GGD
Gooi en Vechtstreek

Datum	**13 juni 2022**
Kenmerk	
Inlichtingen	
Telefoon	
Onderwerp	**Besluit op Wob/WOO-verzoek**

de heer

Geachte heer ,

In uw brief van 15 februari 2022 heeft u aan GGD Gooi en Vechtstreek namens uw cliënt, de Stichting Initiatieven Collectieve Acties Massaschade **(ICAM)**, met een beroep op artikel 3 lid 1 van de Wet openbaarheid van bestuur (Wob) verzocht om:

i) Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de (door)ontwikkeling, implementatie en uitrol van, CoronIT, HPZone en/of HPZone Lite, waaronder in ieder geval:

a) Offertes GGD GHOR CoronIT d.d. 7 april 2020 en 6 juli 2020;
b) Plan van aanpak GGD GHOR Fase 1 incl. begroting d.d. 7 april 2020;
c) Plan van aanpak GGD GHOR Fase 2 incl. begroting d.d. 2 juni 2020;
d) Vervolgaanpak GGD GHOR digitale ondersteuning testprocessen COVID 19 d.d. 27 oktober 2020 incl. bijbehorende offerte;
e) De ARVODI-2018 ten aanzien van de ontwikkeling en implementatie van CoronIT;

ii) Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de inrichting en instandhouding van een klantcontactcentrum voor test- en vaccinatieafspraken en bron- en contactonderzoek;

iii) Alle offerteaanvragen, programma's van eisen, offertes en overeenkomsten, inclusief bijlagen, met betrekking tot de uitbesteding aan derde partijen van klantcontact en/of callcenterwerkzaamheden;

iv) Audits, rapportages, analyses en onderzoeken (intern of door derde partijen) met betrekking tot privacy(risico's) en beveiliging(srisico's) in verband met CoronIT, HPZone en HPZone Lite, waaronder in ieder geval:

a) Risicoanalyse uitgevoerd over de test- en traceerketen d.d. 22 december 2020;
b) Analyse KPMG interne systemen d.d. 20 januari 2020;
c) IT-assessment op het IT landschap van de COVID-19 bestrijding door GGD GHOR Nederland van december 2020;
d) IT -audit KPMG d.d. 18 december 2020;

v) Audits, rapportages, analyses en/of onderzoeken (intern of door derde partijen) ten aanzien van de effectiviteit van (beveiligings)maatregelen doorgevoerd na publiek bekend worden van het datalek, waaronder in ieder geval:

e) Rapportage functionele beveiligingstest uitgevoerd door Fox IT;
f) Extern onderzoek naar de kwaliteit van de software en de kwaliteit van de dienstverlening van de softwareleverancier van HPZone;
g) Gateway reflectie en Gateway Review op verbeterplannen;
h) Externe (technische en cutuur) audits genoemd in Kamerbrief d.d. 23 maart 2021;

vi) Verslagen en notulen Regiegroep DOTT en Landelijke Coördinatiestructuur Testcapaciteit (LCT) met betrekking tot

GGD
Gooi en Vechtstreek

CoronIT en HPZone (Lite);

vii) Informatie over de verschillen in beveiliging tussen het reeds voor de coronacrisis bestaande systeem HPZone en het later ontwikkelde HPZone Lite;

viii) Data Protection Impact Assessments (DPIA) ten aanzien van CoronIT, HPZone en HPZone Lite;

ix) Het gehanteerde beveiligings- of privacybeleid omtrent het omgaan met persoonsgegevens en datalekken in verband met testen, vaccineren en bron- en contactonderzoek, waaronder het beleid ten aanzien van toegangsrechten en autorisatiebeheer en logging en monitoring;

x) Informatie over signaleringen van gebreken of kwetsbaarheden in de (informatie)beveiliging In het kader van het testen, vaccineren en bron- en contactonderzoek, en de wijze waarop daarop is gereageerd en welke maatregelen daarop zijn genomen, waaronder signaleringen van (externe) GGD-medewerkers, van medewerkers van VWS;

xi) Informatie over de overname van het beheer van HPZone (Lite) door GGD GHOR;

xii) Informatie over de uitfasering van HPZone (Lite) en de vervanging van HPZone (Lite) door GGD Contact, waaronder in ieder geval:

i) DPIA GGD Contact;
j) Verwerkingsovereenkomst voor landelijke partner GGD Contact;
k) Inbeheername GGD Contact door GGD GHOR en DICTUR;
l) Autorisaties medewerkers GGD'en binnen GGD Contact;
m) Werkinstructie GGD Contact;

xiii) Overeenkomsten met GGD medewerkers en externen die gebruik maken en hebben gemaakt van CoronIT, HPZone en/of HPZone Lite, waaronder maar niet beperkt tot arbeidsovereenkomsten, opdrachtovereenkomst en/of geheimhoudingsovereenkomsten;

xiv) Informatie en documenten met betrekking tot de training van (externe) medewerkers ten aanzien van het gebruik van Coron1T en HPZone (Lite) en de omgang met persoonsgegevens, waaronder beleid, protocollen, instructies en presentaties;

xv) Informatie die in het kader van de melding van het datalek bij de Autoriteit Persoonsgegevens over en weer is gedeeld, alsmede informatie die over en weer is verstrekt ten behoeve van het onderzoek door de Autoriteit Persoonsgegevens naar aanleiding van het datalek;

xvi) Informatie en documenten over het onderzoek dat heeft plaatsgevonden naar de omvang van de groep gedupeerden en de potentiële schadelijke gevolgen van het datalek;

Alle informatie die uw cliënte in staat stelt om in het kader van het datalek (i) de betrokkenheid, rol en verantwoordelijkheid van de verschillende partijen vast te stellen, (ii) de omvang van het datalek en de schade die de gedupeerden ten gevolg daarvan hebben geleden, te kunnen bepalen en (iii) ten aanzien van de IT-systemen vast te stellen welke eisen voorafgaand aan en na het publiekelijk bekend worden van het datalek zijn gesteld en welke organisatorische en technische beveiligingsmaatregelen zijn getroffen.

In uw brief van 15 februari 2022, die wij hebben ontvangen op 16 februari 2022, heeft u namens ICAM verzocht om uiterlijk vier weken na dagtekening van de brief te voldoen aan het verzoek. Wij hebben de beslistermijn echter op 24 februari 2022 op grond van artikel 6 lid 2 Wob verlengd met vier weken. Bij brief van 11 april 2022 hebben wij kenbaar gemaakt dat verder uitstel noodzakelijk was om (zorgvuldig) aan het verzoek te kunnen voldoen. In voormelde brief hebben wij de beslistermijn aldus verlengd tot en met 1 juni 2022.

Deze brief bevat het besluit dat GGD Gooi en Vechtstreek neemt op het Wob verzoek van ICAM van 15 februari 2022.

GGD
Gooi en Vechtstreek

1. Wettelijk kader

Op 1 mei 2022 is de Wet open overheid (Woo) 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 ICAM 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

Binnen de reikwijdte van het verzoek van ICAM zijn in totaal 29 documenten bij de GGD Gooi en Vechtstreek aangetroffen, niet meegerekend de (landelijke, uniforme) documenten die reeds door de GGD Zeeland openbaar zijn gemaakt. Deze documenten staan in de inventarisatielijst die wij als Bijlage 1 bij dit besluit hebben gevoegd. De documenten zijn genummerd en staan in de volgorde die overeenkomt met de wijze waarop de documenten in het verzoek van 15 februari 2022 zijn gecategoriseerd (nummers i tot en met xvi). Voor zover wij besloten hebben om (delen van) documenten niet openbaar te maken, hebben wij in de inventarislijst aangegeven wat daarvoor de toepasselijke uitzonderingsgrond uit de Woo is.

3. Besluit

Wij hebben besloten om de informatie waar u, namens ICAM, om heeft verzocht, opgenomen in documenten openbaar te maken, waarbij bij sommige documenten uitzondering wordt gemaakt voor de daarin vermelde persoonsgegevens, en/of waarbij informatie in sommige documenten gedeeltelijk niet openbaar wordt gemaakt voorzover dit gevoelige informatie betreft als bedoeld in 5.1, tweede lid, aanhef en onder f en onder i Woo, een en ander zoals per documentnummer is aangegeven op de inventarislijst (Bijlage 1). Wij hebben besloten om twee documenten in zijn geheel niet openbaar te maken: (1) Werkschema voortgangsrapportage AP –Inventarisatie GGD Gooi en Vechtstreek (ad v) en (2) GGD security inventarisatie GGD Gooi en Vechtstreek (ad v.).

Voor de motivering van het besluit verwijzen wij naar het onderdeel 'Overwegingen' onder 4. van dit besluit.

4. 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. Hieronder volgen de uitzonderingsgronden voor de openbaarmaking van de gevraagde informatie.

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.
De drie gronden van uitzondering op de openbaarmaking van de verzochte informatie zijn:

1. *de persoonlijke levenssfeer (artikel 5.1, tweede lid, aanhef en onder e Woo)*

Op grond van artikel 5.1, 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 is vermeld op de inventarislijst (Bijlage 1), waarop per document is aangegeven of hierin persoonsgegevens zijn verwijderd. 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. Dit geldt tevens voor de persoonsgegevens van ambtenaren die uit hoofde van hun functie niet in de openbaarheid treden. In het kader van goed werkgeverschap is GGD Gooi en Vechtstreek van oordeel dat ten aanzien van deze gegevens het belang dat de persoonlijke levenssfeer wordt geëerbiedigd, zwaarder moet wegen dan het belang van openbaarheid. Deze gegevens hebben wij daarom ook uit de documenten verwijderd.

2. *concurrentiegevoelige bedrijfsgegevens (artikel 5.1, tweede lid, aanhef en onder f Woo)*

In enkele documenten staan tarieven genoemd van de bedrijven die aan de GGD Gooi en Vechtstreek diensten hebben geleverd op het gebied van bestrijding van Covid-19. Deze financiële gegevens worden niet geopenbaard aangezien het belang van het beschermen van de concurrentie gevoelige gegevens zwaarder weegt dan het belang van openbaarheid.

3. *gevoelige informatie (artikel 5.1, tweede lid, aanhef en onder i Woo)*

Op grond van artikel 5.1, tweede lid, aanhef en onder i Woo blijft verstrekking van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen. In bepaalde documenten staat dergelijke informatie. Hiervoor verwijzen wij naar hetgeen is vermeld op de inventarislijst (Bijlage 1). De hiervoor genoemde documenten bevatten gevoelige informatie over de beveiliging van systemen en applicaties, die gebruikt zijn bij de bestrijding van de coronapandemie. Indien deze informatie openbaar zou worden, kunnen derden mogelijk misbruik hiervan maken. Wij zijn van oordeel dat ten aanzien van deze gevoelige informatie het belang dat derden hiervan geen misbruik kunnen maken en het goed functioneren van onze organisatie ernstig kunnen belemmeren, zwaarder moet wegen dan het belang van openbaarheid. Daarom hebben wij deze informatie verwijderd uit de documenten.
Twee documenten maken wij in zijn geheel niet openbaar. De reden voor het niet openbaar maken van deze documenten is dat beide documenten informatie bevatten over de inrichting en het beveiligingsniveau van onze ICT infrastructuur. Dit is een risico voor de continuïteit en beschikbaarheid van onze IT-voorzieningen omdat kwaadwillende personen daar hun voordeel mee kunnen doen. Mede gelet op het onderwerp van dit Wob/Woo-verzoek is het realistisch te verwachten dat de gepubliceerde informatie op bovengemiddelde interesse kan rekenen, hetgeen invloed heeft op de omvang van het risico. Wij zijn van mening dat in dit geval aan het goed en veilig blijven functioneren van onze systemen een hoger belang toekomt dan aan het algemeen belang van het openbaar maken van gevraagde informatie.

<u>Informatie is reeds openbaar gemaakt</u>

GGD Zeeland heeft bepaalde documenten van GGD GHOR als eerste op 1 juni 2022 openbaar gemaakt. Deze documenten zijn te raadplegen via de website van de GGD Zeeland en kunnen worden geraadpleegd via de volgende weblink: Woo-verzoek inzake datadiefstal CoronIT - deelbesluit 1 - GGD Zeeland. De documenten zijn niet alle geheel openbaar gemaakt. Uitzondering wordt gemaakt op grond van de persoonlijke levenssfeer ex artikel 5.2, tweede lid, aanhef en onder e Woo. Wij nemen de uitzonderingsgronden en de belangenafweging van deze openbaar gemaakte stukken integraal over van de GGD Zeeland.

GGD
Gooi en Vechtstreek

5. Wijze van openbaarmaking

Alle documenten, met uitzondering van de niet openbaar gemaakte documenten, worden tezamen met dit besluit (geanonimiseerd) en bijbehorende bijlagen op onze website geplaatst. De documenten zijn te raadplegen via deze link en kunnen worden gedownload.

Tot slot:
Ik heb uw verzoek, namens ICAM, van 15 februari 2022 met de grootst mogelijke zorgvuldigheid uitgevoerd. Vanwege de grote hoeveelheid documenten en de complexiteit van het verzoek kan het zijn dat ik bepaalde documenten over het hoofd heb gezien. Mocht ICAM desondanks menen dat er documenten ontbreken, dan verneem ik dat graag. U kunt daartoe contact opnemen met de contactpersoon door middel van onderstaande contactgegevens.

6. 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 R. . contactpersoon voor informatie over de GGD). In het kader van dit besluit kunt u contact opnemen met die bereikbaar is via de volgende contactgegevens:

7. 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 de Regio Gooi en Vechtstreek, Postbus 251, 1400 AG te Bussum. Voor meer informatie zie: www.regiogv.nl. 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 Regio Gooi en Vechtstreek (GGD Gooi en Vechtstreek is onderdeel),

Directeur GGD Gooi en Vechtstreek

Bijlage 1: Inventarislijst

Categorie verzoek 15-02-22	Nummer docu-ment	Naam document	Document verstrekt Ja/nee/gedeeltelijk	Uitzonderingsgrond bij (deels) niet verstrekken
i)				
ii)	1	ii.addendum.hoofd.dienstverleningsovereen-komst	Gedeeltelijk	Art. 5.1 lid 2 sub e
iii)	2	iii. offerte.externe.dienstverlening	Gedeeltelijk	Art. 5.1 lid 2 sub f
	3	iii. dienstverleningsovereenkomst	Gedeeltelijk	Art. 5.1 lid 2 sub e en f
	4	iii. hoofd.dienstverleningsovereenkomst	Gedeeltelijk	Art. 5.1 lid 2 sub e en f
	5	iii.overeenkomst van opdracht vaccinatiewerkzaamheden	Ja	
	6	iii.addendum1.dienstverleningsovereenkomst	Gedeeltelijk	Art. 5.1 lid 2 sub e
	7	iii.addendum2.dvovereenkomst	Gedeeltelijk	Art. 5.1 lid 2 sub e
iv				
v	8	v. GGD privacy inventarisatie - GGD GenV	gedeeltelijk	Art. 5.1 lid 2 sub e en i
	9	v. Werkschema voortgangsrapportage AP – Inventarisatie GGD Gooi en Vechtstreek	Nee	Art. 5.1 lid 2 sub i
	10	v. GGD security inventarisatie GGD Gooi en Vechtstreek	Nee	Art. 5.1 lid 2 sub i
vi				
vii				
viii				
ix	11	ix. privacybeleid-regio-gooi-en-vechtstreek	Gedeeltelijk	Art. 5.1 lid 2 sub e en i
	12	ix. procedure-afhandeling-meldingen-datalekken-avg	Gedeeltelijk	Art. 5.1 lid 2 sub e
	13	ix. handreiking-beoordeling-datalekken-avg	Gedeeltelijk	Art. 5.1 lid 2 sub e
	14	ix.Strategisch Informatiebeveiligingsbeleid	gedeeltelijk	Art. 5.1 lid 2 sub e
x				
xi				
xii	15	xii.Inventarisatie rollen ihkv GGD-datalek	Gedeeltelijk	Art. 5.1 lid 2 sub e
	16	xii. Vraag rol DBCO-Werkverdeler	Gedeeltelijk	Art. 5.1 lid 2 sub e
	17	xii. Toegang tot BCO-Portaal	Gedeeltelijk	Art. 5.1 lid 2 sub e
	18	xii. Reminder Update Autorisatiematrix GGD	gedeeltelijk	Art. 5.1 lid 2 sub e
xiii	19	xiii.aanbod.kandidaten	Gedeeltelijk	Art. 5.1 lid 2 sub e en f
	20	xiii.Arbeidsovereenkomst-voor-bepaalde-tijd	Ja	
	21	xiii.Gedragscode Integriteit	ja	
	22	xiii.IntegriteitsverklaringGGD-Corona	ja	
	23	xiii. VOG.voorwaarden	gedeeltelijk	Art. 5.1 lid 2 sub e
xiv	24	xiv. VeiligThuisWerken	ja	
	25	xiv.veiligwerken	Gedeeltelijk	Art. 5.1 lid 2 sub e
	26	xiv.instructie.privacy	ja	
	27	xiv.inwerken	Gedeeltelijk	Art. 5.1 lid 2 sub e
	28	xiv.scholing	Ja	
	29	xiv.instructie	gedeeltelijk	Art. 5.1 lid 2 sub e
xv				
xvi				

ADDENDUM

Dienstverleningsovereenkomst op het gebied van bestrijding COVID 19

TUSSEN

Regio Gooi en Vechtstreek
Burgemeester de Bordesstraat 80
1404 GZ Bussum

EN

Bender Detachering B.V., gevestigd te Amsterdam

Kenmerk : [redacted]

Datum : 4 oktober 2021

Dit addendum behoort bij de Dienstverleningsovereenkomst tussen de Regio Gooi en Vechtstreek (opdrachtgever) en Bender Detachering B.V. (Contractant) met kenmerk [redacted] hierna samen te noemen: Partijen.

PARTIJEN KOMEN HET VOLGENDE OVEREEN:Overeenkomstig en ter effectuering van de bepaling, zoals vermeld in artikel 3 lid 2 van de Dienstverleningsovereenkomst, besluiten partijen de overeenkomst voort te zetten voor de duur van één (1) keer zes (6) maanden, te weten de periode 1 januari 2022 t/m 30 juni 2022.

- Deze overeenkomst kan door Opdrachtgever met een opzegtermijn van 30 kalenderdagen beëindigd worden, indien naar de mening van Opdrachtgever, de inzet niet meer nodig.

- De overige bepalingen en voorwaarden van de Overeenkomst van Opdracht waar dit addendum betrekking op heeft, blijven verder onverkort van toepassing.

Aldus opgemaakt en in tweevoud ondertekend,

Bussum, 4 oktober 2021

Regio Gooi en Vechtstreek

[redacted]

Manager RVE GGD

Amsterdam,

Bender Detachering B.V.

[redacted]

Directeur

DIENSTVERLENINGSOVEREENKOMST

inzake

dienstverlening op het gebied van bestrijding COVID 19

tussen

De Regio Gooi en Vechtstreek

en

Uw Zorgbemiddelaar

Kenmerk

DE ONDERGETEKENDEN:

De Regio Gooi en Vechtstreek, ten deze rechtsgeldig vertegenwoordigd door de RVE Manager GGD, hierna te noemen: Opdrachtgever

en

Uw Zorgbemiddelaar gevestigd te , ten deze rechtsgeldig vertegenwoordigd door , hierna te noemen: Contractant

gezamenlijk aan te duiden als "Partijen"

OVERWEGENDE:

1. dat Opdrachtgever voornemens is werkzaamheden te laten verrichten door artsen op het gebied van de bestrijding van COVID 19;
2. dat Contractant hiervoor Personeel kan plaatsen bij Opdrachtgever die de vereiste expertise bezitten om deze werkzaamheden uit te voeren;
3. dat Partijen hierover hun afspraken nader wensen vast te leggen in deze Overeenkomst,

KOMEN OVEREEN ALS VOLGT:

Artikel 1 Begrippen

In deze Overeenkomst 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 inkoopvoorwaarden Regio Gooi en Vechtstreek 2019 (hierna te noemen: Algemene inkoopvoorwaarden).

Artikel 2 Voorwerp van de overeenkomst

1. Opdrachtgever neemt gedurende de periode zoals bepaald in artikel 3 van deze overeenkomst, dienstverlening van Contractant af op het resultaatgebied bestrijding COVID 19, inzet artsen. De taken van de artsen staan beschreven in Bijlage 1.
2. De volgende Bijlagen maken integraal onderdeel uit van deze Overeenkomst:
   Bijlage 1. Taakkaart arts
   Bijlage 2. Algemene inkoopvoorwaarden Regio Gooi en Vechtstreek 2019
3. In geval van strijdigheid tussen deze Overeenkomst en een of meer van de in het vorige lid genoemde bijlagen, prevaleert het gestelde in de Overeenkomst.
4. Wijzigingen van deze Overeenkomst of aanvullingen daarop worden eerst rechtsgeldig en bindend voor Partijen, nadat zij schriftelijk, in de vorm van een aan deze overeenkomst te hechten bijlage, tussen Opdrachtgever en Contractant zijn overeen gekomen.
5. Op deze Overeenkomst zijn uitsluitend van toepassing de Algemene inkoopvoorwaarden Regio Gooi en Vechtstreek 2019, voor zover daar bij deze Overeenkomst niet van wordt afgeweken. De toepasselijkheid van (eventuele) algemene en bijzondere voorwaarden van Contractant zijn uitgesloten.

Artikel 3 Duur van de overeenkomst

1. De in het kader van deze Overeenkomst te verrichten Diensten worden gedurende de periode 1 mei 2021 tot 1 november 2021 uitgevoerd.
2. Deze Overeenkomst kan in onderling overleg maximaal twee (2) keer voor de duur van maximaal drie (3) maanden, worden verlengd onder gelijkblijvende voorwaarden. Indien Opdrachtgever en Contractant gebruik wensen te maken van de optie tot verlenging van de Dienstverlening, dan wordt voor deze uiterlijk één (1) maand voor het einde van de looptijd overeengekomen en schriftelijk vastgelegd in een bijvoegsel (addendum) op deze overeenkomst.
3. De overeenkomst kan verder door partijen tussentijds worden opgezegd, indien deze bevoegdheid van een partij uit de wet voortvloeit. De opzegging dient schriftelijk te geschieden onder opgave van redenen.

Artikel 4 Prijs en overige financiële bepalingen

1. Opdrachtgever betaalt Contractant voor het verrichten van werkzaamheden zoals genoemd in [redacted] per uur voor een junior arts en [redacted] een senior arts (exclusief BTW en weekendtoeslag conform cao SGO).
2. De onkosten van de Contractant zijn in de vergoeding van de Contractant inbegrepen. Onder onkosten vallen ook de parkeer-, en verblijfkosten, administratie - en telefoonkosten en alle andere overige onkosten van de Contractant.
3. Contractant brengt voor elke arts een reiskostenvergoeding var[redacted]n rekening.
4. Het uurtarief genoemd in het eerste lid en de reiskostenvergoeding genoemd in het derde lid, is vast en onveranderlijk gedurende de duur van deze Overeenkomst.
5. Partijen verklaren beiden uitdrukkelijk dat de Opdrachtgever buiten de overeengekomen vergoeding en onkosten voor het verrichten van de werkzaamheden welke in deze overeenkomst zijn overeengekomen geen betalingen is verschuldigd aan Contractant.

Artikel 5 Facturering

1. Contractant zal voor de verrichte werkzaamheden aan Opdrachtgever maandelijks een factuur (doen) zenden, voorzien van een urenspecificatie voor de ingezette arts(en).
   De factuur zal voldoen aan de wettelijke vereisten.
2. Facturen dienen digitaal te worden verzonden naar het mailadres: facturen@regiogv.nl.
   De factuur dient gericht te zijn aan 'Regio Gooi en Vechtstreek, ter attentie van de RVE GGD Burgemeester de Bordesstraat 80, 1440 GZ Bussum.
3. Voor betaling van facturen dient als betalingskenmerk altijd het nummer[redacted] op de factuur te worden vermeld.
4. Voor een adequate en snelle afhandeling van facturen moet op de factuur tevens worden vermeld:
   - kostenplaats: 533100
   - kostendrager: 501032
   - grootboekrek.: 41311

Artikel 6 Contactpersonen

Contactpersonen voor de uitvoering van deze overeenkomst zijn:
- voor de Opdrachtgever:
- voor de Contractant:
Contactpersonen kunnen Partijen alleen vertegenwoordigen en binden voor zover het betreft de uitvoering van deze Overeenkomst. Tot wijziging van deze Overeenkomst zijn zij niet bevoegd.

Artikel 7 Plaats uitvoering dienstverlening

De Diensten worden in beginsel verricht vanuit de vaccinatielocatie in Naarden en indien nodig vanuit andere (vaccinatie)locaties van de Opdrachtgever.

