1 Zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke is het Verwerker niet toegestaan om Persoonsgegevens te verstrekken aan derden, behoudens door Verwerker ingeschakelde ZZP'ers en (sub)verwerkers in overeenstemming met artikel 13 van deze Verwerkersovereenkomst.

6.2 Zonder dat een of meerdere waarborgen als bedoeld in artikel 44 t/m artikel 49 AVG zijn getroffen, is het Verwerker niet toegestaan om Persoonsgegevens te verwerken en/of door te geven aan

derde landen of internationale organisaties buiten de Europese Economische Ruimte. Verwerker is verplicht Verwerkingsverantwoordelijke schriftelijk te informeren over de door haar voorgenomen doorgifte van persoonsgegevens aan derde landen of internationale organisaties buiten de Europese Economische Ruimte en de getroffen maatregelen in dit kader.

7. CONTROLE EN AUDIT

7.1 Verwerker zal Verwerkingsverantwoordelijke voorzien van redelijkerwijs benodigde informatie en meewerken aan audits door Verwerkingsverantwoordelijke, of door een door Verwerkingsverantwoordelijke aangewezen derde, die redelijkerwijs verzocht worden en vereist zijn om aan te tonen dat Verwerker voldoet aan diens verplichtingen op grond van deze Verwerkersovereenkomst.

7.2 Het tijdstip waarop een audit zal plaatsvinden wordt in onderling overleg bepaald.

7.3 Verwerkingsverantwoordelijke zal aan Verwerker met inachtneming van een redelijke termijn vooraf een schriftelijke mededeling doen van een audit die Verwerkingsverantwoordelijke verzoekt uit te voeren in overeenstemming met artikel 7.1 met daarbij een toelichting van de gronden van de inspectie. Verwerkingsverantwoordelijke zal de hoeveelheid audits beperken en zorgdragen dat Verwerkingsverantwoordelijke of de door Verwerkingsverantwoordelijke aangewezen derde gebonden is aan geheimhoudingsverplichtingen, de redelijke instructies en aanwijzingen van Verwerker opvolgt, de ter plaatse van de inspectie geldende veiligheids- en andere voorschriften naleeft en geen schade veroorzaakt en ook niet anderszins de bedrijfsvoering verstoort. De Verwerker zal niet gehouden zijn om toegang te geven tot diens bedrijfsruimten voor de doeleinden van een inspectie:

i. aan personen die zich niet kunnen identificeren en geen bewijs van bevoegdheid kunnen overleggen; of
ii. buiten normale werkuren en/of in de weekenden.

7.4 De kosten verbonden aan een audit zullen volledig voor rekening komen van de Verwerkingsverantwoordelijke.

7.5 Verwerkingsverantwoordelijke zal Verwerker zo spoedig mogelijk na het einde van een audit voorzien van een afschrift van het auditrapport en Verwerker een redelijke mogelijkheid bieden om schriftelijk op het auditrapport te reageren.

8. AUTORITEITEN

8.1 Verwerker erkent de bevoegdheid van Autoriteiten om:

i. informatie in te winnen bij Verwerker respectievelijk bij door Verwerker ingeschakelde derden en/of de externe accountant van Verwerker omtrent de verwerking van Persoonsgegevens; en/of
ii. desgewenst onderzoek te doen of te laten doen bij Verwerker respectievelijk bij door Verwerker ingeschakelde derden en/of de externe accountant van Verwerker, bijvoorbeeld onderzoeken naar de bedrijfsvoering en bedrijfsprocessen in het kader van de verwerking van Persoonsgegevens. En verplicht zich om aan dergelijke verzoeken redelijke medewerking te verlenen.

9. RECHTEN VAN BETROKKENE

9.1 Verwerker is verplicht Verwerkingsverantwoordelijke binnen een kalenderweek, te informeren als een Betrokkene een verzoek heeft gedaan ter uitoefening van zijn of haar rechten als bedoeld in artikel 12 t/m artikel 22 AVG.

9.2 Verwerker zal alleen communiceren met een Betrokkene en verzoeken als bedoeld in het vorige artikellid in behandeling nemen na voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

9.3 Verwerker is verplicht om Verwerkingsverantwoordelijke redelijke medewerking te verlenen die redelijkerwijze noodzakelijk is voor de uitoefening van de rechten van Betrokkene op basis van de AVG.