Artikel 8 Aansprakelijkheid

1. De door Contractant te vergoeden schade als bedoeld in artikel 14.2 van de Algemene inkoopvoorwaarden is beperkt tot maximaal één (1) maal het bedrag dat ingevolge deze Overeenkomst in totaliteit door Contractant aan Opdrachtgever kan worden gefactureerd.
2. Indien er sprake is van (voortijdige) opzegging van de Overeenkomst door een partij, dan dient eventuele schade die hieruit in redelijkheid voortvloeit vergoed te worden aan de andere partij.
3. Bij de aansprakelijkheidsverdeling tussen Opdrachtgever en Contractant dienen de normen van redelijkheid en billijkheid en de in de branche gebruikelijke beperkingen van aansprakelijkheid in acht te worden genomen.

Artikel 9 Ontbinding

Buiten hetgeen in artikel 21 van de Algemene inkoopvoorwaarden is bepaald, is Opdrachtgever gerechtigd, zonder dat enige aanmaning of ingebrekestelling is vereist, de Overeenkomst zonder rechterlijke tussenkomst door middel van een aangetekende brief met onmiddellijke ingang te ontbinden indien Contractant zich schuldig heeft gemaakt aan valse verklaringen bij het verstrekken van inlichtingen in het kader van de opdrachtverstrekking die heeft geleid tot gunning van deze Opdracht.

Artikel 10 Overige voorwaarden

1. Met 'tijdig' in artikel 7.2 van de Algemene inkoopvoorwaarden wordt onder deze overeenkomst bedoeld een periode van 1 werkdag.
2. Hoofdstuk III 'Koop en levering' van de Algemene inkoopvoorwaarden is niet van toepassing op deze overeenkomst.
3. Voor de uitvoering van de dienstverlening zoals omschreven in artikel 2 en overeenkomstig artikel 30 lid 4 van Algemene inkoopvoorwaarden, garandeert Contractant dat het in te zetten Personeel in het bezit is van een geldige Verklaring Omtrent Gedrag (VOG) als bedoeld in artikel 28 van de Wet justitiële en strafvorderlijke gegevens (WJSG), en overlegt deze verklaring(en) aan Opdrachtgever.
4. In navolging van artikel 30 lid 2 van de Algemene inkoopvoorwaarden stelt Opdrachtgever, voordat de uitvoering van de dienstverlening zoals omschreven in artikel 2 een aanvang neemt, de identiteit vast aan de hand van een geldig identiteitsbewijs van het Personeel van de Contractant. Het identiteitsbewijs (paspoort of identiteitskaart, geen rijbewijs) dient door het Personeel van de Contractant persoonlijk te worden overlegd aan Opdrachtgever.
5. Opdrachtgever verstrekt aan Contractant de 'gedragscode integriteit' inclusief een integriteitsverklaring. Personeel van Contractant dient te handelen in overeenstemming met deze gedragscode en verklaart dit door persoonlijke ondertekening van de integriteitsverklaring.

Artikel 11 Verwerkersovereenkomst

1. Indien Contractant persoonsgegevens verwerkt in haar systemen overeenkomstig de definitie van 'verwerking' zoals vastgelegd in artikel 4 van de EU Verordening 2016/679 (de Algemene verordening gegevensbescherming), dan dient op grond van deze verordening Opdrachtgever een verwerkersovereenkomst af te sluiten met Contractant. Indien van toepassing zal de ondertekende verwerkersovereenkomst onlosmakelijk deel uit maken van deze overeenkomst.

2. Pas nadat de separaat door Opdrachtgever opgestelde verwerkersovereenkomst door beide partijen is ondertekend worden persoonsgegevens door Opdrachtgever overgedragen aan Contractant.

Artikel 12 Slotbepalingen

1. Wijzigingen en afwijkingen van deze Overeenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen beide Partijen schriftelijk zijn overeengekomen.
2. Contractant dient Opdrachtgever van elke substantiële wijziging in de situatie van Contractant en/of diens bedrijf, die van invloed kan zijn op de uitvoering van deze Overeenkomst op de hoogte te stellen.

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

Bussum, 16-4-2021

Regio Gooi en Vechtstreek

Manager RVE GGD

Utrecht 16-4-2021

Uw Zorgbemiddelaar

CCO & Accounting manager UZB

Taakkaart arts

De arts is verantwoordelijk voor de medische onderdelen van het volledige vaccinatieproces op locatie. Op voorhand is de arts verantwoordelijk voor het beoordelen van eventuele contra-indicaties en tijdens en na de vaccinatie kan de arts opgeroepen worden in geval van post-vaccinale verschijnselen. Waar nodig verleent de arts eerste hulp en is hij verantwoordelijk voor het inschakelen van de juiste hulp.

Taken / verantwoordelijkheden op hoofdlijnen

A. Inrichten van vaccinatielocatie (samen met locatiehoofd);
B. Controleert dagelijks of de gebruikte documentatie (taakkaarten, landelijk draaiboek werkprocessen, RIVM vaccinatie richtlijn, etc.) en locatie inrichting nog up-to-date is (samen met locatiehoofd);
C. Geeft uitleg aan medewerkers in priklijn en borgt daarmee bekwaamheid en bevoegdheid van prikkers;
D. Houdt toezicht op de kwaliteit van het handelen van de prikkers;
E. Adviseert burger over vaccinatie indien één of meer van de triagevragen (gezondheidsverklaring) met 'ja' wordt beantwoord;
F. Adviseert burger over vervolgstap wanneer vaccin incorrect is toegediend;
G. Noteert eventuele incorrecte vaccinatie in het dossier van de burger (CoronIT) en maakt een MIC-melding;
H. Monitort de bijwerkingen op de GGD-locatie en registreert bijwerkingen in CoronIT;
I. Meldt bijwerkingen en ernstige post-vaccinale reacties aan het Bijwerkingencentrum Lareb;
J. Past eerste hulp toe indien nodig.

Additionele locatie specifieke taken / verantwoordelijkheden

K. De arts heeft pauze
van ____ tot ____
& van ____ tot ____
& van ____ tot ____

L. Additionele taken zijn (*door locatie zelf aan te vullen*):

Taken / verantwoordelijkheden van de arts in detail

A. <u>Inrichten van vaccinatielocatie (samen met locatiehoofd)</u>
   a. Tezamen met het locatiehoofd is de arts verantwoordelijk voor de inrichting van de vaccinatielocatie. De arts waarborgt hierbij voornamelijk de 'veilig werken richtlijn' zoals in bijlage 4 van de uitvoeringsrichtlijn[1] beschreven staat. Specifieke locatievereisten die relevant zijn voor de arts (en waar de arts medeverantwoordelijk voor is) zijn:
      i. Zorgt voor een af te sluiten ruimte voor een medicijnkoelkast (of de koelkast zelf dient afsluitbaar te zijn, zie uitvoeringsrichtlijn);
      ii. Zorgt voor een medicijnkoelkast (2-8°C (optimaal is 5°C), temperatuur monitoring, alarm, remote uitlezing, richtlijn inhoud 100 a 200L); Aanvullende specificaties bevinden zich in de uitvoeringsrichtlijn. Het IGJ toetsingskader spreekt verder van een 'noodvoorziening koeling/opslag', bijvoorbeeld twee koelkasten in combinatie met een noodstroomvoorziening;

iii. Zorgt voor een afsluitbare kamer voor hulpmiddelen (spuiten en naalden, oplosvloeistof, PBM's, pleisters, etc.);

iv. Zorgt voor voldoende privacy voor degene die gevaccineerd wordt, bijvoorbeeld door middel van schermen rondom het vaccinatiepunt;

v. Zorgt voor mogelijkheden voor personen die liggend gevaccineerd moeten worden;

vi. Creëert een wachtruimte voor 15 minuten na vaccineren (vijf stoelen per priklijn, stoelen op voldoende afstand, maximaal 30 personen wachtend per ruimte, EHBO'er / surveillance in ruimte). Aandacht voor looproute, dus bij voorkeur gescheiden in- en uitgang;

vii. Zorgt voor aanwezigheid van een behandelkamer voor eerste hulp bij shock, een protocol incidenten (uitvoeringsrichtlijn) en een EHBO kit;

viii. Zorgt voor een afsluitbare ruimte voor medisch afval. (Lege) vaccin flacons en spuiten dienen in een Wiva vat gedeponeerd worden. De naalden moeten in de naalden container.

B. Controleert dagelijks of de gebruikte documentatie (taakkaarten, landelijk draaiboek werkprocessen, RIVM vaccinatie richtlijn, etc.) en locatie-inrichting nog up-to-date is (samen met locatiehoofd)

a. Controleert en waarborgt dagelijks de bij stap A benoemde locatie-inrichting;

b. Controleert dagelijks, voor aanvang van de dagstart, of er updates geplaatst zijn op GGD kennisnet van RIVM vaccinatierichtlijnen, het landelijk draaiboek werkprocessenen/of werkbeschrijvingen. De arts communiceert hierover met het locatiehoofd in het geval medische richtlijnen veranderen;

c. Bij wijzigingen ondersteunt de arts het locatiehoofd bij het doorvoeren van de veranderingen in de eigen vaccinatielocatie, zodat deze gedeeld kunnen worden gedurende de dagelijkse dagstart;

d. Draagt zorg voor het beschikbaar hebben van de juiste documentatie, zoals taakkaarten en het landelijk draaiboek werkprocessen, voor medewerkers in de priklijn en dient derhalve zorg te dragen voor geprinte versies van eventuele updates van documenten.

C. Geeft uitleg aan medewerkers in priklijn en borgt daarmee bekwaamheid en bevoegdheid van prikkers

a. Geeft uitleg aan alle vaccinatiemedewerkers die medische handelingen gaan verrichten of omgaan met medische gegevens (werkvoorbereiders, prikkers, administratoren).

i. Arts introduceert zichzelf aan alle medewerkers in de priklijn;

ii. Instrueert de vaccinatiemedewerkers: zorgt dat duidelijk is wie bij welke priklijn aan de slag gaat, welke werkbeschrijvingen relevant zijn voor werkvoorbereiders, prikkers en administratoren;

iii. Instrueert de administratoren dat de burger zich dient te melden bij de arts zodra er bij één van de triagevragen (gezondheidsverklaring) een "ja" is geantwoord.

D. Houdt toezicht op de kwaliteit van het handelen van de prikkers

a. Gedurende de werkzaamheden van de arts, is de arts ook actief bezig met toezicht houden op de kwaliteit van handelen van de prikkers. De arts geeft proactief advies aan prikkers als het opvalt dat een bepaalde handeling beter uitgevoerd kan worden.

E. Adviseert burger over vaccinatie indien één of meer van de triagevragen (gezondheidsverklaring) met 'ja' wordt beantwoord

a. Burger wordt door administrator (of op sommige locaties, de host) verwezen naar de arts indien één of meer van de triagevragen in de gezondheidsverklaring met 'ja' is beantwoord. De arts adviseert de burger over vervolgstappen na bespreking van de contra-indicatie met de burger; [Er komt een stroomdiagram voor artsen op Kennisnet beschikbaar om hier ondersteuning bij te bieden]

b. Afhankelijk van of er gevaccineerd kan worden, adviseert de arts ook de prikker over hoe te prikken en waar er specifiek op gelet moet worden bij een bepaalde burger.

F. Adviseert burger over vervolgstap wanneer vaccin incorrect is toegediend;

a. *Te weinig vaccin toegediend:* De arts adviseert burger over eventueel opnieuw toedienen van het vaccin. Wanneer er te weinig vaccin is toegediend, kan de burger in principe direct opnieuw worden gevaccineerd (met een volledige nieuwe dosis vaccin);

b. *Te veel vaccin toegediend:* De burger hoeft niet opnieuw met de juiste dosis te worden gevaccineerd. De arts adviseert burger over mogelijke vergrootte bijwerkingen in het geval van een dubbele dosis, of multidoses (5 doses totaal). Het is verder niet schadelijk, wel aanleiding tot extra zorg voor de gevaccineerde. De meeste bijwerkingen zijn mild en binnen een tot twee dagen verdwenen. Als pijn of koorts toch heftig is, kan hiervoor paracetamol worden ingenomen. De volgende klachten komen vaak voor:

i. Pijn op de injectieplaats, meestal zonder roodheid en zwelling;
ii. Vermoeidheid;
iii. Hoofdpijn;
iv. Spierpijn;
v. Rillingen;
vi. Gewrichtspijn;
vii. Koorts.

c. *Vaccin foutief toegediend*: De arts adviseert burger over eventueel opnieuw toedienen van het vaccin. Bij toediening van enkel oplosvloeistof wordt de vaccinatie als niet toegediend beschouwd. Indien er te veel oplosvloeistof is toegevoegd en het actieve deel van het vaccin te veel verdund is, moet de vaccinatie ook opnieuw met de correcte menging, zodra de fout ontdekt is. Mocht foutieve toediening pas ontdekt worden als de burger niet meer op locatie is, dan dient er contact met de burger te worden opgenomen om uitleg te geven en een nieuwe afspraak te maken;

d. *Te oud vaccin toegediend:* De arts adviseert burger over eventueel opnieuw toedienen van het vaccin. Bij toediening van te oud vaccin kan de werking niet meer worden gegarandeerd. De vaccinatie moet opnieuw worden toegediend. Mocht toediening van te oud vaccin pas ontdekt worden als de burger niet meer op locatie is, dan dient er contact met de burger te worden opgenomen om uitleg te geven en een nieuwe afspraak te maken;

e. *Prikaccident prikker/burger, burger/ prikker:* De arts volgt het protocol omtrent prikaccidenten (verschilt per lokale GGD). De richtlijnen voor prikaccidenten komen wel bij het RIVM vandaan en kunnen hier gevonden worden.

G. Noteert eventuele incorrecte vaccinatie in het dossier van de burger (CoronIT) en maakt een MIC-melding

a. De arts registreert onjuiste toediening van het vaccin (te weinig vaccin toegediend, te veel vaccin toegediend, vaccin foutief toegediend, te oud vaccin toegediend, prikaccident). De arts:

i. Maakt een MIC (meldingen incidenten cliënten)-melding;
ii. Registreert de foutieve toediening in CoronIT. Dit kan in het opmerkingenveld op de gezondheidsverklaring (in de eerste ronde) of het formulier tweede intake (in de tweede ronde). Zie hoofdstuk vier van de werkinstructie van CoronIT.

H. Monitort de bijwerkingen op de GGD-locatie en registreert bijwerkingen in CoronIT

a. De arts monitort op locatie of burgers bijwerkingen ervaren van de vaccinatie. Als dit het geval is, dan dient de arts dit te registreren. Dit dient geregistreerd te worden in het profiel van de burger in CoronIT. De instructie voor hoe dit moet, is te vinden in de werkinstructie 'vaccineren'.

I. Meldt bijwerkingen en ernstige post-vaccinale reacties aan het Bijwerkingencentrum Lareb.

a. De arts heeft de verplichting om elke bijwerking en ernstige post-vaccinale reactie te melden aan het Lareb door een speciaal hiervoor opgesteld formulier in te vullen. De burger dient toestemming te verlenen voor het doorgeven van relevante (medische) informatie aan Lareb. Noteer ook in CoronIT of de burger wel/geen toestemming gegeven heeft hiervoor. Hoe de melding aan het Lareb gedaan kan worden, staat uitgelegd in de werkinstructie CoronIT 'medische beoordeling en bijwerkingen';

b. Registratie bij Lareb dient te gebeuren in de volgende gevallen:

i. Ernstige gebeurtenissen, zoals ziekenhuisopnames, blijvende invaliditeit of overlijden, ongeacht het vermeende causale verband;

ii. Onverwachte of bijzondere bijwerkingen;

iii. Twijfel over vervolgvaccinaties;

iv. Onrust of negatieve publiciteit;

v. Alles wat u verder van belang vindt.;

c. Bij melding van post vaccinale reacties moet het batchnummer van het betreffende vaccin worden toegevoegd aan de registratie.

J. <u>Past eerste hulp toe indien nodig</u>

a. Mocht er op locatie iets voorvallen met een burger, dan is de arts verantwoordelijk voor adequate hulpverlening. De arts zal normaliter ingelicht worden over een voorval door een EHBO-er die toezicht houdt op de wachtruimte. Informeer altijd op locatie welke communicatiemethode hiervoor afgesproken is (zoals telefoon, portofoon, etc).;

b. De arts heeft voor het goed kunnen uitvoeren van eerste hulp een noodkit met stappenplan, een defibrillator en medicatie (o.m. adrenaline / epipen) nodig. De arts zet deze middelen naar eigen inzicht in waar hij dit benodigd acht;

c. De arts is verantwoordelijk voor het laten inschakelen van de gepaste hulp (denk aan bijv. traumahelikopter, ambulance, etc).

DIENSTVERLENINGSOVEREENKOMST

Inzake

dienstverlening op het gebied van bestrijding COVID 19

tussen

De Regio Gooi en Vechtstreek

en

Bender detachering B.V.

Kenmerk:

DE ONDERGETEKENDEN:

De Regio Gooi en Vechtstreek, ten deze rechtsgeldig vertegenwoordigd door
RVE Manager GGD, hierna te noemen: Opdrachtgever

en

Bender Detachering B.V., gevestigd te Amsterdam, ten deze rechtsgeldig vertegenwoordigd door de bestuurder, hierna te noemen: Contractant

gezamenlijk aan te duiden als "Partijen"

OVERWEGENDE:

1. dat Opdrachtgever voornemens is werkzaamheden te laten verrichten op het gebied van de bestrijding van COVID 19 (callcenter, testen, bron- en contactonderzoek, vaccineren) ;
2. dat Opdrachtgever een vooraankondiging met kenmerk heeft gepubliceerd van de voorgenomen gunning van de opdracht aan Bender Detachering B.V.;
3. dat op deze vooraankondiging geen bezwaar is aangetekend;
4. dat Contractant hiervoor Professionals kan plaatsen bij Opdrachtgever die de vereiste expertise bezitten om deze werkzaamheden uit te voeren;
5. dat Partijen hierover hun afspraken nader wensen vast te leggen in deze Overeenkomst,

KOMEN OVEREEN ALS VOLGT:

Artikel 1 Begrippen

In deze Overeenkomst 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 inkoopvoorwaarden Regio Gooi en Vechtstreek 2019 (hierna te noemen: Algemene inkoopvoorwaarden).

Artikel 2 Voorwerp van de overeenkomst

1. Opdrachtgever neemt gedurende de periode zoals bepaald in artikel 3 van deze overeenkomst voor 24 tot 36 uur per Professional per week, dienstverlening van Contractant af op het resultaatgebied bestrijding COVID 19. Het resultaatgebied staat beschreven in Bijlage 1.
2. De volgende Bijlagen maken integraal onderdeel uit van deze Overeenkomst:
   Bijlage 1. Beschrijving van de dienstverlening op het resultaatgebied.
   Bijlage 2. Algemene inkoopvoorwaarden Regio Gooi en Vechtstreek 2019In geval van strijdigheid tussen deze Overeenkomst en een of meer van de in het vorige lid genoemde bijlagen, prevaleert het gestelde in de Overeenkomst.
4. Wijzigingen van deze Overeenkomst of aanvullingen daarop worden eerst rechtsgeldig en bindend voor Partijen, nadat zij schriftelijk, in de vorm van een aan deze overeenkomst te hechten bijlage, tussen Opdrachtgever en Contractant zijn overeen gekomen.
5. Op deze Overeenkomst zijn uitsluitend van toepassing de Algemene inkoopvoorwaarden Regio Gooi en Vechtstreek 2019, voor zover daar bij deze Overeenkomst niet van wordt afgeweken. De toepasselijkheid van (eventuele) algemene en bijzondere voorwaarden van Contractant zijn uitgesloten.

Artikel 3 Duur van de overeenkomst

1. De in het kader van deze Overeenkomst te verrichten Diensten worden gedurende de periode 1 maart 2021 tot 1 januari 2022 uitgevoerd.
2. Deze Overeenkomst kan in onderling overleg maximaal twee (2) keer voor de duur van maximaal drie (3) maanden, worden verlengd onder gelijkblijvende voorwaarden. Indien Opdrachtgever en Contractant gebruik wensen te maken van de optie tot verlenging van de Dienstverlening, dan wordt voor deze uiterlijk één (1) maand voor het einde van de looptijd overeengekomen en schriftelijk vastgelegd in een bijvoegsel (addendum) op deze overeenkomst.
3. De overeenkomst kan verder door partijen tussentijds worden opgezegd, indien deze bevoegdheid van een partij uit de wet voortvloeit. De opzegging dient schriftelijk te geschieden onder opgave van redenen.

Artikel 4 Prijs en overige financiële bepalingen

1. Opdrachtgever betaalt Contractant voor het verrichten van werkzaamheden zoals genoemd in Bijlage 1 [redacted] (exclusief BTW en weekendtoeslag conform cao SGO) met een maximum van 36 uur per week per Professional. Voor overige werkzaamheden / profielen (o.a. arts, teamcoördinator) wordt het tarief na overleg bepaald.
2. De onkosten van de Contractant zijn in de vergoeding van de Contractant inbegrepen. Onder onkosten vallen ook de parkeer-, en verblijfkosten, administratie - en telefoonkosten en alle andere overige onkosten van de Contractant.
3. Contractant brengt voor elke Professional een [redacted] per dag in rekening. Daarnaast wordt voor het uitvoeren van de werkzaamheden een mobiele telefoon van Opdrachtgever ter beschikking gesteld.
4. Het uurtarief genoemd in het eerste lid en de reiskostenvergoeding genoemd in het derde lid, is vast en onveranderlijk gedurende de duur van deze Overeenkomst.
5. Partijen verklaren beiden uitdrukkelijk dat de Opdrachtgever buiten de overeengekomen vergoeding en onkosten voor het verrichten van de werkzaamheden welke in deze overeenkomst zijn overeengekomen geen betalingen is verschuldigd aan Contractant.

Artikel 5 Facturering

1. Contractant zal voor de verrichte werkzaamheden aan Opdrachtgever maandelijks een factuur (doen) zenden, voorzien van een urenspecificatie voor de ingezette Professional(s). De factuur zal voldoen aan de wettelijke vereisten.
2. Facturen dienen digitaal te worden verzonden naar het mailadres: facturen@regiogv.nl. De factuur dient gericht te zijn aan 'Regio Gooi en Vechtstreek, ter attentie van de RVE GGD Burgemeester de Bordesstraat 80, 1440 GZ Bussum.
3. Voor betaling van facturen dient als betalingskenmerk altijd het nummer [redacted] op de factuur te worden vermeld.
4. Voor een adequate en snelle afhandeling van facturen moet op de factuur tevens worden vermeld:
   - kostenplaats: 533100
   - kostendrager: 501032
   - grootboekrek.: 41311

Artikel 6 Contactpersonen

Contactpersonen voor de uitvoering van deze overeenkomst zijn:
- voor de Opdrachtgever:

- voor de Contractant:
Contactpersonen kunnen Partijen alleen vertegenwoordigen en binden voor zover het betreft de uitvoering van deze Overeenkomst. Tot wijziging van deze Overeenkomst zijn zij niet bevoegd.

Artikel 7 Plaats uitvoering dienstverlening

De Diensten worden in beginsel verricht vanuit meerdere locaties van de Opdrachtgever en daar waar mogelijk vanuit huis (bijv. medewerker BCO/callcenter).

Artikel 8 Aansprakelijkheid

1. De door Contractant te vergoeden schade als bedoeld in artikel 14.2 van de Algemene inkoopvoorwaarden is beperkt tot maximaal één (1) maal het bedrag dat ingevolge deze Overeenkomst in totaliteit door Contractant aan Opdrachtgever kan worden gefactureerd.
2. Indien er sprake is van (voortijdige) opzegging van de Overeenkomst door een partij, dan dient eventuele schade die hieruit in redelijkheid voortvloeit vergoed te worden aan de andere partij.
3. Bij de aansprakelijkheidsverdeling tussen Opdrachtgever en Contractant dienen de normen van redelijkheid en billijkheid en de in de branche gebruikelijke beperkingen van aansprakelijkheid in acht te worden genomen.

Artikel 9 Ontbinding

Buiten hetgeen in artikel 21 van de Algemene inkoopvoorwaarden is bepaald, is Opdrachtgever gerechtigd, zonder dat enige aanmaning of ingebrekestelling is vereist, de Overeenkomst zonder rechterlijke tussenkomst door middel van een aangetekende brief met onmiddellijke ingang te ontbinden indien Contractant zich schuldig heeft gemaakt aan valse verklaringen bij het verstrekken van inlichtingen in het kader van de opdrachtverstrekking die heeft geleid tot gunning van deze Opdracht.

Artikel 10 Overige voorwaarden

1. Met 'tijdig' in artikel 7.2 van de Algemene inkoopvoorwaarden wordt onder deze overeenkomst bedoeld een periode van 1 werkdag.
2. Hoofdstuk III 'Koop en levering' van de Algemene inkoopvoorwaarden is niet van toepassing op deze overeenkomst.
3. Voor de uitvoering van de dienstverlening zoals omschreven in artikel 2 en overeenkomstig artikel 30 lid 4 van Algemene inkoopvoorwaarden, garandeert Contractant dat hij/zij in het bezit is van een geldige Verklaring Omtrent Gedrag (VOG) als bedoeld in artikel 28 van de Wet justitiële en strafvorderlijke gegevens (WJSG), en overlegt deze verklaring(en) aan Opdrachtgever.
4. In navolging van artikel 30 lid 2 van de Algemene inkoopvoorwaarden stelt Opdrachtgever, voordat de uitvoering van de dienstverlening zoals omschreven in artikel 2 een aanvang neemt, de identiteit vast aan de hand van een geldig identiteitsbewijs van Contractant.
Het identiteitsbewijs (paspoort of identiteitskaart, geen rijbewijs) dient door Contractant persoonlijk te worden overlegd.
5. Opdrachtgever verstrekt aan Contractant de 'gedragscode integriteit' inclusief een integriteitsverklaring. Contractant dient te handelen in overeenstemming met deze gedragscode en verklaart dit door persoonlijke ondertekening van de integriteitsverklaring.

Artikel 11 Verwerkersovereenkomst

1. Indien Contractant persoonsgegevens verwerkt in haar systemen overeenkomstig de definitie van 'verwerking' zoals vastgelegd in artikel 4 van de EU Verordening 2016/679 (de Algemene verordening gegevensbescherming), dan dient op grond van deze verordening Opdrachtgever een verwerkersovereenkomst af te sluiten met Contractant. Indien van toepassing zal de ondertekende verwerkersovereenkomst onlosmakelijk deel uit maken van deze overeenkomst.
2. Pas nadat de separaat door Opdrachtgever opgestelde verwerkersovereenkomst door beide partijen is ondertekend worden persoonsgegevens door Opdrachtgever overgedragen aan Contractant.

Artikel 12 Slotbepalingen

1. Wijzigingen en afwijkingen van deze Overeenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen beide Partijen schriftelijk zijn overeengekomen.
2. Contractant dient Opdrachtgever van elke substantiële wijziging in de situatie van Contractant en/of diens bedrijf, die van invloed kan zijn op de uitvoering van deze Overeenkomst op de hoogte te stellen.

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

Bussum, 26-02-2021	Amsterdam, d.d. 26-02-2021 .....
Regio Gooi en Vechtstreek	Bender detachering B.V.
	
Manager RVE GGD	Directeur

Bijlage 1 De dienstverlening/werkzaamheden van Contractant betreft het volgende resultaatgebied.

Per resultaatgebied een teamleider en dagcoördinator(en) conform organisatiestructuur en taakkaarten. De werkzaamheden bestaan minimaal uit:

Callcenter
- Het telefonisch en schriftelijk beantwoorden van vragen van burgers m.b.t. corona
- Het inplannen van afspraken middels CoronIT

Teststraat
- Het afnemen van coronatesten in de teststraat conform richtlijnen
- Het assisteren bij het afnemen van de coronatesten in de teststraat middels CoronIT

BCO
- Het uitvoeren van Bron- en Contactonderzoek conform de richtlijnen
- Het verwerken van (lab)gegevens in HPZone/Osiris en CoronIT

Vaccinatie
- Het administreren en registreren bij het vaccineren middels CoronIT
- Het voorbereiden en toedienen van vaccins conform de richtlijnen

ADDENDUM

Dienstverleningsovereenkomst op het gebied van bestrijding COVID 19

TUSSEN

Regio Gooi en Vechtstreek
Burgemeester de Bordesstraat 80
1404 GZ Bussum

EN

Uw Zorgbemiddelaar, gevestigd te Utrecht

Kenmerk : [redacted]

Datum : 4 oktober 2021

Dit addendum behoort bij de Dienstverleningsovereenkomst tussen de Regio Gooi en Vechtstreek (opdrachtgever) en Uw zorgbemiddelaar (Contractant) met kenmerk [redacted] hierna samen te noemen: Partijen.

PARTIJEN KOMEN HET VOLGENDE OVEREEN:Overeenkomstig en ter effectuering van de bepaling, zoals vermeld in artikel 3 lid 2 van de Dienstverleningsovereenkomst, besluiten partijen de overeenkomst voort te zetten voor de duur van één (1) keer zes (6) maanden, te weten de periode 1 november 2021 t/m 30 april 2022.

- Deze overeenkomst kan door Opdrachtgever met een opzegtermijn van 30 kalenderdagen beëindigd worden, indien naar de mening van Opdrachtgever, de inzet niet meer nodig.

- De overige bepalingen en voorwaarden van de Overeenkomst van Opdracht waar dit addendum betrekking op heeft, blijven verder onverkort van toepassing.

Aldus opgemaakt en in tweevoud ondertekend,

Bussum, 4 oktober 2021

Regio Gooi en Vechtstreek

Manager RVE GGD

Utrecht,

Uw Zorgbemiddelaar

CCO & Accounting manager UZBD

ADDENDUM

BIJ DE DIENSTVERLENINGSOVEREENKOMST

TUSSEN

Regio Gooi en Vechtstreek
Burgemeester de Bordesstraat 80
1404 GZ Bussum

EN

Uw Zorgbemiddelaar
Gevestigd te Utrecht

Kenmerk : [redacted]

Datum : 28 maart 2022

Dit addendum behoort bij de dienstverleningsovereenkomst tussen de Regio Gooi en Vechtstreek (opdrachtgever) en Uw zorgbemiddelaar (opdrachtnemer) met kenmerk 21.0003058 , hierna samen te noemen: Partijen.

PARTIJEN KOMEN HET VOLGENDE OVEREEN:

Overeenkomstig en ter effectuering van de bepaling, zoals vermeld in artikel 3 lid 2 van de dienstverleningsovereenkomst, besluiten partijen de overeenkomst voort te zetten voor de duur van één (1) keer vier (4) maanden, te weten de periode 1 mei 2022 t/m 31 augustus 2022 .

Deze overeenkomst kan door Opdrachtgever met een opzegtermijn van 30 kalenderdagen beëindigd worden, indien naar de mening van Opdrachtgever, de inzet niet meer nodig is.

De overige bepalingen en voorwaarden van de dienstverleningsovereenkomst waar dit addendum betrekking op heeft, blijven verder onverkort van toepassing.

Aldus opgemaakt en in tweevoud ondertekend,

Bussum, 28 maart 2022

Regio Gooi en Vechtstreek

Manager RVE GGD

Utrecht,

Uw Zorgbemiddelaar

CCO & Accounting manager UZBD,

OFFERTE

Uw
Zorgbemiddelaar

Paraaf

Offerte

Uw Zorgbemiddelaar Uitzendbureau – Doelgroep specialist sinds 2018

Wij zijn landelijk actief en leveren Mbo (18%) , Hbo (27%) & Wo (55%) studenten, starters, ervaren deskundigen en specialisten in alle segmenten van de medische arbeidsmarkt: van student tot aanstormend talent, van adhoc tot vaste baan.

500		78UUR		167	
Relaties en opdrachtgevers	Groot netwerk onder Hogescholen en Universiteiten	78 uur per week geopend (7 dagen per week). Doordeweeks van 07:00 tot 19:00 uur	Unieke en exclusieve database met ruim 5.000 kandidaten	Werkende UZB-ers per week	Onze uitzendkrachten worden zorgbreed onderverdeeld in verschillende specialisaties

Specialisaties: Office, Logistiek, Klantcontact en Smart Hands

Uw aanvraag komt terecht bij één van onze specialisaties. Per specialisatie onderwerpen wij onze studenten aan relevante tests/assessments. Zo volgen administratief medewerkers een nauwkeurigheidstest en logistiek medewerkers een snelheidstest. Andere testen zijn onze taaltesten, intelligentietesten en de normen & waarden academie. Onder de afdeling Smart Hands verstaan wij alle klussen en bijbanen waar slimme inzet voor vereist is.
Binnen deze specialisaties werken wij met ervaren Recruiters die bekend zijn met de uitdagingen binnen uw branche en uw organisatie.

Klantcontact

Logistiek

Smart Hands

Office

De 7 stappen van ons selectieproces

Door middel van onze uitgebreide selectieprocedure selecteren wij enkel de beste kandidaten:

- Mailing en matching
- Gerichte sollicitatie van de kandidaat
- Telefonische selectie
- Persoonlijk sollicitatiegesprek bij Uw Zorgbemiddelaar
- Optie: Assessment en/of training
- Optie: Videovoorstel
- Uw Zorgbemiddelaar stelt een kandidaat aan u voor
- Optie: Bij u op gesprek
- Start uitzendkracht
- Betrokkenheid Uw Zorgbemiddelaar

Na de start van een kandidaat blijft Uw Zorgbemiddelaar betrokken bij u en bij de starter(s). Wij houden de voortgang in de gaten en zullen regelmatig evaluatiemomenten inplannen en staan klaar voor vragen en opmerkingen.

Paraaf

.

FUNCTIE

Functies: Bron - en contactonderzoek Medewerkers, Vaccinatie Medewerkers, Callcenter Medewerkers, Teststraat Medewerkers en Basisartsen.

Werkzaamheden:

Persoonskenmerken:

- HBO/WO werk- & denkniveau;
- Relevante (para)medische studie achtergrond:
- Representatief;
- Goede communicatieve en sociale vaardigheden;
- Accuraat;
- Geïnteresseerd in de thematiek of maakt deze kennis zich snel eigen;
- Maatschappelijk betrokken, empathisch;
- Stressbestendig, staat stevig in de schoenen;
- Werkt netjes, precies, secuur en gestructureerd;
- Biedt een luisterend oor en is professioneel;
- Beschikbaar voor minimaal 2 tot 4 dagen per week;
- Aansluitende beschikbaarheid;
- In het bezit van eigen vervoer;
- Eventuele verdere eisen in nader overleg

LOONVERHOUDINGSVOORSCHRIFT

Het uurtarief is vastgesteld op basis van de met u gemaakte afspraken met betrekking tot de ter beschikking stelling van de uitzendkracht(en) en de door u verstrekte informatie inzake CAO en inschaling (loon). Eventuele wijzigingen en/of correcties graag doorgeven, dan passen wij deze in overleg aan. Wij hanteren deze afspraken tot nader order*

Nr	Onderwerp	Opgenomen administratie Uw Zorgbemiddelaar
1	Inschaling conform	Nader overeen te komen
2	Formele CAO naam + SBI Code	Nader overeen te komen
3	Intern beleid	Nader overeen te komen
4	Intern beleid afgeleide van CAO	Nader overeen te komen
5	Volgt u een Loontabel/ Salarishuis	Nader overeen te komen
6	Arbeidsduur per week (regulier)	Nader overeen te komen
7	Formele functiebenaming	Nader overeen te komen
8	Zijn er meerdere medewerkers in dezelfde functie werkzaam	Nader overeen te komen
9	Inschaling per functie	Functiegroep/ Schaal: Nader overeen te komen Functietrede: Nader overeen te komen
10	Brutoloon	Nader overeen te komen
11	Onregelmatigheidtoeslagen	Nader overeen te komen
12	Overwerktoeslag	Nader overeen te komen
13	Toepassing periodieke loonsverhoging	Nader overeen te komen
14	Data initiële verhogingen	Nader overeen te komen
15	Reiskostenvergoeding:	Nader overeen te komen
16	Reisuren/- tijd vergoeding:	Nader overeen te komen
17	Overige kostenvergoeding	Nader overeen te komen
18	ATV/ ADV	Nader overeen te komen
19	Overige afspraken	Nader overeen te komen

**Bovenstaande informatie ontlenen wij uit onze interpretatie van de CAO/inlenersbeloning. Indien dit onjuist of incompleet is of uw onderneming hiervan afwijkt vernemen wij dit graag van u. Door middel van een ondertekende CAO Matrix kan* Uw Zorgbemiddelaar *extra functies toevoegen aan de voorwaarden zoals vastgelegd in deze offerte.*

Offerte

Uw Zorgbemiddelaar
HEALTHCARE SPECIALIST

Paraaf

TARIEF

Voor de bovenstaande functie(s) hanteren wij de vaste lage . Het tarief berekent u door het bruto uurloon te vermenigvuldigen met de factor. Ons uurtarief is exclusief 21% BTW.

Rekenvoorbeeld tarief: Bij een loon van u betaalt Uw Zorgbemiddelaar een bedrag van per uur.

Het uurtarief is een ALL-IN bedrag. Werving, selectie, administratie en planning zijn inbegrepen. Tevens het brutoloon, compleet werkgeversdeel, vakantiegeld, vakantiedagen, verzekeringen salarisspecificaties en jaaropgaven.

OVERIGE VOORWAARDEN

Kortingsregeling
Bij een bepaalde afname van uren per week kunnen wij de volgende kortingsregeling aanbieden:

0 t/m 50	=	geen korting over alle ingeleende uren ten opzichte van het regulier
50 t/m 100	=	uurtarief over alle ingeleende uren ten opzichte van het regulier
100 of meer	=	uurtarief

No Cure No Pay
Voor alle opdrachten werken wij op "No Cure, No Pay basis". Het uurtarief geldt enkel per daadwerkelijk gewerkt uur.

Oproep
Ter bescherming van de uitzendkracht geldt een minimale afname van 4 uur (per persoon) per oproep.

Paraaf

ZIJ KIEZEN OOK VOOR UW ZORGBEMIDDELAAR

VOORWAARDEN VAN OVEREENKOMST

1. Uw Zorgbemiddelaar verplicht zich tot vertrouwelijke behandelingen en tot geheimhouding jegens derden van alle gegevens en informatie, welke haar omtrent de organisatie en bedrijfsvoering van Inlener worden toevertrouwd.

2. Uw Zorgbemiddelaar draagt er zorg voor, dat de aan Inlener ter beschikking gestelde uitzendkrachten:
   - in redelijkheid voldoen aan de door haar gestelde functie-eisen;
   - overeengekomen zijn welke werkzaamheden zij gaan verrichten;
   - bij verhindering van de te verrichten arbeid wegens ziekte, daarvan tijdig, dat wil zeggen voordat de werkzaamheden normaliter zouden aanvangen, mededeling doen aan zowel Inlener als ook aan Uw Zorgbemiddelaar;
   - in alle gevallen van verhindering daarvan zo vroeg mogelijk mededeling doen en, voor zover dit redelijkerwijs verlangd kan worden, overleg plegen met Inlener

3. Payroll binnen deze overeenkomst is uitgesloten. Voor alle medewerkers heeft Uw Zorgbemiddelaar de werving verricht en geldt er een uitsluiting van exclusiviteit voor de opdrachtgever.

4. Uw Zorgbemiddelaar is afhankelijk van de door Inlener juiste verstrekte informatie betreffende de inleners cao en/of inschaling en aanvullende arbeidsvoorwaarden. Eventuele onjuistheden kunnen achteraf worden gecorrigeerd en doorberekend.

5. De tarieven zoals genoemd in dit samenwerkingsvoorstel, zijn exclusief BTW en eventuele reis- en/of verblijfskosten. De tarieven zijn van toepassing op uitzendkrachten in fase 1 en fase 2 volgens de NBBU CAO. De tarieven blijven van toepassing totdat wijzigingen, verstrekt door de bedrijfsvereniging en/of brancheorganisaties, een aanpassing noodzakelijk maken. Tevens zullen tariefaanpassingen door wettelijke en/of sociale maatregelen doorgevoerd worden. Voor fase 3 uitzendkrachten volgens de NBBU CAO geldt er een toeslag

Paraaf

Offerte

Uw Zorgbemiddelaar
HEALTHCARE SPECIALIST

6. Inlener heeft geen afnameverplichting bij start werkzaamheden. Na 1 jaar gewerkt te hebben voor Uw Zorgbemiddelaar heeft de uitzendkracht recht op een contract met vaste uren(de hoeveelheid uur is gebaseerd op het gemiddeld aantal gewerkte uren in dat jaar). Uw Zorgbemiddelaar informeert Inlener over de rechten en plichten voor de uitzendkracht.

7. Indien de opdracht vervalt en c.q. geen doorgang vindt, dient dat door de opdrachtgever 4 werkdagen voor aanvang van de dienst te worden gemeld bij Uw Zorgbemiddelaar. Indien deze tijd niet in acht is genomen en de uitzendkracht beschikbaar is gesteld c.q. gepland voor uw opdracht, dan krijgt de uitzendkracht de volledige dienst uitbetaald en brengt Uw Zorgbemiddelaar de volledige dienst in rekening tegen het afgesproken tarief.

8. De opdrachtgever is vrij na 1040 gefactureerde uren, per uitzendkracht, de flexkracht zonder bijkomende kosten over te nemen. Indien de opdrachtgever besluit een flexkracht eerder dan bovengenoemde uren een contract aan te bieden is zij Uw Zorgbemiddelaar een afkoopfee verschuldigd van de niet gegenereerde uren vermenigvuldigd met de op dat moment gehanteerde nominale marge. Indien een uitzendkracht gaat werken bij een gelieerde onderneming geldt dezelfde afkoopfee (Holding, moedermaatschappijen of andere gelieerde Bv's) of wordt het reguliere uurtarief voortgezet.

9. Uw Zorgbemiddelaar zal Inlener per week factureren middels een gespecificeerde factuur. Inlener zal de factuurbedragen voldoen binnen 14 dagen na de factuurdatum tenzij de facturen onjuistheden bevatten. Alleen indien Inlener melding doet van deze onjuistheden binnen 8 werkdagen na ontvangst van de factuur zal deze reclamatie in behandeling worden genomen. Nadien wordt de factuur akkoord bevonden.

10. Uitzendkrachten vallen onder de bedrijfs-WA-verzekering van de opdrachtgever.

11. Alle transitievergoedingen worden, indien van toepassing, op basis van kostprijs aan u doorberekend en gefactureerd (zie www.nbbu.nl).

12. Inlener stelt op aanvraag de RI&E ter beschikking aan de uitzendkracht van Uw Zorgbemiddelaar.

13. Indien Inlener uitzendkrachten zelf (besproken tussen Inlener en uitzendkracht) inplant is deze gebonden aan de arbeidstijdenwet. Indien de arbeidstijdenwet overtreden wordt ligt de verantwoordelijkheid bij Inlener.

14. Indien de uitzendkracht(en) 6 weken of langer niet wordt opgeroepen, wordt de opdracht met terugwerkende kracht beëindigd na de laatst gewerkte dag.

15. Op al onze leveringen en diensten zijn de 'Algemene Voorwaarden van de NBBU' van toepassing, zie www.nbbu.nl. Hierbij verklaart Inlener deze voorwaarden te hebben ontvangen, ingezien en begrepen. Tevens zijn de voorwaarden akkoord bevonden.

Bij akkoord vragen wij u het gehele document getekend en per e-mail te retourneren.

Voor akkoord op datum: ____-____-_____

Handtekening Inlener _____

KvK-nummer:

Mevrouw / heer: _____

Functie: _____

Kenmerk: ……

OVEREENKOMST VAN OPDRACHT VOOR VACCINATIEWERKZAAMHEDEN

Partijen:

1. De Regio Gooi en Vechtstreek, organisatieonderdeel GGD Gooi en Vechtstreek, ten deze rechtsgeldig vertegenwoordigd door .....el, manager GGD/Directeur Publieke Gezondheid, hierna te noemen: Opdrachtgever
   De GGD is ingeschreven bij de Kamer van Koophandel onder het nummer 32170415 op het adres Burgemeester de Bordesstraat 80 in Bussum, hierna te noemen de opdrachtgever;

2. ……, huisarts, ingeschreven bij de Kamer van Koophandel (KvK-nummer ……..) op het adres ……., ……., hierna te noemen de opdrachtnemer;

Hierna gezamenlijk te noemen partijen

In aanmerking nemende:

- Dat de opdrachtgever de instelling is die krachtens wet bevoegd is tot het vaccineren tegen het coronavirus (COVID-19);
- Dat de opdrachtnemer als zelfstandig opdrachtnemer werkzaam is op het gebied van de huisartsenzorg en voor eigen rekening en risico de werkzaamheden uitoefent;
- Dat opdrachtnemer als arts met als specialisatie huisarts staat ingeschreven in het BIG-register;
- Dat de opdrachtgever gebruikt wenst te maken van de diensten van de opdrachtnemer vanwege het vaccinatieprogramma COVID-19 en daarbij ontstane tijdsdruk om te vaccineren. Op dit moment zijn er te weinig artsen werkzaam bij de GGD om het vaccinatieprogramma volledig te kunnen uitvoeren;
- Dat de opdrachtgever, door het verlenen aan opdrachtnemer van deze overeenkomst van opdracht, opdrachtnemer deel wil laten nemen aan het vaccinatieprogramma, zodat de vaccinaties kunnen worden gegeven onder toezicht van een aanwezige arts;
- Dat opdrachtnemer bereid en in staat is deze diensten – van medisch toezicht op de vaccinaties - te verlenen;
- Dat partijen met deze overeenkomst de voorwaarden willen aangeven, waaronder zij met elkaar wensen te contracteren;
- Dat partijen uitdrukkelijk niet beogen om een arbeidsovereenkomst aan te gaan in de zin van artikel 7:610 e.v. B.W. en uitsluitend met elkaar wensen te contracteren op basis van een overeenkomst van opdracht in de zin van artikel 7:400 B.W.
- Dat partijen ervoor kiezen om in voorkomende gevallen de fictieve dienstbetrekking van thuiswerkers of gelijkgestelden zoals bedoeld in de artikelen 2b en 2c Uitvoeringsbesluit Loonbelasting 1965 en de artikelen 1 en 5 van het Besluit aanwijzing gevallen waarin arbeidsverhouding als dienstbetrekking wordt beschouwd (Besluit van 24 december 1986, Stb. 1986, 655), buiten toepassing te laten en daartoe deze overeenkomst opstellen en ondertekenen voordat uitbetaling plaatsvindt;
- Dat partijen met het oog op een juiste interpretatie van onderstaande contractsbepalingen, de door partijen beoogde uitvoering van de overeenkomst van opdracht en de kwalificatie van hun rechtsverhouding in het algemeen het navolgende opmerken:
- Dat de opdrachtnemer als huisarts een eigen professionele verantwoordelijkheid heeft en verantwoordelijk is voor en aanspreekbaar zal zijn op zijn of haar professionele handelen;

- Dat het de opdrachtnemer (natuurlijk) uitdrukkelijk vrijstaat om ook voor andere derden werkzaam te zijn. Hij / zij verricht de dienst immers tijdelijk en voor een beperkt aantal uren;
- Dat de opdrachtnemer voor de bij opdrachtgever naar de mening van partijen niet verplicht verzekerd is voor de werknemersverzekeringen, alsmede geen loonbelasting en sociale premies door de opdrachtgever behoeven te worden afgedragen;
- Dat de opdrachtnemer zich er van bewust is, dat hij vanwege het ontbreken van een fictieve- of echte dienstbetrekking, geen (sociale verzekerings)uitkering kan claimen.
- Dat deze overeenkomst is gebaseerd op de door de Belastingdienst op 14 oktober 2015 onder nummer 9051585731-B1, versie 08-11-2016, beoordeelde overeenkomst.

zijn overeengekomen als volgt:

Artikel 1. Onderwerp van de overeenkomst

1.1 Met inachtneming van de zorgplicht als omschreven in artikel 7:401 B.W. verleent de opdrachtnemer de diensten zelfstandig en is opdrachtnemer vrij te bepalen op welke wijze de diensten worden verleend. Het staat opdrachtgever vrij ter zake van de diensten aanwijzingen te geven als bedoeld in artikel 7:402 BW, hetgeen betekent dat aanwijzingen en instructies mogen worden gegeven ter zake van het resultaat van de opdracht, maar geen aanwijzingen of instructies kunnen worden gegeven aangaande de wijze waarop de opdracht feitelijk moet worden verricht.

1.2 Opdrachtnemer houdt zich in de overeengekomen periode bezig met het toezien op het vaccineren ten behoeve van het vaccinatieprogramma COVID – 19 voor mensen die zich bij de GGD laten vaccineren. Opdrachtnemer gaat op eigen initiatief medische diensten en handelingen verrichten. Opdrachtnemer zal naar eigen inzicht medische adviezen verstrekken. Opdrachtnemer bepaalt zelf de werktijden, binnen de door de opdrachtgever gestelde kaders/rooster. Opdrachtnemer beoordeelt daarbij voor het vaccineren eventuele contra-indicaties. Tijdens en na de vaccinatie, kan de opdrachtnemer opgeroepen worden bij post-vaccinale verschijnselen. Waar het nodig is verleent de opdrachtnemer eerste hulp en coördineert overige hulpverlening. Andere taken zijn o.a. (zie ook taakkaart voor meer informatie, in bezit van Opdrachtnemer):
   - Meewerken bij het inrichten van vaccinatielocatie en medewerking bij de dagelijkse controle of deze volgens richtlijnen werkt;
   - Uitleg geven aan medewerkers in de priklijn en borgen van hun bekwaamheid;
   - Toezichthouden op de medische kwaliteit van handelen van de medewerkers;
   - Adviseren van de burgers over vaccinatie indien één of meer van de triagevragen met ‘ja’ worden beantwoord;
   - Monitoren van de bijwerkingen en registreren van de bijwerkingen op de GGD-locatie;
   - Adviseren van de burgers over vervolgstap wanneer vaccin incorrect is toegediend;
   - Toepassen eerste hulp indien nodig.