10. GEHEIMHOUDING

10.1 Verwerker is verplicht tot geheimhouding van de Persoonsgegevens. Verwerker zal deze verplichting tot geheimhouding opleggen aan haar medewerkers en aan door Verwerker ingeschakelde derden.

10.2 Zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke, is het Verwerker niet toegestaan om informatie die redelijkerwijze te herleiden is tot deze Verwerkersovereenkomst en/of een Beveiligingsincident en/of een Datalek mede te delen met derden, waaronder maar niet beperkt tot Betrokkene, toezichthoudende autoriteiten en de media.

11. DUUR VAN DEZE VERWERKERSOVEREENKOMST

11.1 Deze Verwerkersovereenkomst treedt in werking na rechtsgeldige ondertekening door Partijen en wordt aangegaan voor de duur van de Overeenkomst. Behoudens hetgeen is bepaald in artikel 12 Verwerkersovereenkomst, eindigt deze Verwerkersovereenkomst van rechtswege op het moment van beëindiging of ontbinding van de Overeenkomst.

11.2 Artikel 10 (Geheimhouding) en artikel 16 (Toepasselijk recht en forumkeuze) zullen ook na de beëindiging of ontbinding van deze Verwerkersovereenkomst voor onbepaalde tijd tussen Partijen voortduren.

12. GEVOLGEN BEEINDIGING VERWERKERSOVEREENKOMST

Voor zover Verwerker na de beëindiging of ontbinding van deze Verwerkersovereenkomst nog beschikt over Persoonsgegevens, zal zij deze zo spoedig mogelijk vernietigen, danwel – naar keuze van Verwerkingsverantwoordelijke – aan Verwerkingsverantwoordelijke retourneren, tenzij Verwerker op grond van geldende wet- of regelgeving gehouden is de Persoonsgegevens te bewaren. In dit laatstgenoemde geval zal Verwerker al haar verplichtingen uit deze Verwerkersovereenkomst nakomen gedurende de gehele periode waarin zij op grond van geldende wet- of regelgeving gehouden is de Persoonsgegevens te bewaren.[1]

13. INSCHAKELEN (SUB)VERWERKERS

13.1 Verwerkingsverantwoordelijke verleent algemene toestemming voor het inschakelen van een (sub)verwerker. Voorafgaand aan het inschakelen van een (sub)verwerker licht Verwerker Verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervangen van andere (sub)verwerkers, waarbij Verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.[2]

13.2 Op eerste verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker aan Verwerkingsverantwoordelijke een overzicht van door haar ingeschakelde (sub)verwerkers.

---

[1] Artikel 28 lid 3 sub g AVG verplicht Verwerker om Persoonsgegevens terug te geven dan wel te verwijderen na beëindiging van deze Verwerkersovereenkomst, naargelang van Verwerkingsverantwoordelijke.

[2] Artikel 28 lid 2 AVG bepaalt dat Verwerker geen andere verwerker in dienst neemt zonder voorafgaande specifieke of algemene schriftelijke toestemming van Verwerkingsverantwoordelijke. In het geval van algemene schriftelijke toestemming licht Verwerker Verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van andere verwerkers.

14. KOSTEN

Kosten voortvloeiend uit rechten van Betrokkene zoals bedoeld in artikel 14 t/m artikel 22 AVG, uit Gegevensbescherming-effectbeoordelingen (ook wel genoemd 'Privacy Impact Assessments') zoals bedoeld in artikel 35 AVG en/of uit onderzoeken of audits van de Autoriteit met betrekking tot de Persoonsgegevens zullen worden gedragen door Verwerkingsverantwoordelijke. Kosten die gemaakt worden door Verwerker op verzoek van Verwerkingsverantwoordelijke of Autoriteiten zijn voor rekening van Verwerkingsverantwoordelijke.

15. WIJZIGING IN WET- EN/OF REGELGEVING

Bij de wijziging van bestaande wet- en/of regelgeving en bij de invoering van nieuwe wet- en/of regelgeving, verleent Verwerker op het eerste verzoek van Verwerkingsverantwoordelijke alle medewerking die redelijkerwijze van haar verwacht mag worden, zoals maar niet beperkt tot het wijzigen van deze Verwerkersovereenkomst.