1.3 Aangezien partijen uitsluitend met elkaar willen contracteren op basis van een overeenkomst van opdracht als bedoeld in artikel 7:400 B.W., verbinden partijen zich ertoe om hun feitelijke gedragingen bij de uitvoering van de diensten in overeenstemming te doen zijn met de inhoud en strekking van de overeenkomst teneinde de uitvoering van de wederzijdse contractuele verplichtingen binnen het wettelijk kader van een overeenkomst van opdracht te kunnen uitvoeren.

1.4 Opdrachtgever kan aanwijzingen en instructies geven omtrent het beoogde doel van de Opdracht, voor zover dit niet de wijze van uitvoeren van de Opdracht raakt.

Artikel 2. Uitvoering van de werkzaamheden

Opdrachtgever neemt gedurende de periode zoals bepaald in artikel 9 van deze overeenkomst diensten op flexibele basis van Opdrachtnemer af. Een dienst bedraagt maximaal 8 uur per dag (exclusief pauze) waarbij opdrachtnemer op basis van het rooster/planning wordt ingedeeld.

Artikel 3. Verplichtingen en Faciliteiten van de opdrachtgever

3.1 De opdrachtgever zal de opdrachtnemer in staat stellen de overeengekomen diensten te verlenen, door al hetgeen in dat kader redelijkerwijs van de opdrachtgever kan worden verlangd, te doen.

3.2 De opdrachtgever stelt ten behoeve van de uitoefening van de werkzaamheden door de opdrachtnemer voldoende personele ondersteuning ter beschikking.

3.3 De opdrachtgever zal zijn vaccinatieadministratie ter beschikking stellen aan de opdrachtnemer, die hiervan enkel op de vaccinatie-locatie naar eigen inzicht bij de uitvoering van deze overeenkomst gebruik kan maken. De opdrachtnemer zal ervoor zorg dragen, dat deze administratie op verantwoorde wijze, zonder nadelige gevolgen voor de patiënten en voor de opdrachtgever, plaatsvindt.

3.4 De opdrachtgever stelt voor zijn rekening aan opdrachtnemer de werklocatie en de overige voorzieningen ter beschikking. Opdrachtgever zal zorgdragen voor alle materialen die opdrachtnemer nodig heeft om de opdracht goed te kunnen vervullen, zoals instrumentarium, PBM en overige ge- en verbruiksmaterialen. De opdrachtgever verplicht zich ertoe zich te onthouden van het geven van verplichtende voorschriften met betrekking tot de wijze van gebruik van de werklocatie.

3.5 Alle goederen, daaronder begrepen schriftelijke stukken (originelen, afschriften en fotokopieën), welke de opdrachtnemer ten behoeve van de opdrachtgever gedurende het bestaan van deze overeenkomst onder zich krijgt, zijn en blijven eigendom van de opdrachtgever. De originelen van de schriftelijke stukken dienen te allen tijde op de werklocatie van de opdrachtgever te blijven en bewaart deze gegevens gedurende de wettelijke bewaartermijn.

3.6 Bij de beëindiging van deze overeenkomst is de opdrachtnemer gehouden alle goederen van of ten behoeve van de opdrachtgever, die hij op het moment van beëindiging onder zich heeft (waaronder de in lid 5 bedoelde schriftelijke stukken), onverwijld ter beschikking te stellen aan de opdrachtgever.

Artikel 4. Verplichtingen van de opdrachtnemer

4.1 De opdrachtnemer is uit hoofde van het zijn van geregistreerd huisarts bevoegd en bekwaam om de diensten te verlenen.

4.2 De opdrachtnemer verklaart dat hij/zij tijdens de duur van deze overeenkomst blijft voldoen aan de beroepseisen zoals die voor de herregistratie zijn gesteld. Voorts verklaart de opdrachtnemer door ondertekening van de overeenkomst dat hij voldoet aan de eisen en kwaliteitsnormen die aan solistisch werkende zorgverleners gesteld worden in de Wet Kwaliteit, Klachten en Geschillen Zorg (Wkkgz).

4.3 Ter zake de te verlenen zorg die valt onder de Wkkgz komen partijen overeen dat opdrachtnemer zich aansluit bij de volgende door opdrachtgever getroffen regelingen:

a. de verplichting tot bewaking en beheersing van de kwaliteit van zorg als genoemd in artikel 7 van de Wkkgz;
b. de meldcode huiselijk geweld en kindermishandeling als genoemd in artikel 8 van de Wkkgz;
c. de procedure ‘Veilig Incident Melden’ als genoemd in artikel 9 Wkkgz;
d. de klachtenregeling als genoemd in artikel 13 van de Wkkgz;
e. de klachtenfunctionaris als genoemd in artikel 15 van de Wkkgz.

4.4 Binnen het kader van de gemaakte afspraken ten aanzien van aard en omvang van de opdracht bepaalt de opdrachtnemer zelf, hoe hij zijn werkzaamheden zal verrichten.

4.5 De opdrachtnemer zal de opdrachtgever er onmiddellijk van in kennis stellen indien en zodra de BIG-registratie als arts met als specialisme huisarts vervalt.

4.6 Opdrachtnemer en opdrachtgever komen overeen dat klachten van personen die gevaccineerd worden jegens opdrachtnemer worden afgewikkeld op grond van de klachtenregeling en met gebruik van de klachtenfunctionaris van opdrachtgever. Ter zake de geschillenbeslechting komen partijen overeen dat personen die gevaccineerd worden zich ter zake handelen of nalaten van opdrachtnemer kunnen wenden tot de geschilleninstantie waarbij opdrachtnemer zelfstandig is aangesloten. Het in de vorige zin gestelde geldt enkel indien het een geschil betreft ter zake de door opdrachtnemer verleende zorg waarop de Wkkgz van toepassing is. Indien de geschilleninstantie waarbij de huisarts is aangesloten het geschil op formele gronden niet inhoudelijk in behandeling neemt, zal het geschil worden voorgelegd aan de geschilleninstantie van opdrachtgever.

4.7 De opdrachtnemer verklaart ingeschreven te staan in het handelsregister van de Kamer van Koophandel.

4.8 Indien de opdrachtnemer verhinderd is om de overeenkomst van opdracht zelf uit te voeren, zal de opdrachtnemer zijn vervanging regelen met de opdrachtnemers waar opdrachtgever een dienstverleningsovereenkomst mee is aangegaan.

Artikel 5. Geheimhouding

5.1 De opdrachtnemer zal de wettelijke bepalingen met betrekking tot bescherming van de persoonlijke levenssfeer en privacy van de personen die gevaccineerd worden in achtnemen. De opdrachtgever is eigenaar en beheerder van alle vaccinatiedossiers in de informatiesystemen van de opdrachtgever. Het is de opdrachtnemer niet toegestaan de dossiers in te zien van andere dan aan zijn zorg toevertrouwde te vaccineren personen.

5.2 De Opdrachtnemer zal geheimhouding betrachten van alle (persoons)gegevens en informatie die hem/haar in het kader van de opdracht ter kennis komen. Dit betreft eveneens informatie over en van de organisatie en informatie ten aanzien van de door GGD GHOR Nederland en de GGD'en in gebruik zijnde systemen .en van en over GGD GHOR Nederland, de GGD'en waar de opdracht wordt uitgevoerd, haar medewerkers, betrokkenen en derden.

5.3 De informatie en gegevens zullen niet anders worden gebruikt dan voor de taak waarvoor deze door GGD GHOR Nederland en de desbetreffende GGD'en aan beschikbaar worden gesteld en niet langer dan de opdracht duurt.

5.4 Zonder uitdrukkelijke toestemming van opdrachtgever is het niet toegestaan om kopieën, en/of foto's te maken en/of op andere wijze gebruik maken van mogelijkheden om informatie te dupliceren.

5.5 De geheimhoudingsverplichting geldt zowel tijdens als na de afloop van de overeenkomst.

Artikel 6. Honorering en declaratie

6.1 De opdrachtgever betaalt aan de opdrachtnemer uitsluitend voor de gewerkte uren een vergoeding ter grootte van maximaal:

- € ..... per uur (exclusief BTW) voor diensten door-de-weeks tussen 08.00 en 20.00 uur (max. 8 uur
  per dienst);
- € ..... per uur (exclusief BTW) voor diensten op zaterdag, zondag en feestdagen (max. 8 uur per dienst).

6.2 De opdrachtgever gaat ervan uit dat de werkzaamheden van opdrachtnemer binnen de BTW-vrijstelling vallen. Indien in individuele gevallen dit toch mocht leiden tot een BTW-heffing dan zal het ministerie van VWS deze kosten vergoeden.

6.3 De onkosten van de Opdrachtnemer zijn in de vergoeding van de Opdrachtnemer inbegrepen. Onder onkosten vallen ook de reis-, parkeer-, en verblijfkosten, administratie - en telefoonkosten en alle andere overige onkosten van de Opdrachtnemer.

6.4 Het uurtarief is vast en onveranderlijk gedurende de duur van deze Overeenkomst.

6.5 De opdrachtnemer zal maandelijks met de daarbij behorende urenspecificatie een door hem/haar vervaardigde factuur aan opdrachtgever doen toekomen voor de verleende diensten.

6.6 De factuur zal voldoen aan de wettelijke vereisten.
Facturen dienen digitaal te worden verzonden naar het mailadres: facturen@regiogv.nl
De factuur dient gerichte te zijn aan 'Regio Gooi en Vechtstreek, ter attentie van de RVE GGD, Burgemeester de Bordesstraat 80, 1440 GZ Bussum.

6.7 Voor betaling van facturen dient als betalingskenmerk altijd het nummer 21.0003764 op de factuur te worden vermeld.
Voor een adequate en snelle afhandeling van facturen moet op de factuur tevens worden vermeld:
- kostenplaats : 533100
- kostendrager : 501032
- grootbroekrek. : 41311

6.8 Indien de opdrachtgever voor haar facturatie nadere gegevens nodig heeft, verplicht de opdrachtnemer zich jegens de opdrachtgever om binnen 14 dagen na een verzoek daartoe de verzochte gegevens te verstrekken.

6.9 De opdrachtgever zal het door de opdrachtnemer gefactureerde bedrag binnen 30 dagen voldoen.

6.10 Indien de opdrachtnemer door ziekte, arbeidsongeschiktheid of om andere redenen afwezig is en de overeengekomen werkzaamheden niet kan leveren, dan is de opdrachtgever geen vergoedingen verschuldigd aan de opdrachtnemer.

Artikel 7. Contactpersonen

Contactpersonen voor de uitvoering van deze overeenkomst zijn:
- voor de Opdrachtgever: …….
- voor de Contractant: ……..

Contactpersonen kunnen Partijen alleen vertegenwoordigen en binden voor zover het betreft de uitvoering van deze Overeenkomst. Tot wijziging van deze Overeenkomst zijn zij niet bevoegd.

Artikel 8. Aansprakelijkheid

8.1 De opdrachtnemer staat in voor de door hem/haar verleende diensten. Opdrachtnemer is jegens de gevaccineerde persoon en/of opdrachtgever aansprakelijk voor schade die de gevaccineerde persoon lijdt als gevolg van gedragingen of nalaten van opdrachtnemer. Opdrachtnemer is daarbij niet aansprakelijk voor handelen en/of nalaten van werknemers en/of hulppersonen van opdrachtgever. Opdrachtgever vrijwaart opdrachtnemer tegen aanspraken van gevaccineerde personen en anderen ter zake handelen en/of nalaten van werknemers en/of hulppersonen van opdrachtgever die onder het toezicht van de opdrachtnemer vallen.

8.2 De opdrachtnemer draagt zorg voor een passende beroeps- en bedrijfsaansprakelijkheidsverzekering (met een binnen het werkveld gangbare dekking). Indien die geen dekking zou bieden, zal de beroeps- en bedrijfsaansprakelijkheidsverzekering van de opdrachtgever (GGD) dekking bieden en voor zover dat ook niet het geval zou zijn staat het Ministerie van VWS in voor de voldoening van eventuele schade.

Artikel 9. Duur en beëindiging

9.1 De overeenkomst wordt aangegaan voor bepaalde tijd vanaf 10 mei 2021 en eindigt op 31 december 2021van rechtswege zonder dat hiervoor opzegging vereist is.

9.2 De overeenkomst kan door ieder der partijen tussentijds schriftelijk worden opgezegd met inachtneming van een opzegtermijn van een week.

Artikel 10. Overige bepalingen

10.1 Wijzigingen van en/of aanvullingen op de overeenkomst kunnen uitsluitend schriftelijk door partijen worden overeengekomen.

10.2 Indien enige bepaling van de overeenkomst nietig is dan wel vernietigd wordt, zullen de overige bepalingen van kracht blijven en zullen partijen in overleg treden teneinde nieuwe bepalingen ter vervanging van de nietige c.q. vernietigde bepalingen overeen te komen, waarbij zoveel mogelijk het doel en de strekking van de nietige c.q. vernietigde bepalingen in acht worden genomen.

Artikel 11. Geschil en rechtskeuze

11.1 Op de overeenkomst is Nederlands recht van toepassing.

11.2 Alle geschillen, welke tussen ondergetekenden mochten opkomen, zowel juridische als feitelijke, met betrekking tot de uitleg of de uitvoering van deze overeenkomst, zullen de partijen in eerste instantie gezamenlijk trachten op te lossen met behulp van mediation. De partij, die mediation verlangt zal daarvan schriftelijk mededeling doen aan de andere partij. De mededeling dient tevens een aanduiding te bevatten van het onderwerp waarover mediation verlangd wordt.

11.3 Wanneer binnen een termijn van 14 dagen geen overeenkomst is bereikt omtrent het voorleggen van het geschil aan een mediator, dan wel indien het niet mogelijk is gebleken het geschil middels mediation op te lossen, staat het partijen vrij het geschil voor te leggen aan de competente Rechtbank.

Aldus overeengekomen en in tweevoud ondertekend op ……. 2021.

Te Bussum

Opdrachtgever: Opdrachtnemer:

..... ……

Kenmerk: ……

OVEREENKOMST VAN OPDRACHT VOOR VACCINATIEWERKZAAMHEDEN

Partijen:

1. De Regio Gooi en Vechtstreek, organisatieonderdeel GGD Gooi en Vechtstreek, ten deze rechtsgeldig vertegenwoordigd door .....el, manager GGD/Directeur Publieke Gezondheid, hierna te noemen: Opdrachtgever
   De GGD is ingeschreven bij de Kamer van Koophandel onder het nummer 32170415 op het adres Burgemeester de Bordesstraat 80 in Bussum, hierna te noemen de opdrachtgever;

2. ……, huisarts, ingeschreven bij de Kamer van Koophandel (KvK-nummer ……..) op het adres ……., ……., hierna te noemen de opdrachtnemer;

Hierna gezamenlijk te noemen partijen

In aanmerking nemende:

- Dat de opdrachtgever de instelling is die krachtens wet bevoegd is tot het vaccineren tegen het coronavirus (COVID-19);
- Dat de opdrachtnemer als zelfstandig opdrachtnemer werkzaam is op het gebied van de huisartsenzorg en voor eigen rekening en risico de werkzaamheden uitoefent;
- Dat opdrachtnemer als arts met als specialisatie huisarts staat ingeschreven in het BIG-register;
- Dat de opdrachtgever gebruikt wenst te maken van de diensten van de opdrachtnemer vanwege het vaccinatieprogramma COVID-19 en daarbij ontstane tijdsdruk om te vaccineren. Op dit moment zijn er te weinig artsen werkzaam bij de GGD om het vaccinatieprogramma volledig te kunnen uitvoeren;
- Dat de opdrachtgever, door het verlenen aan opdrachtnemer van deze overeenkomst van opdracht, opdrachtnemer deel wil laten nemen aan het vaccinatieprogramma, zodat de vaccinaties kunnen worden gegeven onder toezicht van een aanwezige arts;
- Dat opdrachtnemer bereid en in staat is deze diensten – van medisch toezicht op de vaccinaties - te verlenen;
- Dat partijen met deze overeenkomst de voorwaarden willen aangeven, waaronder zij met elkaar wensen te contracteren;
- Dat partijen uitdrukkelijk niet beogen om een arbeidsovereenkomst aan te gaan in de zin van artikel 7:610 e.v. B.W. en uitsluitend met elkaar wensen te contracteren op basis van een overeenkomst van opdracht in de zin van artikel 7:400 B.W.
- Dat partijen ervoor kiezen om in voorkomende gevallen de fictieve dienstbetrekking van thuiswerkers of gelijkgestelden zoals bedoeld in de artikelen 2b en 2c Uitvoeringsbesluit Loonbelasting 1965 en de artikelen 1 en 5 van het Besluit aanwijzing gevallen waarin arbeidsverhouding als dienstbetrekking wordt beschouwd (Besluit van 24 december 1986, Stb. 1986, 655), buiten toepassing te laten en daartoe deze overeenkomst opstellen en ondertekenen voordat uitbetaling plaatsvindt;
- Dat partijen met het oog op een juiste interpretatie van onderstaande contractsbepalingen, de door partijen beoogde uitvoering van de overeenkomst van opdracht en de kwalificatie van hun rechtsverhouding in het algemeen het navolgende opmerken:
- Dat de opdrachtnemer als huisarts een eigen professionele verantwoordelijkheid heeft en verantwoordelijk is voor en aanspreekbaar zal zijn op zijn of haar professionele handelen;

- Dat het de opdrachtnemer (natuurlijk) uitdrukkelijk vrijstaat om ook voor andere derden werkzaam te zijn. Hij / zij verricht de dienst immers tijdelijk en voor een beperkt aantal uren;
- Dat de opdrachtnemer voor de bij opdrachtgever naar de mening van partijen niet verplicht verzekerd is voor de werknemersverzekeringen, alsmede geen loonbelasting en sociale premies door de opdrachtgever behoeven te worden afgedragen;
- Dat de opdrachtnemer zich er van bewust is, dat hij vanwege het ontbreken van een fictieve- of echte dienstbetrekking, geen (sociale verzekerings)uitkering kan claimen.
- Dat deze overeenkomst is gebaseerd op de door de Belastingdienst op 14 oktober 2015 onder nummer 9051585731-B1, versie 08-11-2016, beoordeelde overeenkomst.

zijn overeengekomen als volgt:

Artikel 1. Onderwerp van de overeenkomst

1.1 Met inachtneming van de zorgplicht als omschreven in artikel 7:401 B.W. verleent de opdrachtnemer de diensten zelfstandig en is opdrachtnemer vrij te bepalen op welke wijze de diensten worden verleend. Het staat opdrachtgever vrij ter zake van de diensten aanwijzingen te geven als bedoeld in artikel 7:402 BW, hetgeen betekent dat aanwijzingen en instructies mogen worden gegeven ter zake van het resultaat van de opdracht, maar geen aanwijzingen of instructies kunnen worden gegeven aangaande de wijze waarop de opdracht feitelijk moet worden verricht.

1.2 Opdrachtnemer houdt zich in de overeengekomen periode bezig met het toezien op het vaccineren ten behoeve van het vaccinatieprogramma COVID – 19 voor mensen die zich bij de GGD laten vaccineren. Opdrachtnemer gaat op eigen initiatief medische diensten en handelingen verrichten. Opdrachtnemer zal naar eigen inzicht medische adviezen verstrekken. Opdrachtnemer bepaalt zelf de werktijden, binnen de door de opdrachtgever gestelde kaders/rooster. Opdrachtnemer beoordeelt daarbij voor het vaccineren eventuele contra-indicaties. Tijdens en na de vaccinatie, kan de opdrachtnemer opgeroepen worden bij post-vaccinale verschijnselen. Waar het nodig is verleent de opdrachtnemer eerste hulp en coördineert overige hulpverlening. Andere taken zijn o.a. (zie ook taakkaart voor meer informatie, in bezit van Opdrachtnemer):
   - Meewerken bij het inrichten van vaccinatielocatie en medewerking bij de dagelijkse controle of deze volgens richtlijnen werkt;
   - Uitleg geven aan medewerkers in de priklijn en borgen van hun bekwaamheid;
   - Toezichthouden op de medische kwaliteit van handelen van de medewerkers;
   - Adviseren van de burgers over vaccinatie indien één of meer van de triagevragen met ‘ja’ worden beantwoord;
   - Monitoren van de bijwerkingen en registreren van de bijwerkingen op de GGD-locatie;
   - Adviseren van de burgers over vervolgstap wanneer vaccin incorrect is toegediend;
   - Toepassen eerste hulp indien nodig.

1.3 Aangezien partijen uitsluitend met elkaar willen contracteren op basis van een overeenkomst van opdracht als bedoeld in artikel 7:400 B.W., verbinden partijen zich ertoe om hun feitelijke gedragingen bij de uitvoering van de diensten in overeenstemming te doen zijn met de inhoud en strekking van de overeenkomst teneinde de uitvoering van de wederzijdse contractuele verplichtingen binnen het wettelijk kader van een overeenkomst van opdracht te kunnen uitvoeren.

1.4 Opdrachtgever kan aanwijzingen en instructies geven omtrent het beoogde doel van de Opdracht, voor zover dit niet de wijze van uitvoeren van de Opdracht raakt.

Artikel 2. Uitvoering van de werkzaamheden

Opdrachtgever neemt gedurende de periode zoals bepaald in artikel 9 van deze overeenkomst diensten op flexibele basis van Opdrachtnemer af. Een dienst bedraagt maximaal 8 uur per dag (exclusief pauze) waarbij opdrachtnemer op basis van het rooster/planning wordt ingedeeld.

Artikel 3. Verplichtingen en Faciliteiten van de opdrachtgever

3.1 De opdrachtgever zal de opdrachtnemer in staat stellen de overeengekomen diensten te verlenen, door al hetgeen in dat kader redelijkerwijs van de opdrachtgever kan worden verlangd, te doen.

3.2 De opdrachtgever stelt ten behoeve van de uitoefening van de werkzaamheden door de opdrachtnemer voldoende personele ondersteuning ter beschikking.

3.3 De opdrachtgever zal zijn vaccinatieadministratie ter beschikking stellen aan de opdrachtnemer, die hiervan enkel op de vaccinatie-locatie naar eigen inzicht bij de uitvoering van deze overeenkomst gebruik kan maken. De opdrachtnemer zal ervoor zorg dragen, dat deze administratie op verantwoorde wijze, zonder nadelige gevolgen voor de patiënten en voor de opdrachtgever, plaatsvindt.

3.4 De opdrachtgever stelt voor zijn rekening aan opdrachtnemer de werklocatie en de overige voorzieningen ter beschikking. Opdrachtgever zal zorgdragen voor alle materialen die opdrachtnemer nodig heeft om de opdracht goed te kunnen vervullen, zoals instrumentarium, PBM en overige ge- en verbruiksmaterialen. De opdrachtgever verplicht zich ertoe zich te onthouden van het geven van verplichtende voorschriften met betrekking tot de wijze van gebruik van de werklocatie.

3.5 Alle goederen, daaronder begrepen schriftelijke stukken (originelen, afschriften en fotokopieën), welke de opdrachtnemer ten behoeve van de opdrachtgever gedurende het bestaan van deze overeenkomst onder zich krijgt, zijn en blijven eigendom van de opdrachtgever. De originelen van de schriftelijke stukken dienen te allen tijde op de werklocatie van de opdrachtgever te blijven en bewaart deze gegevens gedurende de wettelijke bewaartermijn.

3.6 Bij de beëindiging van deze overeenkomst is de opdrachtnemer gehouden alle goederen van of ten behoeve van de opdrachtgever, die hij op het moment van beëindiging onder zich heeft (waaronder de in lid 5 bedoelde schriftelijke stukken), onverwijld ter beschikking te stellen aan de opdrachtgever.

Artikel 4. Verplichtingen van de opdrachtnemer

4.1 De opdrachtnemer is uit hoofde van het zijn van geregistreerd huisarts bevoegd en bekwaam om de diensten te verlenen.

4.2 De opdrachtnemer verklaart dat hij/zij tijdens de duur van deze overeenkomst blijft voldoen aan de beroepseisen zoals die voor de herregistratie zijn gesteld. Voorts verklaart de opdrachtnemer door ondertekening van de overeenkomst dat hij voldoet aan de eisen en kwaliteitsnormen die aan solistisch werkende zorgverleners gesteld worden in de Wet Kwaliteit, Klachten en Geschillen Zorg (Wkkgz).

4.3 Ter zake de te verlenen zorg die valt onder de Wkkgz komen partijen overeen dat opdrachtnemer zich aansluit bij de volgende door opdrachtgever getroffen regelingen:

a. de verplichting tot bewaking en beheersing van de kwaliteit van zorg als genoemd in artikel 7 van de Wkkgz;
b. de meldcode huiselijk geweld en kindermishandeling als genoemd in artikel 8 van de Wkkgz;
c. de procedure ‘Veilig Incident Melden’ als genoemd in artikel 9 Wkkgz;
d. de klachtenregeling als genoemd in artikel 13 van de Wkkgz;
e. de klachtenfunctionaris als genoemd in artikel 15 van de Wkkgz.

4.4 Binnen het kader van de gemaakte afspraken ten aanzien van aard en omvang van de opdracht bepaalt de opdrachtnemer zelf, hoe hij zijn werkzaamheden zal verrichten.

4.5 De opdrachtnemer zal de opdrachtgever er onmiddellijk van in kennis stellen indien en zodra de BIG-registratie als arts met als specialisme huisarts vervalt.

4.6 Opdrachtnemer en opdrachtgever komen overeen dat klachten van personen die gevaccineerd worden jegens opdrachtnemer worden afgewikkeld op grond van de klachtenregeling en met gebruik van de klachtenfunctionaris van opdrachtgever. Ter zake de geschillenbeslechting komen partijen overeen dat personen die gevaccineerd worden zich ter zake handelen of nalaten van opdrachtnemer kunnen wenden tot de geschilleninstantie waarbij opdrachtnemer zelfstandig is aangesloten. Het in de vorige zin gestelde geldt enkel indien het een geschil betreft ter zake de door opdrachtnemer verleende zorg waarop de Wkkgz van toepassing is. Indien de geschilleninstantie waarbij de huisarts is aangesloten het geschil op formele gronden niet inhoudelijk in behandeling neemt, zal het geschil worden voorgelegd aan de geschilleninstantie van opdrachtgever.

4.7 De opdrachtnemer verklaart ingeschreven te staan in het handelsregister van de Kamer van Koophandel.

4.8 Indien de opdrachtnemer verhinderd is om de overeenkomst van opdracht zelf uit te voeren, zal de opdrachtnemer zijn vervanging regelen met de opdrachtnemers waar opdrachtgever een dienstverleningsovereenkomst mee is aangegaan.

Artikel 5. Geheimhouding

5.1 De opdrachtnemer zal de wettelijke bepalingen met betrekking tot bescherming van de persoonlijke levenssfeer en privacy van de personen die gevaccineerd worden in achtnemen. De opdrachtgever is eigenaar en beheerder van alle vaccinatiedossiers in de informatiesystemen van de opdrachtgever. Het is de opdrachtnemer niet toegestaan de dossiers in te zien van andere dan aan zijn zorg toevertrouwde te vaccineren personen.

5.2 De Opdrachtnemer zal geheimhouding betrachten van alle (persoons)gegevens en informatie die hem/haar in het kader van de opdracht ter kennis komen. Dit betreft eveneens informatie over en van de organisatie en informatie ten aanzien van de door GGD GHOR Nederland en de GGD'en in gebruik zijnde systemen .en van en over GGD GHOR Nederland, de GGD'en waar de opdracht wordt uitgevoerd, haar medewerkers, betrokkenen en derden.

5.3 De informatie en gegevens zullen niet anders worden gebruikt dan voor de taak waarvoor deze door GGD GHOR Nederland en de desbetreffende GGD'en aan beschikbaar worden gesteld en niet langer dan de opdracht duurt.

5.4 Zonder uitdrukkelijke toestemming van opdrachtgever is het niet toegestaan om kopieën, en/of foto's te maken en/of op andere wijze gebruik maken van mogelijkheden om informatie te dupliceren.

5.5 De geheimhoudingsverplichting geldt zowel tijdens als na de afloop van de overeenkomst.

Artikel 6. Honorering en declaratie

6.1 De opdrachtgever betaalt aan de opdrachtnemer uitsluitend voor de gewerkte uren een vergoeding ter grootte van maximaal:

- € ..... per uur (exclusief BTW) voor diensten door-de-weeks tussen 08.00 en 20.00 uur (max. 8 uur
  per dienst);
- € ..... per uur (exclusief BTW) voor diensten op zaterdag, zondag en feestdagen (max. 8 uur per dienst).

6.2 De opdrachtgever gaat ervan uit dat de werkzaamheden van opdrachtnemer binnen de BTW-vrijstelling vallen. Indien in individuele gevallen dit toch mocht leiden tot een BTW-heffing dan zal het ministerie van VWS deze kosten vergoeden.

6.3 De onkosten van de Opdrachtnemer zijn in de vergoeding van de Opdrachtnemer inbegrepen. Onder onkosten vallen ook de reis-, parkeer-, en verblijfkosten, administratie - en telefoonkosten en alle andere overige onkosten van de Opdrachtnemer.

6.4 Het uurtarief is vast en onveranderlijk gedurende de duur van deze Overeenkomst.

6.5 De opdrachtnemer zal maandelijks met de daarbij behorende urenspecificatie een door hem/haar vervaardigde factuur aan opdrachtgever doen toekomen voor de verleende diensten.

6.6 De factuur zal voldoen aan de wettelijke vereisten.
Facturen dienen digitaal te worden verzonden naar het mailadres: facturen@regiogv.nl
De factuur dient gerichte te zijn aan 'Regio Gooi en Vechtstreek, ter attentie van de RVE GGD, Burgemeester de Bordesstraat 80, 1440 GZ Bussum.

6.7 Voor betaling van facturen dient als betalingskenmerk altijd het nummer 21.0003764 op de factuur te worden vermeld.
Voor een adequate en snelle afhandeling van facturen moet op de factuur tevens worden vermeld:
- kostenplaats : 533100
- kostendrager : 501032
- grootbroekrek. : 41311

6.8 Indien de opdrachtgever voor haar facturatie nadere gegevens nodig heeft, verplicht de opdrachtnemer zich jegens de opdrachtgever om binnen 14 dagen na een verzoek daartoe de verzochte gegevens te verstrekken.

6.9 De opdrachtgever zal het door de opdrachtnemer gefactureerde bedrag binnen 30 dagen voldoen.

6.10 Indien de opdrachtnemer door ziekte, arbeidsongeschiktheid of om andere redenen afwezig is en de overeengekomen werkzaamheden niet kan leveren, dan is de opdrachtgever geen vergoedingen verschuldigd aan de opdrachtnemer.

Artikel 7. Contactpersonen

Contactpersonen voor de uitvoering van deze overeenkomst zijn:
- voor de Opdrachtgever: …….
- voor de Contractant: ……..

Contactpersonen kunnen Partijen alleen vertegenwoordigen en binden voor zover het betreft de uitvoering van deze Overeenkomst. Tot wijziging van deze Overeenkomst zijn zij niet bevoegd.

Artikel 8. Aansprakelijkheid

8.1 De opdrachtnemer staat in voor de door hem/haar verleende diensten. Opdrachtnemer is jegens de gevaccineerde persoon en/of opdrachtgever aansprakelijk voor schade die de gevaccineerde persoon lijdt als gevolg van gedragingen of nalaten van opdrachtnemer. Opdrachtnemer is daarbij niet aansprakelijk voor handelen en/of nalaten van werknemers en/of hulppersonen van opdrachtgever. Opdrachtgever vrijwaart opdrachtnemer tegen aanspraken van gevaccineerde personen en anderen ter zake handelen en/of nalaten van werknemers en/of hulppersonen van opdrachtgever die onder het toezicht van de opdrachtnemer vallen.

8.2 De opdrachtnemer draagt zorg voor een passende beroeps- en bedrijfsaansprakelijkheidsverzekering (met een binnen het werkveld gangbare dekking). Indien die geen dekking zou bieden, zal de beroeps- en bedrijfsaansprakelijkheidsverzekering van de opdrachtgever (GGD) dekking bieden en voor zover dat ook niet het geval zou zijn staat het Ministerie van VWS in voor de voldoening van eventuele schade.

Artikel 9. Duur en beëindiging

9.1 De overeenkomst wordt aangegaan voor bepaalde tijd vanaf 10 mei 2021 en eindigt op 31 december 2021van rechtswege zonder dat hiervoor opzegging vereist is.

9.2 De overeenkomst kan door ieder der partijen tussentijds schriftelijk worden opgezegd met inachtneming van een opzegtermijn van een week.

Artikel 10. Overige bepalingen

10.1 Wijzigingen van en/of aanvullingen op de overeenkomst kunnen uitsluitend schriftelijk door partijen worden overeengekomen.

10.2 Indien enige bepaling van de overeenkomst nietig is dan wel vernietigd wordt, zullen de overige bepalingen van kracht blijven en zullen partijen in overleg treden teneinde nieuwe bepalingen ter vervanging van de nietige c.q. vernietigde bepalingen overeen te komen, waarbij zoveel mogelijk het doel en de strekking van de nietige c.q. vernietigde bepalingen in acht worden genomen.

Artikel 11. Geschil en rechtskeuze

11.1 Op de overeenkomst is Nederlands recht van toepassing.

11.2 Alle geschillen, welke tussen ondergetekenden mochten opkomen, zowel juridische als feitelijke, met betrekking tot de uitleg of de uitvoering van deze overeenkomst, zullen de partijen in eerste instantie gezamenlijk trachten op te lossen met behulp van mediation. De partij, die mediation verlangt zal daarvan schriftelijk mededeling doen aan de andere partij. De mededeling dient tevens een aanduiding te bevatten van het onderwerp waarover mediation verlangd wordt.

11.3 Wanneer binnen een termijn van 14 dagen geen overeenkomst is bereikt omtrent het voorleggen van het geschil aan een mediator, dan wel indien het niet mogelijk is gebleken het geschil middels mediation op te lossen, staat het partijen vrij het geschil voor te leggen aan de competente Rechtbank.

Aldus overeengekomen en in tweevoud ondertekend op ……. 2021.

Te Bussum

Opdrachtgever: Opdrachtnemer:

..... ……

Regio Gooi en Vechtstreek

MEMO

Handreiking beoordeling datalekken AVG

Algemeen	
Aan	CMT
Van	[redacted]
Datum	27 september 2019
Verspreiden	Nee
Kenmerk	19.0013574

1. Inleiding

Vaak begint een datalek als vermoeden van een datalek of een 'informatieveiligheidsincident'. Zo'n vermoeden of incident is daadwerkelijk een datalek indien sprake is van toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is.

De Europese toezichhouders hebben Richtsnoeren opgesteld die de verwerkingsverantwoordelijke ondersteunen bij de beoordeling of een mogelijk datalek daadwerkelijk een datalek is en of aan de AP (en betrokkene) moet worden gemeld. Deze Richtsnoeren dienen tevens als uitgangspunt voor de AP bij het toepassen van handhavende maatregelen.

Ten behoeve van het Team Privacyincidenten is een handzame en praktische handreiking gemaakt van de vragen die in het kader van de beoordeling van een mogelijk datalek nagelopen en beantwoord moeten worden. Deze handreiking is opgesteld aan de hand van de hiervoor genoemde Richtsnoeren en informatie van de Autoriteit Persoonsgegevens.

2. Definities en omschrijvingen

Er is sprake van een datalek als er bij een informatieveiligheidsincident toegang tót of vernietiging, wijziging of vrijkomen ván persoonsgegevens heeft plaatsgevonden zonder dat dit de bedoeling is. Een datalek moet ruim worden opgevat. Het gaat om voorvallen waarbij de bescherming van persoonsgegevens is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies, onrechtmatige inzage of onrechtmatige verwerking. Voorbeelden van datalekken zijn:

- kwijtraken van een brief met persoonsgegevens bij de post
- verzenden van persoonsgegevens naar een verkeerd e-mailadres
- versturen/beschikbaar stellen via een portal van te veel (onnodige) gegevens aan derden
- kwijtraken van een onbeveiligde USB-stick met persoonsgegevens
- diefstal van een laptop, iPad e.d. met persoonsgegevens
- een malware besmetting
- verzenden van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden (CC i.p.v. BCC)

Overige definities relevant in het kader van de beoordeling van datalekken zijn:

- betrokkene: degene op wie een persoonsgegeven betrekking heeft.
- inbreuk op de beveiliging/informatieveiligheidsincident: inbreuk op de passende technische en organisatorische maatregelen die moeten worden getroffen om een op het risico afgestemd beveiligingsniveau te waarborgen.
- datalek/privacyincident: een informatieveiligheidsincident waarbij persoonsgegevens vernietigd of verloren zijn gegaan, zijn gewijzigd, verstrekt of toegankelijk gemaakt.

- persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
- bijzondere persoonsgegevens: persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt en genetische gegevens, biometrische gegevens met het oog op unieke identificatie van een persoon, gegevens over gezondheid en gegegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.
- verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In dit geval de Regio.
- verwerker: degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
- verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen 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, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

3. Te beantwoorden vragen

De vier belangrijkste vragen om een datalek en de te nemen stappen te kunnen beoordelen zijn:

- of er sprake is geweest van een datalek,
- wat er dan precies is gebeurd,
- of een melding gedaan moet worden aan de AP en
- of betrokkene(n) geïnformeerd moeten worden

In het navolgende wordt voor deze vragen aan de hand van de Richtsnoeren en informatie van de Autoriteit Persoonsgegevens een handreiking gegeven.

Stap 1) Is er sprake van een datalek?

Een datalek is 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 (art. 4 AVG). Persoonsgegevens komen waar ze niet behoren te zijn. Ook als redelijkerwijs niet kan worden uitgesloten dat dit gebeurd is, is sprake van een datalek.

Inbreuk op de beveiliging?
Er moet sprake zijn geweest van een daadwerkelijke inbreuk op de beveiliging. Hiermee wordt gedoeld op inbreuk op de (in artikel 32 AVG vereiste) passende technische en organisatorische maatregelen die moeten worden getroffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Enkel een tekortkoming of zwakke plek in de beveiliging is nog geen inbreuk op de beveiliging. De eventueel getroffen beveiligingsmaatregelen moet onvoldoende zijn gebleken. Voorbeelden zijn de zoek geraakte USB-stick, gestolen laptop, een mail die naar een verkeerd mailadres wordt gestuurd of een calamiteit zoals brand in een datacentrum. Binnen de Regio spreken we in plaats van over een inbreuk op de beveiliging, over een informatieveiligheidsincident.

Als vast staat dat sprake is van een informatieveiligheidsincident moet gekeken worden of er (als gevolg van het incident) iets met de persoonsgegevens is gebeurd dat niet de bedoeling is.
Dat betekent dat er door het incident per ongeluk of op onrechtmatige wijze persoonsgegevens vernietigd of verloren zijn gegaan, zijn gewijzigd, verstrekt of toegankelijk gemaakt. Bij de Regio is het per ongeluk verstrekken of toegankelijk maken van persoonsgegevens het meest voorkomende scenario. De repressieve maatregelen en de herstelmaatregelen die getroffen zijn, zijn niet voldoende geweest om de gevolgen geheel weg te nemen.

Stap 2) Wat is er precies gebeurd?

Onderstaande vragen helpen om overzicht (wat is er precies gebeurd?) te krijgen op de situatie. Zodat de Regio de juiste vervolgstappen kan nemen. Deze vragen dienen behandeld te worden in het Team Privacyincidenten.

- Om wat voor soort datalek gaat het?
Er zijn drie categorieën datalekken te onderscheiden:
  - Inbreuk op de vertrouwelijkheid
Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.
  - Inbreuk op de integriteit
Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
  - Inbreuk op de beschikbaarheid
Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van, toegang tot, of vernietiging van, persoonsgegevens.

Een datalek kan, afhankelijk van de omstandigheden, in meer dan één van deze drie categorieën vallen. Bij de Regio komt inbreuk op de vertrouwelijkheid echter veruit het meest voor.

- Wat is de oorzaak van het datalek?
- Wanneer is het datalek ontstaan? En bestaat het lek nog steeds?
- Hoe lang na het ontstaan van het datalek is het ontdekt? En hoe is het ontdekt?
- Wat voor soort persoonsgegevens zijn er gelekt? Bijvoorbeeld naam, adres, e-mailadressen, BSN en/of bijzondere persoonsgegevens.
- Hoeveel persoonsgegevens zijn er (bij benadering) gelekt? Om hoeveel personen gaat het?
- Om wat voor groepen mensen gaat het? Bijvoorbeeld werknemers, scholieren, patiënten, inwoners etc. Gaat het om kwetsbare groepen? Bijvoorbeeld kinderen, gehandicapten of bejaarden.
- Hoeveel onbevoegden hadden of hebben bij benadering (mogelijk) toegang tot de gelekte persoonsgegevens?
- Is er zicht op wie de onbevoegden zijn? En is het waarschijnlijk dat de onbevoegden kwade bedoelingen hebben met de gegevens? Of gaat het om een bekende, betrouwbare ontvanger?

- Heeft de Regio vooraf maatregelen getroffen waardoor de gelekte persoonsgegevens (deels) ontoegankelijk zijn voor onbevoegden? Bijvoorbeeld omdat de gegevens versleuteld zijn?

Stap 3) Moeten we het datalek melden aan de AP?
Niet alle datalekken hoeven bij de Autoriteit Persoonsgegevens (AP) te worden gemeld. Er moet gemeld worden tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor rechten en vrijheden van natuurlijke personen. Wel moeten álle datalekken geregistreerd worden.

Voor de beoordeling van het risico kan rekening worden gehouden met de volgende factoren:

- De aard van de inbreuk
Zijn er persoonsgegevens gewist, gewijzigd of verstrekt? Voorbeeld: het verstrekken van medische persoonsgegevens aan een onbevoegde, heeft andere gevolgen dan wanneer deze gegevens verloren zijn gegaan.

- De aard, gevoeligheid en omvang van de persoonsgegevens
Hoe gevoeliger de gegevens, hoe groter het risico op schade. Houd ook rekening met persoonsgegevens die al (openbaar) beschikbaar zijn. Want juist een combinatie van gegevens kan de impact groter maken.

- Gemak waarmee personen kunnen worden geïdentificeerd
Kun je op basis van het datalek eenvoudig zien om wie het gaat?

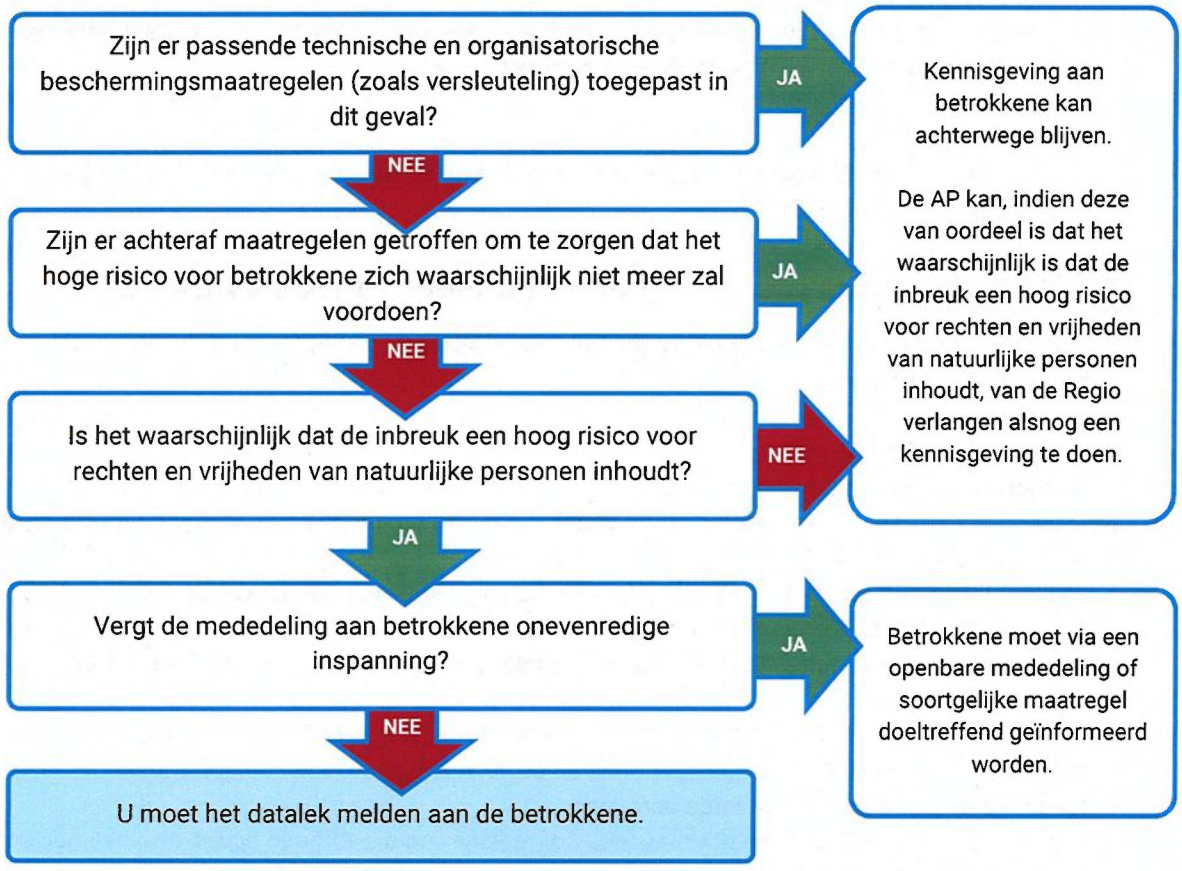
- Ernst van gevolgen voor personen
De gevolgen van een datalek kunnen ernstig zijn. Vooral wanneer het datalek kan leiden tot bijvoorbeeld identiteitsdiefstal of reputatieschade. Het risico wordt kleiner wanneer de gegevens in handen zijn gekomen van een betrouwbare ontvanger die er niet op uit is om schade te veroorzaken.

- Bijzondere kenmerken van de persoon
Wanneer gegevens van kwetsbare personen betrokken zijn bij het datalek, kunnen zij een groter risico op schade lopen. De gevolgen van onbevoegde toegang tot NAW-gegevens zullen voor de meeste mensen beperkt zijn, maar dit ligt anders voor mensen die te maken hebben met stalking of die in een blijf-van-mijn-lijfhuis verblijven. Voor betrokkenen zoals kinderen en mensen met een verstandelijke handicap, kan het moeilijker zijn om adequaat om te gaan met de gevolgen van een datalek. Zo zullen zij mogelijk eerder ingaan op pogingen tot phishing of oplichting.

- Bijzondere kenmerken van de verwerkingsverantwoordelijke
De risico's bij een datalek van een organisatie met veel bijzondere persoonsgegevens (m.n. gezondheidsgegevens) zoals de Regio is, zullen groter zijn dan bij een datalek met een mailinglijst van een krant.

- Het aantal getroffen personen
Over het algemeen kan een datalek grotere gevolgen hebben naarmate er meer personen bij betrokken zijn. Een inbreuk kan echter zelfs voor één persoon ernstige gevolgen hebben.

Stap 4) Moeten we het datalek melden aan de betrokkene?



Het datalek moet gemeld worden aan de betrokkene wanneer het waarschijnlijk is dat het datalek een **hoog** risico voor rechten en vrijheden van natuurlijke personen inhoudt, tenzij er vooraf of achteraf voldoende maatregelen zijn toegepast of mededeling aan betrokkene onevenredige inspanning vergt. In het laatste geval is dan wel een openbare mededeling of soortgelijke maatregel nodig waardoor de betrokkene doeltreffend wordt geïnformeerd. Denk hierbij aan plaatsing op een regionale nieuwswebsite of in een regionale krant.

Een hoog risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor de personen wier gegevens het voorwerp van de inbreuk zijn. Wanneer de inbreuk betrekking heeft op bijzondere persoonsgegevens moet dergelijke schade als waarschijnlijk worden beschouwd. Bijzondere persoonsgegevens zijn:

- persoonsgegevens waaruit ras of etnische afkomst, politieke opvatting, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt en
- genetische gegevens, biometrische gegevens met het oog op unieke identificatie van een persoon, gegevens over gezondheid en gegegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Voorbeelden van **lichamelijke, materiële of immateriële schade** zijn:

- Discriminatie
bijvoorbeeld bij een datalek met gegevens over ras, geloof of seksuele geaardheid.

- Identiteitsdiefstal of –fraude
bijvoorbeeld bij een datalek met complete paspoortkopieën. Of het BSN in combinatie met andere persoonsgegevens (zoals geboortedatum).

- Financiële verliezen
bijvoorbeeld bij een datalek met creditcardgegevens waardoor het risico bestaat dat iemand online bestellingen kan plaatsen op kosten van een ander.

- Reputatieschade
bijvoorbeeld bij een datalek met gegevens over problematische schulden, verslaving of prestaties op het werk.

4. Zwaarwegende redenen voor niet melden (artikel 41 UAVG)

De melding mag, na een zorgvuldige belangenafweging, achterwege blijven in het belang van:
a. de nationale veiligheid;
b. landsverdediging;
c. de openbare veiligheid;
d. de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
e. andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van Nederland, met name een belangrijk economisch of financieel belang van de Europese Unie of van Nederland, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;
f. de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
g. de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
h. een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de gevallen, bedoeld in de onderdelen a, b, c, d, e en g;
i. de bescherming van de betrokkene of van de rechten en vrijheden van anderen; of
j. de inning van civielrechtelijke vorderingen.