Aldus overeengekomen:

[redacted]

GGD Limburg-Noord

[redacted]

GGD GHOR Nederland

[redacted]

Bijlage 1
Beschrijving verwerking Persoonsgegevens
Verwerker zal de Persoonsgegevens uitsluitend verwerken overeenkomstig de onderstaande instructies van Verwerkingsverantwoordelijke.

Onderwerp, aard en geschatte termijn van de verwerking
Het onderwerp, de aard en de geschatte termijn van de verwerking staan nader opgenomen in de Dienstverleningsovereenkomst (inclusief Bijlagen).

Doelen en wettelijke grondslagen van de verwerking
De doeleinden voor de verwerkingen inzake GGD Contact zijn opgenomen in de referentie DPIA inzake GGD Contact, waarbij de dienstverlening van GGD GHOR in dit kader nader is uitgewerkt in de Dienstverleningsovereenkomst (inclusief Bijlagen). De wettelijke grondslag voor de GGD is het uitvoeren van een taak van algemeen belang, zoals tevens nader uitgewerkt in de DPIA inzake GGD Contact.

Categorieën Persoonsgegevens
De categorieën Persoonsgegevens zijn de Persoonsgegevens die worden verwerkt in GGD Contact. Deze persoonsgegevens zijn opgenomen in de referentie DPIA inzake GGD Contact.

Categorieën Betrokkene
De categorieën Betrokkenen zijn de Betrokkenen waarvan Persoonsgegevens worden verwerkt in GGD Contact. Deze Betrokkenen zijn als volgt:
- Index
- Contact Index
- BCO-medewerker

SOC Team
[redacted]
Telefoon [redacted]
Email [redacted]@ggdghor.nl

Checklist Onboarding Applicaties

Eerst controleren, daarna aanschaffen

Definitieve versie: 1.02

Opdrachtgever	[redacted]
Auteur	[redacted]
Rapportnummer	
Classificatie	Intern
Status	Definitief
Datum	26 maart 2021
File Naam	Checklist Onboarding Applicaties

Template versie 0.02

Inhoud

1. Inleiding 4
1.1. Scope en doelgroep 4
1.2. Rollen en verantwoordelijkheden 4
1.3. Richtlijn voor het gebruik van de checklist 4
1.4. Review of audit door het SOC 4
1.5. Onderhoud van de checklist 4

2. Proces voor controle onboarding 5

3. Eisen voor applicaties 7
3.1. Werknemers en applicatiegebruikers 7
3.2. Coding en systeemdocumentatie 8
3.3. Testen op kwetsbaarheden in de beveiliging 9
3.4. Infrastructuur, back-up en monitoring 10
3.5. Organisatie 11
3.6. Dienstverlener 11
3.7. Beheerprocessen 12
3.7.1. Autorisatiebeheer 12
3.7.2. Configuratiebeheer 13
3.7.3. Wijzigingenbeheer 13
3.7.4. Incident- en probleembeheer 14
3.7.5. Beveiligingsbeheer 15

Bijlage A **Lijst van afkortingen 16**

Documentbeheer

Versiebeheer

Versie	Datum	Auteur	Omschrijving verandering	Status
0.01	09-03-2021	[redacted]	Initiële opzet	Concept
0.02	10-03-2021		Beveiligingsmaatregelen	Concept
0.90	10-03-2021		Proces	Concept
1.00	11-03-2021		Finaliseren na accordering	Definitief
1.01	25-03-2021		Verbeteren op basis feedback	Concept
1.02	26-03-2021		Finaliseren na accordering	Definitief

Gecontroleerd door

Versie	Datum	Naam	Functie
0.90	10-03-2021	[redacted]	[redacted]
1.01	26-03-2021		

Geautoriseerd door

Versie	Datum	Naam	Functie
1.00	11-03-2021	[redacted]	[redacted]
1.02	26-03-2021		

Gerelateerde documenten

Documenttitel	Omschrijving
Algemene Verordening Gegevensbescherming (AVG)	Europese privacy-verordening
Baseline Informatiebeveiliging Overheid (BIO)	Nederlandse richtlijn, gebaseerd op de internationale standaard ISO/IEC 27001:2013
NEN 7510 – Informatiebeveiliging in de Zorg	Nederlandse richtlijn, gebaseerd op de internationale standaard ISO/IEC 27001:2013 en specifiek voor de zorgsector

Volgende review en/of herziening, plus accordering (tenzij eerdere update)

Datum	Functie voor bewaking
01-06-2021	[redacted]

1. Inleiding

Met deze checklist wil GGD GHOR borgen dat applicaties die worden aangeschaft passen binnen de infrastructuur van de GGD'en en op een veilige en betrouwbare wijze gegevens verwerken.