Regio
Gooi en Vechtstreek

Privacybeleid Regio Gooi en Vechtstreek

Algemeen	
Aan	CMT, DB, AB, OR
Van	[redacted]
Datum	2 juni 2021
Verspreiden	Nee
Kenmerk	21.0004032

Inhoudsopgave

Privacybeleid Regio Gooi en Vechtstreek 1
Versiebeheer 5
1. Inleiding 6
1.1 Algemeen 6
1.2 Achtergrond privacybeleid 6
1.2.1 Noodzaak 6
1.2.2 Doel en doelgroep privacybeleid 7
1.2.3 Verhouding met andere privacydocumenten 7
1.3 Reikwijdte privacybeleid 7
1.4 Leeswijzer 7
2. Juridisch kader 9
2.1 Wet- en regelgeving 9
2.2 Gehanteerde begrippen 9
3. Verwerkingsverantwoordelijkheid Regio 11
3.1 Delegatie en mandaat aan de Regio 11
3.2 Verwerkingsverantwoordelijkheid 11
4. Uitgangspunten voor bescherming persoonsgegevens 12
4.1 Rechtmatigheid, behoorlijkheid en transparantie 12
4.2 Doelbinding 12
4.3 Dataminimalisatie en juistheid 12
4.4 Bewaartermijnen 12
4.5 Integriteit en vertrouwelijkheid 13
4.6 Verantwoordingsplicht 13
5. Verwerkingen van persoonsgegevens algemeen en RVE-specifiek 13
5.1 Verwerkingen van de Regio 13
5.1.1 Doeleinden 13
5.1.2 Grondslagen 13
5.1.3 Verwerkte persoonsgegevens 14
5.1.4 Betrokkenen 15
5.1.5 Geautomatiseerde en handmatige verwerkingen 16
5.2 Regiobrede verwerkingen 16
5.3 Verwerkingen per RVE 16
6. Risico's 21
6.1 Risico's voor betrokkenen 21
6.2 Risico's voor de Regio 21
7. Maatregelen 22
7.1 Functionaris Gegevensbescherming (FG) 22
7.1.1 Toezicht 22
7.2 Beveiliging 23
7.2.1 Algemeen 23
7.2.2 RVE-specifiek 23
7.3 Transparantie en informatieplicht (privacyverklaring) 23
7.4 Bewustmaking en training 24
7.5 Gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen 24
7.6 Gegevensbeschermingseffectbeoordeling (DPIA) 24
7.7 Register van gegevensverwerkingen 25
7.8 Gegevens uitwisselen met derde partijen 25
7.8.1 Samenwerken 26
7.8.2 Inschakelen derde partijen 26
7.8.3 Afspraken tussen verwerkingsverantwoordelijken 26
7.8.4 Verwerkersovereenkomsten 27
7.9 Afhandelen van datalekken 27
7.10 Bewaren van persoonsgegevens 27

7.11 Omgaan met onderzoeken van de Autoriteit Persoonsgegevens 28
8. Rechten van de betrokkenen en klachten 28
8.1 Algemeen 28
8.2 Welke rechten hebben betrokkenen? 28
8.3 Ingeroepen rechten bij de Regio 29
8.4 Hoe oefenen betrokkenen hun rechten uit? 29
8.5 Toepasselijk wettelijk kader 30
8.6 Afhandelen verzoeken 30
8.6.1 Controle identiteit 30
8.6.2 Behandeling van verzoek 30
8.6.3 Beslissing op verzoek 31
8.6.4 Uitvoering van verzoek 31
8.7 Klachten 31
9. Geautomatiseerde verwerkingen 31
9.1 Geautomatiseerde besluitvorming 31
9.2 Onderzoek 31
9.3 Cameratoezicht 31
10. Overgangs- en slotbepalingen 32
10.1 Geldigheid privacybeleid 32
10.2 Inwerkingtreding, evaluatie en wijziging 32
10.2.1 Inwerkingtreding 32
10.2.2 Evaluatie 32
10.2.3 Wijziging 32
10.3. Slotartikel 32
Bijlagen 33
Bijlage 1 Afwijkingen privacybeleid voor zover Wet politiegegevens van toepassing is 33
5.1.2 Grondslagen 33
5.1.3 Verwerkte persoonsgegevens 33
5.1.4 Betrokkenen 34
7.2 Beveiliging 34
7.8 Delen met derden 34
7.10 Bewaren van persoonsgegevens 35
8.2 Welke rechten hebben betrokkenen? 36
Bijlage 2 Register van gegevensverwerkingen 37
Bijlage 3 Verwijzingen naar de verschillende privacyverklaringen op de websites van de Regio 38
Bijlage 4 Beschrijvingen/verantwoordingen van verwerkingen die de Regio uitvoert maar waarvoor de grondslag niet volkomen duidelijk is 38
Bijlage 5 Verwijzingen naar al vastgestelde stukken in MyCorsa 39

Het Dagelijks Bestuur van de Regio Gooi en Vechtstreek,
Gelezen het bepaalde in artikel 24 lid 2 van de Algemene Verordening Gegevensbescherming (AVG) en artikel 4a lid 1 sub a Wet politiegegevens,
Besluit vast te stellen:

Privacybeleid Regio Gooi en Vechtstreek

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.99	28-04-2021	[redacted]	Versie voor input aandachtsfunctionarissen privacy en werkgroep privacy
1.0	1-06-2021	[redacted]	Feedback [redacted] verwerkt
1.9	13-06-2021	CMT	Kennisneming, geen commentaar
2.0	21-06-2021	DB	Vaststelling

1. Inleiding

1.1 Algemeen

Binnen de Regio Gooi en Vechtstreek (hierna: de Regio) wordt veel gewerkt met persoonsgegevens van inwoners, medewerkers en partners. Persoonsgegevens van inwoners worden voornamelijk verzameld voor het goed uitvoeren van de gemeentelijke, aan de Regio overgedragen, wettelijke taken. Het belang van de Regio om persoonsgegevens te verwerken kan op gespannen voet staan met het privacybelang van de betrokkenen op wie de verzamelde gegevens betrekking hebben.
Het beschermen van privacybelangen wordt wel eens gezien als obstakel bij het uitvoeren van de werkzaamheden, omdat moet worden getoetst of aan de privacywetgeving wordt voldaan. Maar privacy is een belangrijk grondrecht. In de Grondwet is verankerd dat de overheid niet zomaar persoonlijke gegevens mag gebruiken. Het is een wettelijke verplichting dat overheidsorganisaties behoorlijk en zorgvuldig omgaan met persoonsgegevens in verband met de privacy van betrokkenen. Inwoners, bezoekers van de websites van de Regio en medewerkers van zowel de Regio als partijen waarmee de Regio samenwerkt, moeten erop kunnen vertrouwen dat de Regio zorgvuldig en veilig met de persoonsgegevens omgaat. In deze tijd gaat ook de Regio mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van persoonsgegevens. De Regio is zich hiervan bewust en zorgt dat privacy wordt gewaarborgd, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie en transparantie.

De Regio geeft middels dit privacybeleid een duidelijke richting aan privacy en laat zien dat zij privacy waarborgt, beschermt en handhaaft. Dit privacybeleid[1] is in lijn met het algemene beleid van de Regio en de relevante Europese, nationale en regionale wet- en regelgeving. Het privacybeleid sluit aan bij het Strategisch Informatiebeveiligingsbeleid Regio Gooi en Vechtstreek van 2019 tot en met 2022 (Corsa: 19.0013516, hierna Informatiebeveiligingsbeleid). Immers, informatiebeveiliging en het veilig en verantwoord werken met persoonsgegevens overlappen elkaar voor een groot deel. Voor het borgen van de bescherming van persoonsgegevens is het naleven van wat is geregeld in het Informatiebeveiligingsbeleid dan ook van cruciaal belang.

1.2 Achtergrond privacybeleid

1.2.1 Noodzaak

Wanneer een organisatie op grote schaal bijzondere persoonsgegevens verwerkt dient die organisatie een gegevensbeschermingsbeleid (verder: privacybeleid) op te stellen en te hanteren.[2] Binnen de Regio verwerken een aantal onderdelen op grote schaal bijzondere persoonsgegevens, voornamelijk gezondheidsgegevens. Hierbij valt o.a. te denken aan de GGD, Jeugd en Gezin, Veilig Thuis en Zorg- en Veiligheidshuis. Daarom is het hebben van een privacybeleid voor de Regio een verplichting.

[1] Privacybeleid moet inhoudelijk gezien worden als interne instructie voor de medewerkers van de Regio en heeft niet de intentie regels te scheppen (zoals bij de meeste andere soorten van beleid het geval is).
[2] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_verkennend_onderzoek_gegevenschermingsbeleid.pdf

1.2.2 Doel en doelgroep privacybeleid

Het doel van dit privacybeleid is om de belangen van betrokkenen van wie de Regio persoonsgegevens verwerkt centraal te stellen en te waarborgen dat de gegevensverwerking op een rechtmatige wijze plaatsvindt.
Het privacybeleid is bedoeld voor Regio-medewerkers als handleiding voor het werken met persoonsgegevens. Het maakt duidelijk wat er van hen exact wordt verwacht zodat persoonsgegevens rechtmatig worden verwerkt.
In het privacybeleid is beschreven hoe de Regio de privacywetgeving heeft geïmplementeerd. Het privacybeleid geeft aan op welke wijze voldaan wordt aan de van toepassing zijnde wet- en regelgeving en wat het ambitieniveau van de Regio is om aan deze wetgeving te voldoen. De AVG bevat veel open normen waaraan in dit privacybeleid invulling gegeven wordt.

1.2.3 Verhouding met andere privacydocumenten

Naast het privacybeleid hanteert de Regio privacyverklaringen op de verschillende websites. Privacyverklaringen zijn, anders dan dit privacybeleid, extern gericht, namelijk gericht op de betrokkene en geven informatie over hoe en waarom persoonsgegevens van de betrokkene worden verwerkt. Dit privacybeleid is in tegenstelling tot de privacyverklaringen dan ook niet publiekelijk toegankelijk en wordt niet gepubliceerd.
De Autoriteit Persoonsgegevens raadt aan om alle informatie over hoe een organisatie met persoonsgegevens omgaat in één document vast te leggen. Om die reden zijn in de bijlagen bij dit beleid de andere stukken opgenomen die informatie geven over hoe de Regio omgaat met het verwerken van persoonsgegevens. Zie hiervoor 1.4 Leeswijzer

1.3 Reikwijdte privacybeleid

Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en zowel geautomatiseerde als handmatige verwerkingen van persoonsgegevens door de Regio. Vervoer Gooi en Vechtstreek B.V. heeft een eigen privacybeleid en valt dus niet onder dit privacybeleid. De Regio heeft te maken met twee verschillende privacyregimes. Voor het overgrote deel van de organisatie geldt de Algemene Verordening Gegevensbescherming (hierna: AVG) i.c.m. de Uitvoeringswet Algemene Verordening Gegevensbescherming (hierna: UAVG). Voor het strafrechtelijke deel van het werk van de buitengewoon opsporingsambtenaren (hierna: BOA's) bij GAD en RBL geldt in plaats van de AVG de Wet politiegegevens. Beide regimes vereisen een privacybeleid. Dit privacybeleid is het beleid voor deze beide regimes.
Het privacybeleid wordt in een volgend stadium nog verder geoperationaliseerd voor de verschillende organisatieonderdelen.

1.4 Leeswijzer

In hoofdstuk 2 wordt het juridisch kader en het bijbehorende begrippenkader van het privacybeleid beschreven. Hoofdstuk 3 behandelt de verwerkingsverantwoordelijkheid van de Regio en hoe dat in de organisatie is belegd. Hoofdstuk 4 gaat over de uitgangspunten van bescherming van persoonsgegevens. In hoofdstuk 5 komen de verwerkingen van persoonsgegevens binnen de Regio aan de orde.
Hoofdstuk 6 bespreekt risico's voor betrokken en de Regio. Hoofdstuk 7 behandelt de maatregelen die de Regio heeft getroffen om aan te tonen dat wordt voldaan aan de AVG. In hoofdstuk 8 wordt het proces van rechten van betrokkenen en de klachtafhandeling behandeld. Hoofdstuk 9 gaat in op het

voorkomen van geautomatiseerde verwerkingen bij de Regio. Hoofdstuk 10 ten slotte gaat over de geldigheid van het privacybeleid en regelt de inwerkingtreding, evaluatie en wijziging van het beleid.

Bijlage 1: Het privacybeleid geldt als algemeen kader voor de gehele organisatie. Zoals hiervoor aangegeven heeft de Regio voornamelijk met de AVG te maken en voor een klein deel met de Wet politiegegevens. Aangezien beide regimes in grote lijnen hetzelfde zijn, wordt in het privacybeleid uitgegaan van de AVG (en daarmee van de term persoonsgegevens). De afwijkingen die gelden onder de Wet politiegegevens (waar het gaat om politiegegevens, een bijzondere variant van persoonsgegevens) worden in deze bijlage 1 aangegeven.
Bijlage 2: het register van gegevensverwerkingen
Bijlage 3: verwijzingen naar de verschillende privacyverklaringen op de websites van de Regio
Bijlage 4: beschrijvingen/verantwoordingen van verwerkingen die de Regio uitvoert maar waarvoor de grondslag niet volkomen duidelijk is
Bijlage 5: verwijzingen naar al vastgestelde stukken in MyCorsa (o.a. werkinstructies aangaande interne procedures rondom het verwerken van persoonsgegevens)

2. Juridisch kader

2.1 Wet- en regelgeving

De Regio is voor de omgang met persoonsgegevens gebonden aan de volgende wettelijke kaders:
- Algemene Verordening Gegevensbescherming (hierna: AVG)
- Uitvoeringswet Algemene Verordening Gegevensbescherming (hierna: UAVG)
- Besluit politiegegevens buitengewoon opsporingsambtenaren in combinatie met Wet politiegegevens en Besluit politiegegevens (voor het strafrechtelijk deel van het werk van de BOA's van de Regio).

Daarnaast bevatten ook enkele inhoudelijke wetten relevante privacybepalingen die invloed hebben op de wijze waarop de Regio omgaat met persoonsgegevens. Hierbij moet met name gedacht worden aan de volgende wetten:
- Jeugdwet
- Wet op de geneeskundige behandelingsovereenkomst (Wgbo, Boek 7, Titel 7, Afdeling 5 Burgerlijk Wetboek)
- Wet Maatschappelijke Ondersteuning 2015.

2.2 Gehanteerde begrippen

AVG
Algemene Verordening Gegevensbescherming.

UAVG
Uitvoeringswet Algemene Verordening Gegevensbescherming.

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
Feitelijk betreft het elk stukje informatie dat naar een specifieke persoon (of kleine groep personen) is te herleiden.

Politiegegeven
Elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak.

Verwerking van persoonsgegevens
Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Feitelijk betreft het alle handelingen die je met persoonsgegevens kunt doen.

Bestand
Elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid.

Verwerkingsverantwoordelijke
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
In het geval van de Regio is dit meestal (in ieder geval voor de taken die in de Gemeenschappelijke Regeling worden benoemd) het Dagelijks Bestuur van Regio Gooi en Vechtstreek.

Verwerker
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft.
Voor dit beleid wordt er vanuit gegaan dat het met name gaat om verschillende soorten Regio-inwoners (zoals cliënten en hun contacten en jongeren en hun ouders/verzorgers), medewerkers van zowel de Regio als partijen waarmee de Regio samenwerkt (o.a. regiogemeenten, zorgaanbieders en bedrijven), mensen die melding maken over een inwoner en bezoekers van websites van de Regio. In de verschillende privacyverklaringen zijn de betrokkenen nader benoemd.

Ontvanger
Degene aan wie de persoonsgegevens worden verstrekt.

Toestemming van de betrokkene
Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.

Autoriteit Persoonsgegevens
De onafhankelijke overheidsinstantie die op grond van de AVG tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig de AVG en UAVG en op verwerking van politiegegevens overeenkomstig de Wet politiegegevens.

Functionaris Gegevensbescherming (FG)
De interne toezichthouder die op grond van de AVG tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig de AVG, Uitvoeringswet Algemene Verordening Gegevensbescherming en het privacybeleid van de Regio.

Bijzondere persoonsgegevens
Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Medisch dossier
Verzameling van gegevens over een patiënt die een zorgverlener opstelt en bewaart. Het betreft hier vooral gegevens over klachten, diagnoses en behandelingen. Op deze dossiers is de Wet op de geneeskundige behandelingsovereenkomst (Wgbo) van toepassing.

Inbreuk in verband met persoonsgegevens (ook wel: datalek)
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.

Register van gegevensverwerkingen (ook wel: verwerkingsregister)
Het binnen de Regio centraal beheerde register met alle verwerkingen van persoonsgegevens.

3. Verwerkingsverantwoordelijkheid Regio

3.1 Delegatie en mandaat aan de Regio

De Regio is een gemeenschappelijke regeling van de gemeenten in de regio Gooi en Vechtstreek. De meeste taken die de Regio uitvoert zijn via de gemeenschappelijke regeling gedelegeerd aan de Regio. Dit betekent dat de wettelijke gronden waarop de gemeenten deze taken uitvoeren ook voor de Regio gelden. Deze gemeenschappelijke regeling betreft de zwaarste vorm van een publiekrechtelijke samenwerking, namelijk een openbaar lichaam. Er zijn ook enkele taken in mandaat aan de Regio gegeven. Hierbij gelden de wettelijke gronden zowel voor de regiogemeente als voor de Regio.

3.2 Verwerkingsverantwoordelijkheid

Het Dagelijks Bestuur is de verwerkingsverantwoordelijke in de zin van de AVG voor de door de regiogemeenten overgedragen taken. Dit betekent dat zij eindverantwoordelijk is voor alles wat te maken heeft met de bescherming van persoonsgegevens binnen de Regio.[3]
Het lijnmanagement is verantwoordelijk voor de eigen processen, inclusief informatiebeveiliging en gegevensbescherming. Deze verantwoordelijkheid ligt dus bij de Algemeen Directeur, die verantwoordelijk is voor de juiste en volledige implementatie van de privacyregelgeving. En uiteraard bij de RVE-managers. Dit betekent dat de RVE-manager verantwoordelijk is voor een goede uitvoering van de privacywetgeving binnen de eigen RVE. Dit is ook praktisch aangezien de RVE-manager het best zicht heeft op wat er binnen de RVE gebeurt met persoonsgegevens. Uiteraard zijn de medewerkers (inclusief inhuur/externen) ook zelf verantwoordelijk voor de bescherming van de privacy van betrokkene(n) bij de uitvoering van hun werkzaamheden. Dat betekent dat iedereen zorgt voor een veilige, rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens.

Alle RVE-managers hebben één of meerdere aandachtsfunctionarissen privacy benoemd om hen te ondersteunen in hun verantwoordelijkheid. De aandachtsfunctionarissen zijn het eerste aanspreekpunt voor privacy voor de eigen RVE en voor de FG. Zij signaleren wijzigingen in de verwerkingen van persoonsgegevens en coördineren voor hun RVE de afhandeling van de organisatiebrede verzoeken (zoals verzoeken om inzage) die inwoners en medewerkers bij de Regio kunnen indienen.

[3] Bij taken die in mandaat aan de Regio zijn gegeven, zou het (afhankelijk van wie doel en middelen van de verwerking bepaalt) kunnen zijn dat de Regio samen met de opdrachtgevende regiogemeente verwerkingsverantwoordelijke is.

Daarnaast zijn er nog de adviseurs ten aanzien van privacy. De juridisch adviseurs adviseren over privacyissues t.a.v. RVE- en personeelsaangelegenheden. De FG adviseert over concernbrede privacyissues (vraagstukken die niet specifiek voor één RVE spelen maar overal in de organisatie zouden kunnen spelen). Daarnaast houdt de FG binnen de organisatie toezicht op de toepassing en naleving van de privacywetgeving en het privacybeleid.
Voor een uitgebreide versie van de verantwoordelijkheden voor privacyzaken zie Bijlage 5 Rollen, taken en verantwoordelijkheden privacy.[4]

4. Uitgangspunten voor bescherming persoonsgegevens

4.1 Rechtmatigheid, behoorlijkheid en transparantie

Uit de AVG vloeit voort dat voor elke verwerking van persoonsgegevens een wettelijke grondslag aanwezig moet zijn. Hierbij geldt dat de verwerking op een zorgvuldige wijze geschiedt. Verder wordt bij de verwerking van persoonsgegevens transparantie nagestreefd. Hiervoor informeert de Regio betrokkenen via de verschillende privacyverklaringen. Verder kunnen betrokkenen bepaalde rechten met betrekking tot hun persoonsgegevens inroepen.

4.2 Doelbinding

Volgens de AVG mogen persoonsgegevens alleen verzameld worden als daarvoor een doel is vastgesteld. De doelen van de Regio zijn uitdrukkelijk omschreven en gerechtvaardigd. De gegevens worden niet verwerkt voor een ander doel dan waarvoor ze zijn verzameld.
In enkele gevallen zal sprake zijn van een verdere verwerking van de verzamelde persoonsgegevens, waarbij dan voldaan is aan de voorwaarde dat de verdere verwerking verenigbaar is met het oorspronkelijke doel.

4.3 Dataminimalisatie en juistheid

De Regio verwerkt alleen de persoonsgegevens die noodzakelijk zijn voor het vooraf bepaalde doel. De Regio verwerkt echter wel voldoende gegevens om betrokkene op correcte wijze en op basis van de juiste informatie van haar diensten te kunnen voorzien.

4.4 Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan nodig is voor de uitvoering van de aan de Regio opgedragen taken of om wettelijke verplichtingen na te kunnen leven. Dit houdt in dat deze gegevens vernietigd worden of zo worden aangepast dat de informatie niet meer herleid kan worden naar een natuurlijk persoon.
De Regio bewaart digitale en papieren documenten (met persoonsgegevens) volgens het retentiebeleid zoals opgenomen in de intergemeentelijke selectielijst, welke lijst een verplichting is uit de Archiefwet. Zie hiervoor bijlage 5 Goed Geordend Overzicht van Informatie (GGO) Regio Gooi en Vechtstreek 2020 waarin de selectielijst is opgenomen. Anders dan wat vaak wordt gedacht, bevat de AVG zelf dus geen bewaartermijnen.
Enkele bewaartermijnen zijn zo duidelijk dat ze hieronder al kort worden benoemd.
Voor dossiers i.h.k.v. de Wgbo en Jeugdwet en voor de Veilig Thuis-dossiers geldt een bewaartermijn van 20 jaar na laatste wijziging in het dossier tenzij uit specifieke wetgeving een andere bewaartermijn

[4] In dat document is de rol van aandachtsfunctionaris privacy nog niet opgenomen.

volgt.[5] Voor de medisch dossiers van minderjarigen start deze bewaartermijn vanaf de datum waarop het 18e levensjaar wordt bereikt. Bij overlijden begint deze termijn te lopen vanaf de datum van overlijden.
Voor (persoonsgegevens in) financiële stukken geldt een bewaartermijn van 7 jaar.
CV's en brieven van sollicitanten worden in beginsel maximaal 4 weken bewaard. Met toestemming van de sollicitant kan de sollicitatie maximaal 1 jaar 'in portefeuille worden gehouden'.
Camerabeelden mogen maximaal 4 weken worden bewaard. Bij incidenten kunnen de beelden worden bewaard tot het incident is afgehandeld.

4.5 Integriteit en vertrouwelijkheid

De Regio gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk.
Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht (zie hiervoor bijlage 5 de Gedragscode integriteit, na Wnra). Voor vaste medewerkers hoort deze geheimhoudingsplicht van rechtswege bij het ambtenaarschap. Vaste medewerkers dienen vóór indiensttreding ook een verklaring omtrent gedrag (VOG) te overleggen. Externen krijgen ook de Gedragscode integriteit toegestuurd met de vraag deze goed te lezen, daarnaast tekenen zij een integriteitsverklaring waarin ook geheimhouding is opgenomen. Afhankelijk van de gevoeligheid van het werk moeten zijzelf een VOG overleggen of zorgen de organisaties waaraan zij zijn verbonden er voor dat er een VOG is aangevraagd en verkregen.
De Regio zorgt met technische en organisatorische maatregelen voor passende beveiliging van persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft.

4.6 Verantwoordingsplicht

Het Dagelijks Bestuur van de Regio is als verwerkingsverantwoordelijke verantwoordelijk voor de naleving van deze algemene beginselen van de AVG en kan dit aantonen. Met dit privacybeleid (en de naleving daarvan) borgt de Regio deze beginselen in de organisatie. Verder zijn er nog andere registraties die deze verantwoordingsplicht verder invullen. Zo is er naast het register van gegevensverwerkingen en het register van datalekken en incidenten, een registratie van de afgesloten verwerkersovereenkomsten, de ontvangen verzoeken i.h.k.v. rechten van betrokkenen en de door de FG gegeven adviezen en reacties daarop door betreffende RVE-manager.

5. Verwerkingen van persoonsgegevens algemeen en RVE-specifiek

5.1 Verwerkingen van de Regio

5.1.1 Doeleinden

De Regio verwerkt persoonsgegevens van inwoners en medewerkers (betrokkenen) voor verschillende doeleinden die erg gevarieerd zijn gezien de brede organisatie die de Regio is.

5.1.2 Grondslagen

Voor alle doeleinden is het hebben van een grondslag om persoonsgegevens te verwerken vereist.[6]

[5] Een voorbeeld is de samenloop van de Wgbo en de Wet publieke gezondheid op sommige dossiers van de GGD.
[6] Het strafrechtelijke werk van de BOA's valt onder de Wet politiegegevens, welke wet haar eigen grondslagen kent, zie hiervoor Bijlage 1 Afwijkingen privacybeleid voor zover Wet politiegegevens van toepassing is.