1.1. Scope en doelgroep

Deze checklist is van toepassing op alle applicaties die worden aangeschaft ter ondersteuning van de werkzaamheden van GGD GHOR en de GGD'en.

De doelgroep bestaat uit de GGD'en, partners voor de digitale infrastructuur en leveranciers van SaaS-oplossingen, programmatuur en apparatuur.

1.2. Rollen en verantwoordelijkheden

De Chief Information Officer (CIO) van GGD GHOR is verantwoordelijk voor de inhoud van deze checklist.

De inkopende afdelingsmanager is verantwoordelijk voor het invullen van de checklist en deze toe te zenden aan het Security Operating Center (SOC) van GGD GHOR.

Het SOC is verantwoordelijk om de checklist te verifiëren en te interveniëren als blijkt dat een aan te schaffen applicatie leidt tot risico's voor de beschikbaarheid van de dienstverlening, of de integriteit of vertrouwelijkheid van de te verwerken gegevens.

Interventies door het SOC worden gerapporteerd aan de CIO, de Chief Information Security Officer (CISO) en de Functionaris voor de Gegevensbescherming (FG) van GGD GHOR.

1.3. Richtlijn voor het gebruik van de checklist

De checklist bevat een aantal aandachtspunten. Deze zijn niet voor alle toepassingen relevant en, waar nodig, mogen op 'Niet van toepassing' (Nvt) worden gezet. Van belang is dat wordt nagedacht over de betreffende aandachtspunten en weloverwogen wordt vastgesteld of deze wel of niet van toepassing zijn.

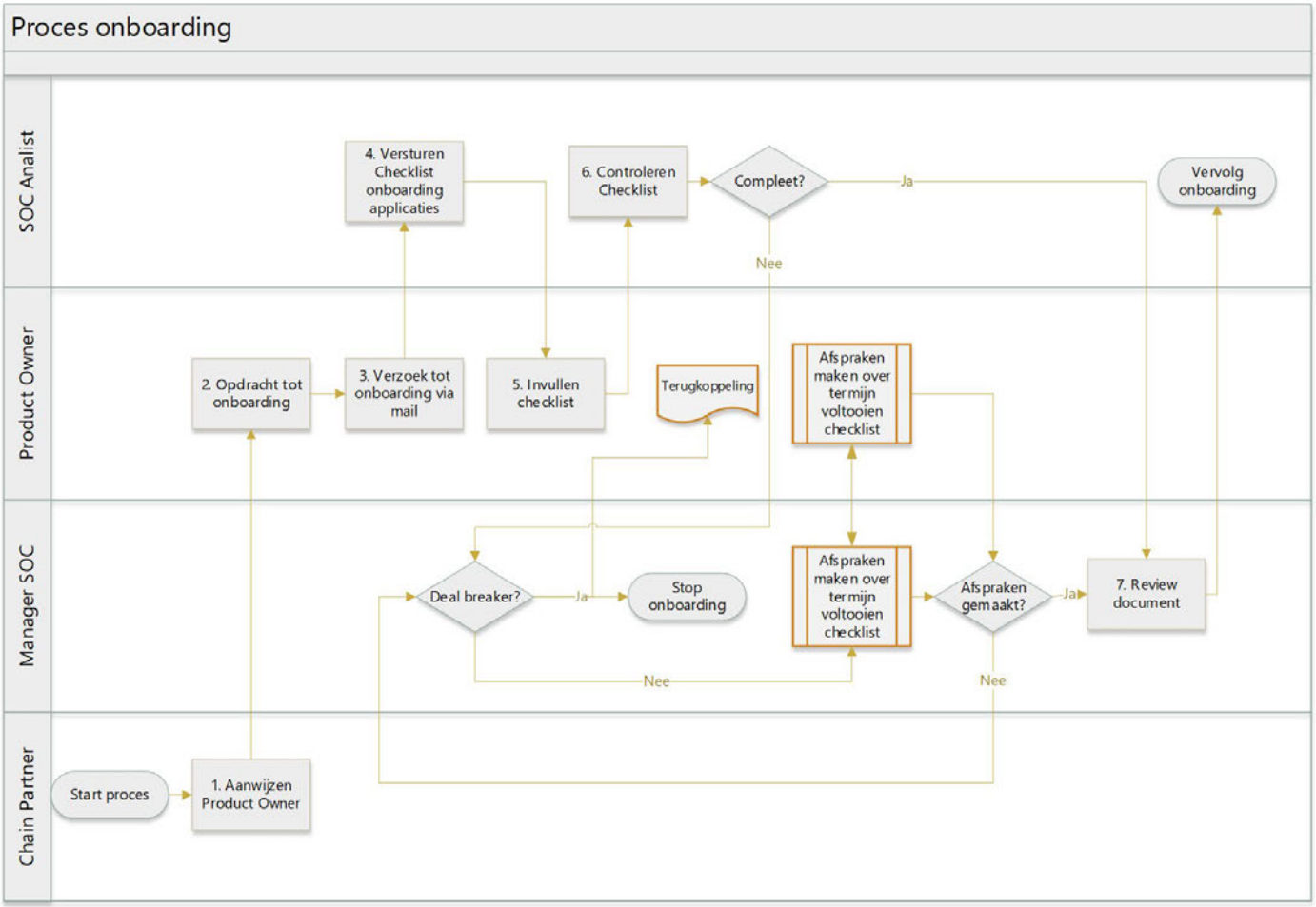
1.4. Review of audit door het SOC

Desgewenst kan het SOC een review of audit uitvoeren op een applicatie. Dit wordt met name geadviseerd voor applicaties die gevoelige persoonsgegevens verwerken of die onderdeel zijn van een essentieel bedrijfsproces bij een GGD.

1.5. Onderhoud van de checklist

Het SOC onderhoudt de checklist en communiceert deze naar de GGD'en.

2. Proces voor controle onboarding



De stappen binnen het proces zijn:

1. **Aanwijzen Product Owner**
   Deze wordt aangewezen door de ketenpartner;

2. **Opdracht tot onboarding**
   De Product Owner besluit dat controle nodig is, gezien een mogelijk risico dat kan worden veroorzaakt door de installatie of het gebruik van de applicatie;

3. **Verzoek tot onboarding via mail**
   De Product Owner licht het SOC in over de voorgenomen aanschaf van de applicatie;

4. **Versturen checklist onboarding applicaties**
   Het SOC stuurt de actuele versie van de checklist aan de Product Owner;

5. **Invullen checklist**
   De Product Owner laat de checklist invullen, bij voorkeur in overleg met de lokale CISO en, indien sprake is van het verwerken van persoonsgegevens, met de lokale Privacy Officer (PO) en/of FG. De ingevulde checklist wordt naar het SOC gestuurd;

6. **Controleren checklist**
   Het SOC controleert de ingevulde checklist op volledigheid en verifieert de risico-inschatting van de Product Owner. Dit kan leiden tot verder overleg, onder andere over aanpassing van de risico-classificatie of over de te treffen mitigerende maatregelen. Dit kan eventueel leiden tot het afwijzen van de applicatie. Als naar de mening van het SOC een getrouw beeld is gevormd van de risico's en risicomitigatie, wordt de review van de ingevulde checklist afgerond;

7. **Review document**
   De Manager SOC neemt het besluit of de onboarding van de applicatie kan worden gecontinu-eerd.

3. Eisen voor applicaties

In de onderstaande tabel is de 'Vlag' bedoeld om het risico van een eventuele afwijking weer te geven, met:

Vlag	Ernst	Toelichting
H	Hoog	Onacceptabel risico voor integere en vertrouwelijke gegevensverwerking.
M	Midden	Risico voor integere en vertrouwelijke gegevensverwerking, waarvoor complexe compenserende maatregelen nodig zijn.
L	Laag	Risico voor integere en vertrouwelijke gegevensverwerking, waarvoor eenvoudige compenserende maatregelen nodig zijn.