De AVG kent de volgende grondslagen voor verwerken van persoonsgegevens:
a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden (hierna: Toestemming);
b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen (hierna: Noodzakelijk voor uitvoering overeenkomst);
c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (hierna: Noodzakelijk voor voldoen wettelijke verplichting);
d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen (hierna: Noodzakelijk voor bescherming vitaal belang);
e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (hierna: Noodzakelijk voor taak algemeen belang of taak openbaar gezag);
f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is (hierna: Noodzakelijk voor behartiging gerechtvaardigd belang).

Het merendeel van de verwerkingen door de Regio vloeit rechtstreeks voort uit een in wetgeving aan de gemeente[7] opgedragen taak in het kader van de uitoefening van het openbaar gezag (grondslag e, ook wel: publieke taak).
Verder verwerkt de Regio voornamelijk persoonsgegevens als dat noodzakelijk is om aan een wettelijke verplichting te voldoen (grondslag c). In Nederlandse wetten is bepaald wat deze (overgedragen) wettelijke verplichtingen en taken zijn.
In enkele gevallen vraagt de Regio toestemming (grondslag a) voor het verwerken van persoonsgegevens (bijvoorbeeld bij aanmelden voor nieuwbrieven en voor door de Regio georganiseerde bijeenkomsten en bij insturen van webformulieren).
Ook worden persoonsgegevens verwerkt als dat noodzakelijk is om een gerechtvaardigd belang van de Regio te behartigen (grondslag f, bijvoorbeeld verwerkingen in het kader van een goede bedrijfsvoering door de Regio).
Twee grondslagen komen slechts bij enkele RVE's voor. Het gaat om verwerkingen die noodzakelijk zijn voor de uitvoering van een overeenkomst met betrokkene (grondslag b, bijvoorbeeld uitvoering van de arbeidsovereenkomst) en verwerkingen die noodzakelijk zijn om vitale belangen van mensen te beschermen (grondslag d, bijvoorbeeld als een bewusteloze patiënt met de ambulance vervoerd wordt).

5.1.3 Verwerkte persoonsgegevens

Herleidbaarheid naar een persoon (of kleine groep personen) is bepalend of sprake is van persoonsgegevens. De meeste mensen zullen bij persoonsgegevens denken aan feitelijke gegevens als NAW, telefoonnummer of geboortedatum. Maar ook een stukje tekst over iemands gezondheid in een dossier is een persoonsgegeven, want herleidbaar naar die persoon.
Er bestaan verschillende soorten persoonsgegevens: gewone persoonsgegevens, bijzondere persoonsgegevens, gevoelige persoonsgegevens, wettelijke identificatienummers, strafrechtelijke persoonsgegevens en politiegegevens.

[7] Via de Gemeenschappelijke Regeling zijn bepaalde gemeentelijke taken aan de Regio gedelegeerd.

Gewone persoonsgegevens betreffen bijvoorbeeld naam, adres, woonplaats en telefoonnummer. Deze worden bij de Regio veelvuldig verwerkt.

Bijzondere persoonsgegevens zijn gegevens die extra beschermd zijn vanwege de verstrekkende negatieve gevolgen (waaronder discriminatie) wanneer met die gegevens niet goed wordt omgegaan. Het gaat om gegevens die informatie bevatten over o.a. ras, etnische afkomst, politieke opvattingen, religie, gezondheid, seksueel gedrag en seksuele gerichtheid. Deze gegevens mogen niet worden verwerkt tenzij een uitzondering op het verwerkingsverbod geldt, bijvoorbeeld omdat dit op grond van de wet mag. Voor de Regio zijn vooral de gezondheidsgegevens (verder: medische gegevens) relevant. In het kader van de GGD-taak seksuele gezondheid kunnen ook gegevens worden verwerkt over seksueel gedrag en seksuele gerichtheid.
De Regio is ook verantwoordelijk voor enkele medisch dossiers, zoals bij J&G, GGD en RAV. Op deze dossiers is de Wgbo van toepassing.

Dan is er de tussencategorie gevoelige persoonsgegevens, waarvoor het hiervoor bedoelde verbod niet geldt, maar welke wel extra moeten worden beschermd.
Het gaat dan bijvoorbeeld om gegevens over de financiële situatie van de betrokkene, gegevens over overtredingen van wettelijke voorschriften, bestuurlijke en/of tuchtrechtelijke maatregelen of sancties, gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene en gegevens die betrekking hebben op kwetsbare groepen. Dergelijke gegevens worden door enkele RVE's verwerkt.

Wettelijke identificatienummers zijn nummers ter identificatie van een persoon die bij wet zijn voorgeschreven. Deze mogen slechts worden verwerkt voor doeleinden die bij wet zijn bepaald. De gedachte hierachter is dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. Het gaat hierbij enkel om in de wet voorgeschreven persoonsidentificerende nummers. Bij de Regio kun je denken aan het burgerservicenummer (BSN) en het BIG-nummer (beroepen in de individuele gezondheidszorg).

Strafrechtelijke persoonsgegevens zijn persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Bij enkele RVE's worden zulke gegevens verwerkt.

Ten slotte zijn er politiegegevens. Dit komt bij de Regio voor bij het strafrechtelijke werk van de BOA's, zie hiervoor Bijlage 1 Afwijkingen privacybeleid voor zover Wet politiegegevens van toepassing is.

5.1.4 Betrokkenen

Bij de meeste RVE's worden voornamelijk persoonsgegevens van inwoners verwerkt.[8] Hierbij kan gedacht worden aan cliënten en patiënten. Bij jongeren gaat het vaak om informatie over kind én ouder(s)/verzorger(s). Bij de RVE's die met ernstige problematiek te maken hebben (en waarbij reconstructie van wat is gebeurd van belang is), zijn betrokkenen van wie de gegevens worden verwerkt niet alleen degenen om wie de Regio zich zorgen maakt, maar ook contacten van deze personen, de melder en betrokken medewerkers. Bij deze RVE's kan het ook voorkomen dat cliënten

[8] Het strafrechtelijke werk van de BOA's valt onder de Wet politiegegevens, welke wet andere categorieën van betrokkenen kent, zie hiervoor Bijlage 1 Afwijkingen privacybeleid voor zover Wet politiegegevens van toepassing is.

gesprekken met medewerkers willen opnemen. Dat recht hebben ze, als ze het maar van tevoren aangeven.
Bij de RVE Bedrijfsvoering worden juist voornamelijk gegevens van medewerkers verwerkt om hen in hun werk goed te kunnen ondersteunen. Bij enkele RVE's worden daarnaast ook gegevens verwerkt van medewerkers van organisaties waarmee de Regio samenwerkt (zoals regiogemeenten, zorgaanbieders en bedrijven). Een aparte groep betrokkenen wordt gevormd door de bezoekers van de websites van de Regio.

Bepaalde betrokkenen zijn kwetsbaarder dan anderen en moeten daarom extra worden beschermd (dit wordt bijvoorbeeld gerealiseerd doordat datalekken van deze betrokkenen eerder gemeld moeten worden bij de Autoriteit Persoonsgegevens). Met kwetsbaar wordt bedoeld dat de negatieve effecten van een (onrechtmatige) gegevensverwerking groter kunnen zijn voor bepaalde betrokkenen dan voor andere. Denk bijvoorbeeld aan minderjarigen, ouderen en mensen die te maken hebben met stalking.

In de verschillende privacyverklaringen van de RVE's worden de betreffende betrokkenen nader benoemd.

5.1.5 Geautomatiseerde en handmatige verwerkingen

De meeste verwerkingen binnen de Regio betreffen geautomatiseerde, digitale, verwerkingen. Maar bij enkele organisatieonderdelen worden ook nog vaak persoonsgegevens handmatig, op papier, verwerkt. De digitale verwerkingen vallen altijd onder de AVG. De handmatige verwerkingen vallen onder de AVG als ze in een gestructureerd geheel van persoonsgegevens die volgens meerdere criteria toegankelijk zijn (ook wel: bestand), zíjn opgenomen of bestemd zijn om daarin te wórden opgenomen.

5.2 Regiobrede verwerkingen

De meeste verwerkingen binnen de organisatie van de Regio zijn specifiek voor een RVE. Maar er zijn ook verwerkingen die overal in de organisatie kunnen plaatsvinden of die geen betrekking hebben op een specifieke RVE.
Hierbij valt te denken aan o.a. de volgende verwerkingen:
- videobellen via Zoom/Teams;
- behandelen van aanmeldingen voor nieuwsbrieven, ingestuurde webformulieren en aanmeldingen voor door de Regio georganiseerde bijeenkomsten;
- secretariële werkzaamheden;
- afhandelen van meldingen mogelijke datalekken; en
- behandelen van klachten over medewerkers/afdelingen.

5.3 Verwerkingen per RVE

Onderstaande informatie over de verwerkingen bij verschillende RVE's betreft een niet-uitputtende samenvatting van de verwerkingen van de Regio. Voor details van specifieke verwerkingen, de doelstellingen, grondslagen, verwerkte persoonsgegevens en meer informatie per verwerking zie bijlage 2 Register van gegevensverwerkingen.

De letteraanduidingen bij de kolom Grondslag hebben de volgende betekenissen:
a) Toestemming
b) Noodzakelijk voor uitvoering overeenkomst
c) Noodzakelijk voor voldoen wettelijke verplichting
d) Noodzakelijk voor bescherming vitaal belang
e) Noodzakelijk voor taak algemeen belang of taak openbaar gezag
f) Noodzakelijk voor behartiging gerechtvaardigd belang
P) Wet politiegegevens is van toepassing op strafrechtelijke werk van de BOA's (bij GAD en RBL).

Door middel van een enkele + (komt soms voor) of dubbele + (komt vaak voor) wordt aangegeven of een grondslag van toepassing is.

RVE/ onderdeel	Doelstelling verwerken persoonsgegevens	Grondslag							Persoonsgegevens/ bijzondere persoonsgegevens
		a	b	c	d	e	f	P	
GAD	-registratie en vastlegging van gebruikers en in bruikleen ter beschikking gestelde toegangspasjes/-druppels en inzamelmiddelen; - emailsignalering ophaaldagen diverse componenten op verzoek, inclusief voorlichting; - registratie ten behoeve van afhandeling van verzoeken en klachten. - registratie van personeelsgegevens om uitvoering te geven aan					+ +	+ [9]		NAW- gegevens, telefoonnummer, e-mail, bar/chipcode, camerabeelden
T&H	Registratie van gegevens processen-verbaal en klachtenkaarten ter ondersteuning van de wettelijke toezicht- en handhavingstaken.			+ +		+ +		+ +	NAW- gegevens, telefoonnummer, e-mail, geboortedatum, KVK informatie, aard van de overtreding, foto's of film m.b.t. overtreding
GGD	Uitvoering van de wettelijke taken van de GGD zoals beschreven in de Wet publieke gezondheid en aanvullende taken uit de gemeentelijke nota's over het lokale beleid gezondheidszorg	+ [10]	+ + [11]	+		+ +			NAW-gegevens, telefoonnummer, e-mail, geboortedatum, BSN, medische gegevens
J&G	----------	-	-	-	-	-	-	-	----------
J&G	Bieden van jeugdgezondheidszorg (consultatiebureau en 'schoolarts') en daarnaast advies en ondersteuning bij groei, ontwikkeling en opvoeding van kinderen.	+	+ + [12]	+		+ +			NAW-gegevens, telefoonnummer, e-mail, naam kind, geboortedatum kind, BSN, medische

[9] Voor bedrijfsvoeringsdoeleinden
[10] Voor verwerkingen via GGD-websites
[11] Door toepasselijkheid Wgbo
[12] Door toepasselijkheid Wgbo

								gegevens
RBL	Zo veel mogelijk jongeren naar school laten gaan en een diploma laten behalen.	+		+ + [13]		+ +	+ +	NAW-gegevens, telefoonnummer, e-mail, geboortedatum, BSN, gegevens onderwijsinstelling(en), DUO verzuimmelding, verzuimoverzicht van de school, door verdachte aangeleverde informatie, (soms) medische gegevens, strafrechtelijk verleden i.v.m. eerdere overtreding Leerplichtwet (strafrechtelijke persoonsgegevens)
MaDi	----------	-	-	-	-	-	-	- ----------
Urgentie-bureau	Het adequaat rapporteren en adviseren over de omstandigheden van urgentieaanvragers ten behoeve van de zorgvuldigheid van de besluitvorming over urgentieaanvragen[14]					+ +		NAW-gegevens, telefoonnummer, email, woonsituatie, huisgenoten, financiële gegevens, (soms) medische gegevens
Veilig Thuis	Uitvoeren van de wettelijke taak van Veilig Thuis.	+		+ +	+	+ +		NAW-gegevens, telefoonnummer, email, geboortedatum, BSN, gezagsverhouding over persoon, woonsituatie en medische gegevens
Veilig Verder	Bespreken van mogelijkheden jeugdhulp vrijwillig kader of noodzaak tot onderzoek naar jeugdbeschermingskader					+ +		NAW-gegevens, telefoonnummer, email, geboortedatum, BSN, gezagsverhouding over persoon, woonsituatie en medische gegevens
I&C	- Opdrachtverstrekking, factuur- en		+	+		+		NAW-gegevens,

[13] O.a. door uitvoeren meldcode en terugmeldverplichting BRP

[14] Deze taak is aan de Regio in mandaat gegeven en maakt geen onderdeel uit van de Gemeenschappelijke Regeling. Tot nu gaat de Regio hier uit van verwerkingsverantwoordelijkheid van de Regio alleen.

	opdrachtcontrole en doorgeven van de betaalverplichting aan gemeenten al dan niet via het Digitaal Leefplein (DLP). - Inkopen, contracteren en beheren van alle producten en dienstverlening van bedrijven en organisaties.			+		+			telefoonnummer, email, geboortedatum, BSN, woonsituatie, beschikkingsnummer, medische gegevens (via productcodes)
WSP	De uitvoering van de dienstverlening aan werkgevers, de registratie van werkzoekenden en vacatures en de regionale samenwerking met het UWV in de arbeidsmarktregio Gooi en Vechtstreek op grond van de artikelen 9 en 10 van de Wet structuur uitvoeringsorganisatie werk en inkomen.	+ +				+ +			NAW-gegevens, CV, klantprofiel, contactgegevens werkgevers
RAV	Het verlenen van professionele, hoogwaardige en veilige ambulancezorg op grond van de Wet ambulancezorgvoorzieningen en de uitvoering van het ambulancedeel in de meldkamer die gemeenschappelijk met politie en brandweer wordt beheerd. Er worden ook gegevens verwerkt voor declaratie bij de zorgverzekeraar.	+	+	+ +	+ +	+			NAW-gegevens, telefoonnummer, email, geboortedatum, BSN, geslacht, verzekeringsnummer, huisarts, medische gegevens en verzekeringsgegevens. Stem en gemoedstoestand van melder.
Sturing	Organiseren van bijeenkomsten	+ +	+			+ +			NAW-gegevens, telefoonnummer, email, soms geslacht, IBAN rekeningnummer en handtekening
Zorg- en Veilig-heidshuis (ZVH)	Via netwerksamenwerking tussen straf-, zorg- en (andere) gemeentelijke partners, onder eenduidige regie komen tot een ketenoverstijgende aanpak van complexe persoons-, systeem- en gebiedsgerichte problematiek om ernstige overlast en criminaliteit te bestrijden. Dit doet ZVH door overleggen op kantoor te organiseren en gegevens vast te leggen in haar systemen.[15]					+ + 16			NAW-gegevens, telefoonnummer, e-mail, geboorteplaats, geboortedatum, medische gegevens, woonsituatie, financiële gegevens, relatiegegevens, toezicht- en handhavingsgegevens, gegevens omtrent bestuursrechtelijke maatregelen,

[15] Voor deze werkzaamheden van de procesregisseur en ondersteuners is de Regio (met de partners van ZVH) gezamenlijk verwerkingsverantwoordelijk.

[16] Bij Zorg- en Veiligheidshuis geldt dat zij (nog) geen eigenstandige wettelijke basis heeft om persoonsgegevens te verwerken. De partijen die deelnemen aan het samenwerkingsverband hebben wel ieder separate rechtsgronden voor de verwerking van persoonsgegevens, op basis waarvan ook gegevens kunnen worden gedeeld.

								strafrechtelijke persoonsgegevens
CenA-team	- Het ondersteunen van wettelijk verwijzers als huisartsen, medisch specialisten en jeugdartsen en het bieden van inhoudelijk advies ten behoeve van de beoordeling tweede prestatie basis GGZ en specialistische GGZ. - Het gezamenlijk organiseren van de toeleiding tot ernstig enkelvoudige dyslexie (EED) en het bij een derde partij beleggen van de screeningstaak van dossiers.	+ +[17]				+ +		NAW-gegevens, medische gegevens
Visit Gooi & Vecht	Het verrichten van marketingactiviteiten en informatievoorziening via toezenden van nieuwsbrieven en het faciliteren van aanmelden van evenementen om de regio Gooi en Vechtstreek te versterken als aantrekkelijke regio voor bezoek en recreatie.	+ +						Voornaam, achternaam, email
Bedrijfs-voering	----------	-	-	-	-	-	-	- ----------
HR[18]	- Voldoen aan wettelijke fiscale en SZ-eisen (Belasting, premie WIA, WW), voldoen aan cao SGO, uitvoering arbeidsvoorwaarden en pensioen (ABP) betrokken medewerker - werving en selectie		+ +	+		+ +	+	NAW-gegevens, telefoonnummer, email (privé en zakelijk), geboortedatum, BSN, personeelsnummer (incl. contractnummer), geslacht, ID-kopie, burgerlijke staat, handtekening, IBAN, persoonsgegevens partner (en kinderen), nationaliteit, soort arbeidscontract, inkomensgegevens, VOG, CV, opleidingen, diploma's en certificaten
Financiën	- Betalen van facturen, registreren van inkomsten en uitgaven t.b.v. financiële administratie. - Adviseren van de eigen organisatie		+ +	+ +		+		NAW-gegevens, telefoonnummer, email, IBAN-nummer, eventuele

[17] Voor de inzet van het CenA-team voor consultatie is toestemming van betrokkenen nodig. Zonder toestemming kunnen de huisartsen en het CenA-team (en de CenA-teamleden onderling) geen gegevens uitwisselen. Nog uitgezocht wordt hoe het zit met andere taken van CenA-team, zoals doorbraaktafel en verlengingen en beoordelen medische geschiktheid om onderwijs te volgen.

[18] Zie bijlage 5 Regeling Bescherming persoonsgegevens voor meer informatie over de verwerkingen van HR.

	- Borgen en toetsen getrouwe en rechtmatige uitvoering van de processen.								persoonsgegevens verwerkt in toelichting factuur, functie, salaris, (soms) gezondheidsgegevens.
I&A	Ervoor zorgen dat alle medewerkers hun werkzaamheden goed kunnen uitvoeren in een prettige werkomgeving met gebruikmaking van stabiele ICT-voorzieningen.			+ +			+ +		Alle verwerkte persoonsgegevens in de organisatie (archief) NAW-gegevens en telefoonnummer (ICT)
Gebouwen beheer	Cameravastlegging in hoofdgebouw en parkeergarage voor beveiligingsdoeleinden en om auto's van medewerkers toegang te verschaffen tot parkeergarage						+ +		Camerabeelden, kentekens

6. Risico's

6.1 Risico's voor betrokkenen

Een belangrijk doel van de AVG is de persoonsgegevens van mensen zo goed mogelijk te beschermen. Daarvoor moeten risico's zo veel mogelijk worden beperkt of uitgesloten.
De risico's van schending van de privacy voor betrokkenen variëren van ongemak, stigmatisering en uitsluiting tot identiteitsfraude of chantage.
Binnen bepaalde organisatieonderdelen worden bijzondere persoonsgegevens, zoals medische gegevens of strafrechtelijke gegevens verwerkt waardoor deze risico's hoger zijn. Aan de verwerking van deze persoonsgegevens zijn strenge voorwaarden gesteld (artikel 9 en 10 AVG), omdat er sprake is van (zeer) gevoelige informatie over personen.
Om de risico's te beperken moeten maatregelen worden getroffen. Deze maatregelen zijn beschreven in hoofdstuk 7 van dit privacybeleid. Leidend daarbij is dat privacyeisen zoveel mogelijk worden geïntegreerd in regulier en/of al bestaand beleid en vertaald naar processtappen die worden geïntegreerd in het reguliere werkproces.

6.2 Risico's voor de Regio

Wanneer schending van de privacywet- en regelgeving plaatsvindt, is de Regio wettelijk aansprakelijk. Het verwijtbaar onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving kan leiden tot:
- het betalen van schadevergoeding;
- reputatieschade en herstelkosten. Deze kunnen fors zijn en leiden tot verlies van vertrouwen in de overheid;
- onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding van de AVG kan de Autoriteit Persoonsgegevens als landelijk toezichthouder, een forse boete opleggen.

7. Maatregelen

Persoonsgegevens worden op behoorlijke en zorgvuldige wijze verwerkt. Dit gebeurt in overeenstemming met de in de AVG voorgeschreven doelbinding en proportionaliteit. Dit houdt in dat persoonsgegevens alleen voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen mogen worden verzameld, dat er niet meer persoonsgegevens worden verwerkt dan voor het doel nodig is en dat er waar mogelijk minder of geen persoonsgegevens worden verwerkt. De Regio moet aantonen dat ze voldoet aan de AVG en kan dat doen aan de hand van onderstaande maatregelen.

7.1 Functionaris Gegevensbescherming (FG)

De Regio heeft een FG aangesteld. De FG moet worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De taken van de FG zijn informeren, adviseren over concernbrede privacyissues, toezicht houden, bewustwording creëren, en optreden als contactpersoon van de AP. Verder houdt de FG samen met de aandachtsfunctionarissen privacy het register van gegevensverwerkingen bij. De FG neemt níet de taken op het gebied van bescherming van de privacy van de RVE's over. De RVE's hebben hun eigen verantwoordelijkheid in het goed omgaan met privacygevoelige gegevens. De FG is verantwoordelijk voor het structureel toetsen van de implementatie en de uitvoering van de wettelijke eisen en het privacybeleid van de Regio. Betrokkenen kunnen volgens de AVG contact opnemen met de FG (via fg@regiogv.nl) met vragen over de verwerking van hun persoonsgegevens. Voor het inroepen van rechten van betrokkenen is de FG bij de Regio niet de primaire ingang. Hiervoor dient de mailbox avgverzoeken@regiogv.nl, waarna de verzoeken door de juridisch adviseurs worden behandeld.
De FG heeft voldoende middelen nodig om zijn taak te kunnen uitvoeren. Hij moet toegang hebben tot de persoonsgegevens en de verwerkingen van de gegevens in de organisatie. Deze bevoegdheden zijn gelijkwaardig aan de bevoegdheden van een toezichthouder zoals geregeld in titel 5.2 van de Algemene wet bestuursrecht (Awb).

Zie bijlage 5 voor het besluit Aanwijzing (plaatsvervangend) Functionaris Gegevensbescherming en daarbij behorende bevoegdheden conform AVG.

7.1.1 Toezicht

Het toezicht op de goede omgang met persoonsgegevens binnen de Regio wordt op de volgende manieren uitgevoerd:
- Proactief toezicht via de aandachtsfunctionarissen en RVE-managers. Hierbij wordt de RVE proactief doorgelicht op actuele privacyonderwerpen;
- Reactief toezicht na datalekken;
- Ad hoc toezichtsactiviteiten o.b.v. signalen uit de organisatie;
- Toezicht op uitvoeren van privacyprocessen. Het betreft processen m.b.t. o.a. honoreren van rechten van betrokkenen, uitvoeren van maatregelen n.a.v. datalekken, uitvoeren van DPIA's en afsluiten verwerkersovereenkomsten;
- Toezicht door verplichte audits (zoals de jaarlijks uit te voeren audit voor de Wpg).

7.2 Beveiliging

7.2.1 Algemeen

De Regio heeft het Strategisch Informatiebeveiligingsbeleid Regio Gooi en Vechtstreek van 2019 tot en met 2022 (zie bijlage 5) vastgesteld. Informatiebeveiliging en het veilig en verantwoord werken met persoonsgegevens overlappen elkaar voor een groot deel. Voor het borgen van de bescherming van persoonsgegevens is het naleven van wat is geregeld in het Informatiebeveiligingsbeleid dan ook van cruciaal belang.
De Regio zorgt voor passende beveiligingsmaatregelen ten aanzien van persoonsgegevens. Dit moet voorkomen dat de persoonsgegevens kunnen worden ingezien of gewijzigd door iemand die daar geen recht toe heeft. De bescherming beperkt zich niet tot een fysieke beveiliging van gegevens, maar gaat ook over logische (technische) toegangsbeveiliging.[19]

Medewerkers maken voor het werken met software altijd gebruik van de officiële licenties van de Regio. Bij officiële licenties is de veiligheid van informatie beter geborgd. Gebruik van persoonlijke (gratis) licenties is dus niet toegestaan.