3.1. Werknemers en applicatiegebruikers

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
1.1	Awareness van gebruikers en beheerders voor integriteit en vertrouwelijkheid bij het gebruik is geborgd					
1.2	De gebruiker ziet een notificatie bij opstarten, waarin staat dat de regels moeten worden gevolgd					
1.3	Procedures voor uitgeven, muteren en innemen van accounts en authenticatiemiddelen, uitgeven en resetten van wachtwoorden etc. zijn ingericht					
1.4	Gebruikers zijn ingelicht dat accounts niet mogen worden gedeeld					
1.5	Use cases voor verdacht en onverdacht gebruik (voor analyse in het SIEM) zijn beschikbaar					
1.6	Monitoren van verdachte en onverdachte activiteiten van de gebruiker is mogelijk					

3.2. Coding en systeemdocumentatie

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
2.1	Een formele standaard wordt gevolgd voor ontwerpdocumentatie					
2.2	Het functioneel ontwerp is beschikbaar					
2.3	Het technisch ontwerp is beschikbaar					
2.4	Het autorisatiebeheer in de applicatie kan worden gekoppeld aan het centrale rollenbeheer					
2.5	Logging en monitoring zijn beschikbaar					
2.6	De schaalbaarheid is geborgd, dus capaciteit kan worden uitgebreid					
2.7	Het uitvoeren van op beveiliging gerichte testsessies is mogelijk					
2.8	Formele standaard documentatie over interface(s) is beschikbaar					
2.9	De koppelingen garanderen volledige en correcte gegevensoverdracht					
2.10	Cryptografie is toegepast op de applicatie en API's					

3.3. Testen op kwetsbaarheden in de beveiliging

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
3.1	Kwetsbaarheden bij het verzamelen van informatie, zoals het ontdekken van toepassingen, toegangspunten voor toepassingen en meer zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.2	Kwetsbaarheden in configuratiebeheer, zoals toegang tot beheerdersinterfaces, SSL-zwakte, XSS-risico en meer zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.3	Autorisatiekwetsbaarheden en authenticatiekwetsbaarheden zoals het opsommen van gebruikers, het doorlopen van paden, het manipuleren van rollen en meer zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.4	Kwetsbaarheden in gegevensvalidatie, zoals SQL / LDAP / SMTP / code-injectie zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.5	Penetratietests zijn uitgevoerd en gepland					

3.4. Infrastructuur, back-up en monitoring

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
4.1	De continuïteit van de applicatie is geborgd via redundante voorzieningen					
4.2	Een realtime beveiligingsservice is toegepast					
4.3	Back-ups worden regelmatig of realtime geproduceerd en restore-testen worden regelmatig uitgevoerd					
4.4	Maatregelen zijn getroffen om back-ups te beschermen tegen ransomware, via isolatie en controles					
4.5	Monitoring van blootgestelde services					
4.6	Monitoring van interne diensten					
4.7	Gevoelige omgevingen zijn geïsoleerd op netwerkniveau, door een veilige netwerkarchitectuur met VLAN's					
4.8	De toegang tot interne services en IP-adressen is beheerst					
4.9	OS- en docker-images zijn up-to-date					
4.10	Gezag en toezicht op de Data Base Administrators (DBA's) is ingericht					
4.11	Gebruik van een Ontwikkel, Test, Acceptatie en Productie (OTAP)-straat is geborgd					

3.5. *Organisatie*

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
5.1	De applicatie past binnen de veiligheidscultuur					
5.2	De applicatie draagt bij aan transparantie over diensten en gegevensverzamelingen					
5.3	De applicatie is niet in strijd met het beleid inzake openbare veiligheid					
5.4	De applicatie is niet in strijd met de naleving van het organisatiebeleid en wettelijke vereisten					
5.5	De applicatie past binnen het beleid voor bedrijfscontinuïteit en noodherstel					

3.6. *Dienstverlener*

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
6.1	De uptime in de SLA, die door dienstverlener wordt verstrekt, is geverifieerd					
6.2	Technische ondersteuning is beschikbaar vanuit de dienstverlener					
6.3	De geldigheid van certificaten, zoals ISO 27001, NEN 7510 etc. is geverifieerd					
6.4	Er is geverifieerd dat uitwijk mogelijk is naar een beveiligde uitwijklocatie					
6.5	Er is geverifieerd dat gegevens worden versleuteld tijdens transport via het interne netwerk					
6.6	Er is geverifieerd dat persoonsgegevens worden verwerkt conform de AVG (dit betreft PII – Personal Identifiable Information)					

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
6.7	Er is geverifieerd dat persoonsgegevens alleen binnen de Europese Economische Ruimte (EER) worden opgeslagen en altijd binnen de EER blijven					

3.7. Beheerprocessen

3.7.1. Autorisatiebeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
7.1	Gedocumenteerde procedures voor autorisatiebeheer zijn beschikbaar					
7.2	Het gezamenlijk gebruik van een account is niet toegestaan (dus geen groepsaccounts, altijd individuele accounts)					
7.3	Rollen zijn gebaseerd op aantoonbare functiescheiding					
7.4	Accounts zijn ingedeeld in logisch opgebouwde groepen (zoals Organizational Units – OU's – in de AD), bijvoorbeeld als eindgebruiker, administrator, mailbox, service-account etc.					
7.5	Het afdwingen van een wachtwoordbeleid dat voldoet aan de BIO is ingericht					
7.6	Een adequate lock-out policy ter voorkoming van brute force aanval met raden van wachtwoorden is ingericht					
7.7	2-Factor Authenticatie is toegepast					
7.8	Periodieke controles op accounts ter voorkoming van vervuiling worden uitgevoerd					
7.9	Rapportage over accounts is beschikbaar					

3.7.2. *Configuratiebeheer*

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
8.1	Configuratie-items zijn geregistreerd in een Configuratie Management Data Base (CMDB), inclusief hun BIV-classificatie					
8.2	Een procedure voor het beheer en onderhoud van de CMDB is ingericht					
8.3	Rapportagefaciliteiten voor de configuratie-items in de CMDB zijn beschikbaar					

3.7.3. *Wijzigingenbeheer*

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
9.1	De classificatie van wijzigingen is ingericht					
9.2	De registratie en afhandeling van wijzigingen is ingericht					
9.3	De bewaking en tijdige afhandeling van wijzigingen is ingericht					
9.4	De evaluatie van mislukte wijzigingen is ingericht					
9.5	Rapportage over wijzigingen, wel of niet succesvol geïmplementeerd, en tijdigheid is ingericht					

3.7.4. Incident- en probleembeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
10.1	De classificatie voor reguliere incidenten en beveiligingsincidenten is ingericht					
10.2	De registratie- en afhandeling van incidenten en problemen is ingericht					
10.3	De bewaking van tijdige afhandeling van incidenten en problemen is ingericht					
10.4	Incidentevaluatie en -preventie is ingericht					
10.5	Een reactieplan voor beveiligingsincidenten (incident response plan) is opgesteld en actueel					

3.7.5. Beveiligingsbeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
11.1	De fysieke toegangsbeveiliging is ingericht					
11.2	De bescherming tegen phishing is ingericht					
11.3	De bescherming tegen DDoS-aanvallen is ingericht					
11.4	De bescherming tegen ransomware is ingericht					
11.5	Domeinen zijn afgeschermd, waar nodig					
11.6	De bescherming van domeinnamen is ingericht					
11.7	Het gebruik van beveiligde wifi-verbindingen is geborgd					
11.8	Het gebruik van Virtual Private Network (VPN), waar noodzakelijk, is geborgd					
11.9	De Demilitarized Zone (DMZ) is ingericht					
11.10	Intrusion Detection System (IDS) en Intrusion Prevention System (IPS) zijn ingericht					
11.11	De web application firewall en reverse proxy zijn ingericht					

Bijlage A Lijst van afkortingen

Afkorting	Toelichting
AD	Active Directory, Microsoft
API	Application Programming Interface
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Data Base
DBA	Data Base Administrator
DMZ	Demilitarized Zone. Dit is een nul-netwerk met een binnen-firewall en een buiten-firewall, om te zorgen voor isolatie tussen netwerken.
DDoS	Distributed Denial of Service
EER	Europese Economische Ruimte
FG	Functionaris voor de Gegevensbescherming
IAM	Identity and Access Management
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LDAP	Lightweight Directory Access Protocol. Het netwerkprotocol dat beschrijft hoe gegevens uit directoryservices moeten worden benaderd.
OS	Operating System
OTAP	Ontwikkel, Test, Acceptatie en Productie
OU	Organizational Units in de AD
PII	Personal Identifiable Information
PO	Privacy Officer
SaaS	Software as a Service. Dit zijn veelal applicaties die via een web-oplossing worden geleverd.
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SOC	Security Operating Center
SQL	Structured Query Language. Dit is een programmeertaal voor toegang tot gegevensbestanden.
SSL	Secure Socket Layer. SSL is verouderd. TLS 1.2 of hoger dient te worden gebruikt.
VLAN	Virtual Local Area Network
VPN	Virtual Private Network. Dit is een versleutelde verbinding over internet.
XSS	Cross Site Scripting