De Regio bevordert het gebruik van Zivver om vertrouwelijke informatie veilig te versturen naar ontvangers buiten de organisatie. Bij gebruik van Zivver wordt gegarandeerd dat deze gevoelige informatie met de modernste beveiliging wordt verstuurd en dat niemand anders dan de beoogde ontvanger de inhoud van de e-mail kan lezen

7.2.2 RVE-specifiek

Er wordt bij een aantal applicaties van de medische RVE's (GGD, J&G, RAV, Sturing/CenA Team) waarin persoonsgegevens in een medisch dossier worden verwerkt, gewerkt met logging van de verwerkingen. Ook in de primaire applicatie van Veilig Thuis (Regipro) vindt logging plaats.[redacted]

Bij het Klantportaal Jeugd en Gezin wordt gebruik gemaakt van DigiD via tussenpartij Pazio. Pazio verzorgt de jaarlijkse DigiD-audit.

7.3 Transparantie en informatieplicht (privacyverklaring)

De Regio is transparant over de manier waarop zij met persoonsgegevens omgaat. De Regio praat niet over de betrokkenen, maar met de betrokkenen.
De Regio informeert de betrokkene over betreffende verwerking van persoonsgegevens met informatie over haar contactgegevens, het doel en de grondslag, eventuele ontvangers buiten de Regio-organisatie en informatie die betrokkene nodig heeft om zijn/haar rechten uit te oefenen (zoals de toepasselijke bewaartermijn en het feit dat men een verzoek om inzage of verwijdering kan indienen bij de Regio en een klacht bij de Autoriteit Persoonsgegevens). De RVE's zijn verantwoordelijk voor de goede invulling van de informatieplicht. Een goede manier om betrokkenen te informeren is via een specifieke privacyverklaring op de websites van de eigen RVE.
Wanneer betrokkenen zelf persoonsgegevens aan de Regio geven, worden zij op dat moment op de hoogte gesteld van de hiervoor genoemde informatie. Dit kan bijvoorbeeld via een formulier gebeuren

[19] Het strafrechtelijke werk van de BOA's valt onder de Wet politiegegevens, welke wet aanvullende regels voor beveiliging kent, zie hiervoor Bijlage 1 Afwijkingen privacybeleid voor zover Wet politiegegevens van toepassing is.

of door verwijzing naar de privacyverklaring op de website. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de Regio persoonsgegevens van hem/haar verzamelt en verwerkt en weet waarom en voor welk doel dat gebeurt.
Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd met de hiervoor bedoelde informatie (en daarnaast informatie over de categorieën persoonsgegevens en herkomst van de gegevens) binnen één maand na verkrijging door de Regio.
Als er verwerkingen van persoonsgegevens op een website (bijvoorbeeld via een webformulier) onder verantwoordelijkheid van de Regio plaatsvinden, is een privacyverklaring met informatie over deze verwerkingen verplicht. Als een website gebruik maakt van meer cookies dan enkel functionele cookies is bovendien een cookieverklaring vereist.
Zie bijlage 3 Verwijzingen naar de verschillende privacyverklaringen op de websites van de Regio voor de privacyverklaringen die de Regio nu al heeft. Op een later moment is het plaatsen van specifiekere privacyverklaringen voor alle Regiowebsites voorzien.

7.4 Bewustmaking en training

Op intranet wordt regelmatig stilgestaan bij privacy en informatiebeveiliging met onderwerpen als veilig (thuis)werken en omgaan met datalekken. Ook wordt in lunchsessies en op maat gemaakte trainingen aandacht besteed aan privacy.
Alle medewerkers worden getraind op het gebied van privacy om ervoor te zorgen dat de bescherming van persoonsgegevens verzekerd kan worden. Hiervoor is door het CMT vastgesteld dat digitale weerbaarheid (op het gebied van privacy en informatiebeveiliging algemeen) een vereiste competentie is van alle medewerkers. Er vindt periodiek een toetsing (e-learning) plaats op de digitale weerbaarheid van de medewerkers. Er wordt ook aandacht besteed aan de basisvaardigheden van medewerkers ten aanzien van informatieveiligheid.

Zie bijlage 5 voor het Voorstel uitrol e-learning privacy.

7.5 Gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen

De Regio zorgt ervoor dat bij het ontwerpen van nieuw beleid, het inrichten van nieuwe processen en aanschaffen van ICT-oplossingen de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen het uitgangspunt zijn en dat duidelijk is wat deze principes inhouden. Gegevensbescherming door ontwerp houdt o.a. in het uit kunnen oefenen van rechten van betrokkenen en niet meer gegevens uitvragen dan nodig. Gegevensbescherming door standaardinstellingen betekent dat standaard de meest privacyvriendelijke instellingen worden gehanteerd. In een volgende versie van het privacybeleid worden deze principes nader ingevuld.

7.6 Gegevensbeschermingseffectbeoordeling (DPIA)

Met een gegevensbeschermingseffectbeoordeling (DPIA) worden de effecten en risico's van nieuwe of bestaande verwerkingen beoordeeld op de bescherming van de privacy. Met een DPIA worden systematisch verwerkingen van persoonsgegevens, doeleinden, risico's en (voorgenomen) maatregelen beschreven om zo de impact van de verwerking op de bescherming van persoonsgegevens in kaart te brengen.
De Regio voert een DPIA uit wanneer er een hoog risico is voor rechten en vrijheden van betrokkenen. Een DPIA wordt o.a. uitgevoerd voor een grootschalige verwerking van bijzondere persoonsgegevens.

Dit geldt in het bijzonder bij verwerkingen waarbij nieuwe technologieën worden gebruikt. De Autoriteit Persoonsgegevens heeft een lijst gepubliceerd met verwerkingen waarvoor een DPIA sowieso verplicht is. De verwerkingen van de Regio worden hierop gecheckt.

7.7 Register van gegevensverwerkingen

De Regio is verantwoordelijk voor het aanleggen van een register van alle verwerkingen waarvan de Regio de verwerkingsverantwoordelijke is. Dit register geldt als één van de belangrijkste verantwoordingsinstrumenten voor een goede omgang met persoonsgegevens. Het is dan ook van belang dat wijzigingen in verwerkingen snel worden verwerkt in het register.
Het register bevat per verwerking een beschrijving van wat er precies gebeurt en welke gegevens daarvoor worden gebruikt, namelijk:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van het soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- De termijnen waarbinnen de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

De Regio zal persoonsgegevens in principe niet verwerken voor andere doeleinden dan in het register van gegevensverwerkingen worden genoemd. Als doelen wijzigen of als er nieuwe doelen bijkomen, is het van belang dat de RVE dit (via de aandachtfunctionaris privacy) signaleert en aangeeft bij de FG. Op een later moment is de ondersteuning door een systeem voor dit proces voorzien.
De inventarisatie en actualisatie van het register van gegevensverwerkingen vindt doorlopend plaats. Separaat wordt aan het Dagelijks Bestuur bij het voorstel tot vaststelling van dit beleid een momentopname gestuurd van het register. Voor een actuele versie zie bijlage 2 Register van gegevensverwerkingen.

7.8 Gegevens uitwisselen met derde partijen

De Regio werkt veel samen met andere partijen waarbij gegevens worden uitgewisseld. De Regio deelt persoonsgegevens met deze derde partijen als dit nodig is voor het uitvoeren van een publieke taak, om te voldoen aan een wettelijke verplichting of met nadrukkelijke, vooraf verleende toestemming van de betrokkene.[20] Daarnaast schakelt de Regio partijen in om voor de Regio diensten te leveren of werkzaamheden uit te voeren waarbij persoonsgegevens worden verwerkt (zoals het leveren van een cloud/SaaS-applicatie). Voor meer informatie over ontvangers van persoonsgegevens per verwerking, zie bijlage 2 Register van gegevensverwerkingen. De Regio verkoopt persoonsgegevens nooit aan derden.
Als het nodig is maakt de Regio met derde partijen afspraken die moeten zorgen voor een veilige en vertrouwelijke behandeling van de uitbestede verwerking van persoonsgegevens (o.a. door geheimhouding).

Op het moment dat de Regio met een andere partij persoonsgegevens gaat uitwisselen, is de AVG-rol die de uitwisselende partijen in de praktijk vervullen van belang om de rechten, plichten en risico's te kunnen bepalen. De AVG kent de rollen van verwerkingsverantwoordelijke, gezamenlijk verwerkingsverantwoordelijke (dus samen met andere partij(en)) en verwerker.

[20] Het strafrechtelijke werk van de BOA's valt onder de Wet politiegegevens, welke wet haar eigen regels over delen van gegevens kent, zie hiervoor Bijlage 1 Afwijkingen privacybeleid voor zover Wet politiegegevens van toepassing is.

De verwerkingsverantwoordelijke is degene die het doel en de middelen van een verwerking bepaalt. Dit kunnen dus ook meerdere partijen zijn. De verwerkingsverantwoordelijke bepaalt waaróm persoonsgegevens worden verzameld en hóe dat gebeurt.
Een verwerker is een partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, waarbij verwerking van persoonsgegevens de primaire opdracht is. De Regio blijft altijd verantwoordelijk voor verwerkingen van persoonsgegevens die door een verwerker plaatsvinden.

7.8.1 Samenwerken

De Regio is zelf in de meeste samenwerkingen zelfstandig verwerkingsverantwoordelijke. De partij waarmee wordt uitgewisseld is vaak ook zelfstandig verwerkingsverantwoordelijke. Dit is vooral het geval als wordt uitgewisseld met ketenpartners binnen en buiten de Regio-organisatie die hun eigen wettelijke taak uitvoeren (zoals Veilig Thuis, gemeenten, UWV, DUO, Belastingdienst en Raad voor de Kinderbescherming). Ook zorgaanbieders zijn altijd zelfstandig verwerkingsverantwoordelijken.
Soms is de Regio samen met andere partij(en) gezamenlijk verwerkingsverantwoordelijke (voor dezelfde verwerking). Dit is bijvoorbeeld het geval bij een website die door enkele GGD'en is bedacht en waarop via webformulieren persoonsgegevens worden verwerkt.

7.8.2 Inschakelen derde partijen

De Regio kan besluiten partijen in te schakelen om voor de Regio diensten te leveren of werkzaamheden uit te voeren waarbij persoonsgegevens worden verwerkt. Als de door de Regio ingeschakelde derde partij zelf kan bepalen hoe zij werkzaamheden of dienstverlening uitvoert en welke gegevens worden gebruikt, is zij zelf verwerkingsverantwoordelijke (denk hierbij aan de bloemist die wordt ingeschakeld om een collega een bosje bloemen te sturen).
Als de ingeschakelde partij ten behoeve en in opdracht van de Regio persoonsgegevens verwerkt en niet zelf mag bepalen hoe de diensten worden geleverd of werkzaamheden worden uitgevoerd is deze partij een verwerker. De gegevensverwerking wordt dan door de Regio gedicteerd en daarmee is gegevensverwerking de primaire opdracht (denk hierbij aan het bedrijf dat de salarisadministratie uitvoert of de leverancier van de Saas-applicatie die de ingevoerde persoonsgegevens direct wegschrijft).
De Regio deelt geen informatie die de ingeschakelde partijen niet nodig hebben en zij mogen deze informatie niet voor andere doeleinden gebruiken. De Regio legt afspraken over het zorgvuldig en veilig omgaan met informatie indien nodig vast in een verwerkersovereenkomst of geheimhoudingsovereenkomst.[21]

7.8.3 Afspraken tussen verwerkingsverantwoordelijken

Tussen twee zelfstandig verwerkingsverantwoordelijken hoeven vanuit de AVG niet per se afspraken gemaakt te worden. In de praktijk gebeurt dit wel vaak (met convenanten, protocollen of samenwerkingsovereenkomsten) en is het ook wel verstandig.
Twee of meer gezamenlijk verwerkingsverantwoordelijken moeten vanuit de AVG wel afspraken (in de zogenaamde 'onderlinge regeling') maken. Deze partijen spelen gezamenlijk een rol in dezelfde verwerking en om te zorgen dat de betrokkene weet wie zijn/haar gegevens verwerkt, zijn afspraken vereist.

[21] Een geheimhoudingsovereenkomst wordt voornamelijk gesloten met leveranciers die support leveren op software die bij de Regio draait.

7.8.4 Verwerkersovereenkomsten

RVE's zijn verantwoordelijk voor het afsluiten van verwerkersovereenkomsten met partijen die diensten aan hen leveren en die aan te merken zijn als verwerker. Het sjabloon voor de verwerkersovereenkomst is te vinden bij de Word-sjablonen van Inkoop-Contractbeheer.
De verwerkersovereenkomst bevat veel standaardafspraken om goed om te gaan met persoonsgegevens (o.a. over spelregels voor de verwerkers zoals geheimhouding en hoe om te gaan met een datalek). Deze standaardafspraken hoeven niet te worden aangepast. Er moeten wel enkele zaken voor de betreffende uitbestede verwerking op maat worden gemaakt. Het gaat dan o.a. om verwijzing naar de hoofdovereenkomst, details over de uitbestede verwerking(en) zoals verwerkingsdoeleinden en te verwerken persoonsgegevens, locatie van verwerkingen (binnen de Europese Economische Ruimte (EER)), ingeschakelde subverwerkers, toepasselijke normenkader voor informatiebeveiliging en de manier waarop getoetst kan worden in hoeverre verwerker aan dat normenkader voldoet.

7.9 Afhandelen van datalekken

Er is sprake van een datalek bij toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is. Vast staat dat datalekken zullen blijven plaatsvinden. Een mail naar de verkeerde persoon sturen, stukken in de verkeerde envelop of een hack door een externe zijn bijvoorbeeld niet 100% uit te sluiten. Het is niet erg als je een datalek constateert of veroorzaakt. Het is een kans voor de organisatie om ervan te leren. Vrijwel elk opgemerkt datalek leidt tot verbetering van procedures of verhoging van het privacybewustzijn.
Daarom worden managers en medewerkers gevraagd mogelijke datalekken zo spoedig mogelijk te melden via het meldingformulier op het intranet. De Regio doet haar best de schending van de privacy zo snel mogelijk op te lossen of de negatieve gevolgen daarvan zo veel mogelijk te beperken. Van de datalekken met een risico voor rechten en vrijheden van betrokkenen wordt binnen 72 uur na ontdekking een melding gemaakt bij de AP/toezichthouder. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor betrokkenen. In dat geval meldt de Regio het datalek ook aan de betrokkenen in eenvoudige en duidelijke taal. Van alle datalekmeldingen wordt een registratie bijgehouden. In deze registratie wordt o.a. aangegeven of een melding een datalek of enkel een incident blijkt te zijn. Om toekomstige datalekken te voorkomen worden de voorgevallen datalekken (samen met de procedure zelf) jaarlijks geëvalueerd.

Zie bijlage 5 voor de Interne procedure afhandeling meldingen datalekken AVG en de Handreiking beoordeling datalekken AVG.

7.10 Bewaren van persoonsgegevens

Uitgangspunt van de AVG is dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze zijn verwerkt.[22] De bewaartermijnen van persoonsgegevens lopen hierdoor uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Deze komen ook terug in de vastgestelde selectielijsten die voortvloeien uit de Archiefwet, welke aangeven hoe lang informatie bewaard moet worden. Zie hiervoor bijlage 5 Goed Geordend Overzicht van Informatie (GGO) Regio Gooi en Vechtstreek 2020 waarin de selectielijst is opgenomen.

[22] Het strafrechtelijke werk van de BOA's valt onder de Wet politiegegevens, welke wet haar eigen bewaartermijnen kent, zie hiervoor Bijlage 1 Afwijkingen privacybeleid voor zover Wet politiegegevens van toepassing is.

Het doel van de Archiefwet is het bewaren van belangrijke informatie. De AVG is gericht op bescherming van persoonsgegevens. Hierbij is dataminimalisatie een belangrijk uitgangspunt. Dit houdt in dat alleen díe persoonsgegevens mogen worden verwerkt die echt noodzakelijk zijn. De Archiefwet en de AVG hebben dus verschillende uitgangspunten. Hierdoor moet in de praktijk soms het belang van archivering worden afgewogen tegen het belang van bescherming van persoonsgegevens.

7.11 Omgaan met onderzoeken van de Autoriteit Persoonsgegevens

Indien de Autoriteit Persoonsgegevens bij de Regio een onderzoek komt doen vanwege vermeende inbreuken op de AVG verleent de Regio alle medewerking aan het onderzoek. De Regio is hiertoe ook verplicht. De Autoriteit Persoonsgegevens heeft vergaande bevoegdheden zoals genoemd in artikel 58 AVG. De Regio kan gevraagd worden alle informatie die voor het onderzoek van belang is te verstrekken. De toezichthouder heeft ook toegang tot bijzondere persoonsgegevens (waaronder medisch dossiers) als dat nodig is voor uitvoering van de taken van de Autoriteit Persoonsgegevens. Een onderzoek kan leiden tot het opleggen van een boete of dwangsom.

8. Rechten van de betrokkenen en klachten

8.1 Algemeen

De AVG is voor een heel groot deel gericht op het verbeteren van de privacyrechten van de betrokkenen. Dit betekent dat er meer aandacht is voor de rechten van betrokkenen en dat een procedure daarvoor van groot belang is. Daarom worden de rechten van betrokkenen en hoe de Regio verzoeken op grond van deze rechten behandelt, hierna beschreven.

8.2 Welke rechten hebben betrokkenen?

Betrokkenen hebben de volgende rechten t.a.v. hun persoonsgegevens[23]:

- Ontvangen van een afschrift (inzage) van de persoonsgegevens;
- Wijzigen (rectificatie of aanvulling) van de persoonsgegevens;
- Verwijderen van de persoonsgegevens;
- Beperken van de verwerking (tijdelijke stopzetting van verwerking) van de persoonsgegevens;
- Overdraagbaarheid van de persoonsgegevens;
- Bezwaar maken tegen de verwerking van persoonsgegevens;
- Intrekken van toestemming, als dit de grondslag van de verwerking van persoonsgegevens is geweest.

Recht op inzage van gegevens (artikel 15 AVG)

De betrokkene heeft het recht om van de Regio uitsluitsel te krijgen of zijn/haar persoonsgegevens worden verwerkt en, wanneer dat het geval is, om inzage te verkrijgen van die persoonsgegevens. Dit recht heeft als doel dat betrokkene zich van de verwerking op de hoogte kan stellen en de rechtmatigheid daarvan kan controleren.
Het recht van inzage is mede bedoeld als opstapje om uitoefening van de andere rechten van betrokkenen (wijziging, verwijdering of beperking) mogelijk te maken.

[23] Het strafrechtelijke werk van de BOA's valt onder de Wet politiegegevens, welke wet haar eigen rechten van betrokkenen kent, zie hiervoor Bijlage 1 Afwijkingen privacybeleid voor zover Wet politiegegevens van toepassing is.

Recht op rectificatie van gegevens (artikel 16 AVG)

De betrokkene heeft het recht om van de Regio een rectificatie van zijn/haar persoonsgegevens te verkrijgen als deze onjuist zijn. Betrokkene heeft ook het recht vervollediging van onvolledige persoonsgegevens te verkrijgen door bijvoorbeeld een aanvullende verklaring te verstrekken.

Recht op verwijdering (artikel 17 AVG)

De betrokkene heeft het recht van de Regio verwijdering van zijn/haar persoonsgegevens te verkrijgen.

Recht op beperking van de verwerking (artikel 18 AVG)

De betrokkene heeft het recht van de Regio beperking van de verwerking te verkrijgen. Dit betekent dat men een tijdelijk slot op de verwerking van persoonsgegevens wil totdat een bezwaar of een probleem is opgelost.

Recht op overdraagbaarheid gegevens, dataportabiliteit (art. 20 AVG)

De betrokkene heeft het recht de hem/haar betreffende persoonsgegevens, die hij/zij aan de Regio heeft verstrekt, in een gestructureerde, gangbare en machinaal leesbare vorm te verkrijgen en heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt.

Recht om bezwaar te maken tegen de verwerking van persoonsgegevens (art. 21 AVG)

De specifieke omstandigheden van een persoon kunnen maken dat een betrokkene bezwaar maakt tegen een verwerking die wordt gedaan voor een taak i.h.k.v. de uitoefening van het openbaar gezag. De Regio moet dan stoppen met de verwerking tenzij zij gronden aanvoert die zwaarder wegen dan de belangen van betrokkene.

8.3 Ingeroepen rechten bij de Regio

Het recht van inzage en het recht van verwijdering worden bij de Regio het vaakst ingeroepen. Overigens is het zo dat enkele rechten niet van toepassing zijn wanneer verwerking van de betreffende persoonsgegevens op bepaalde grondslagen is gebaseerd. Voor de Regio het meest relevant is dat het recht op verwijdering niet kan worden gehonoreerd als de gegevens nog noodzakelijk zijn voor het voldoen aan een wettelijke verwerkingsverplichting of voor het vervullen van een taak van algemeen belang of uitoefenen van het openbaar gezag.

8.4 Hoe oefenen betrokkenen hun rechten uit?

Betrokkenen kunnen een verzoek i.h.k.v. de rechten van betrokkenen sturen naar het Dagelijks Bestuur, via avgverzoeken@regiogv.nl. Ook is het mogelijk een brief te sturen naar Regio Gooi en Vechtstreek, Postbus 251, 1400 AG Bussum onder vermelding van 'Verzoek omtrent persoonsgegevens'. Het is daarbij belangrijk dat betrokkenen desgevraagd kunnen aantonen dat de gegevens waarop het verzoek betrekking heeft daadwerkelijk hun gegevens zijn.
Bepaalde RVE's hebben te maken met materiewetgeving die v.w.b. rechten van betrokkenen verder kan strekken dan de AVG. De afhandeling kan dan verschillen. Zo heeft Veilig Thuis op haar website

een formulier om de rechten van betrokkenen bij Veilig Thuis uit te oefenen (zie https://www.veiligthuisgv.nl/over-ons/privacy-en-rechten/uw-rechten-rond-de-informatie-over-u/)

Betrokkenen kunnen bezwaar aantekenen tegen het besluit op een verzoek door een brief te sturen aan het Dagelijks Bestuur van de Regio, Postbus 251, 1400 AG Bussum. Daarin geeft men aan waarmee men het niet eens is. Betrokkenen ontvangen zo spoedig mogelijk een beslissing op hun bezwaar, maar uiterlijk binnen 6 weken (met een mogelijkheid voor de Regio om de beslistermijn met 6 weken te verlengen). Tegen een beslissing op het bewaar staat beroep open bij de rechtbank.

8.5 Toepasselijk wettelijk kader

Het wettelijk kader waarop men zich beroept (of hoe het verzoek moet worden geïnterpreteerd), is bepalend voor hoe je een verzoek om inzage, rectificatie of verwijdering moet behandelen en ook in welke vorm de beslissing gegoten wordt. Is het een algemeen verzoek of wordt de AVG genoemd dan is de AVG van toepassing. Wordt gevraagd om inzage of verwijdering van een medisch, jeugd- of VT-dossier dan is respectievelijk de Wgbo, Jeugdwet of Wmo 2015 het wettelijk kader.
Bij een verzoek om inzage betekent dit, dat een afschrift van de persoonsgegevens (bij AVG als wettelijk kader) of het document/dossier zelf (bij Wgbo, Jeugdwet of Wmo 2015 als wettelijk kader) moet worden verstrekt.
Als de AVG het wettelijk kader is, moet de beslissing een besluit zijn in de zin van de Awb. Indien de grondslag van het verzoek Wgbo of Jeugdwet betreft, dan is de beslissing een civielrechtelijke handeling binnen de contractuele relatie en is geen sprake van een besluit in de zin van de Awb.

8.6 Afhandelen verzoeken

8.6.1 Controle identiteit

Na ontvangst van een verzoek tot uitoefening van bovenstaande rechten, stuurt de Regio een ontvangstbevestiging. Hierin wordt de betrokkene verzocht zich te identificeren. Voordat de Regio het verzoek namelijk in behandeling kan nemen, wordt de identiteit van de betrokkene altijd gecontroleerd. De betrokkene kan hiervoor een afspraak maken met één van de juridisch adviseurs.
Als verzoeken niet centraal via avgverzoeken@regiogv.nl maar bij een RVE zelf binnenkomen en de verzoeker is een bekende persoon bij betreffende RVE hoeft de identiteit niet vooraf gecontroleerd te worden. Als verzoeken wel centraal bij de Regio binnenkomen, dan is wel identificatie vooraf vereist.

8.6.2 Behandeling van verzoek

Als het verzoek te weinig informatie bevat om het af te handelen (bijvoorbeeld alleen aan mailadres) kan om aanvulling gevraagd worden binnen een redelijke termijn. Ondertussen wordt dan de beslistermijn opgeschort. Als er dan geen aanvullingen komen, kan het verzoek buiten behandeling worden gelaten.
De Regio reageert zo snel mogelijk, maar uiterlijk binnen een maand op verzoeken en geeft dan uitsluitsel over het gevolg dat ze aan het verzoek verbindt. In bijzondere gevallen (complexiteit, grote aantallen verzoeken van eenzelfde verzoeker) kan deze termijn eenmalig verlengd worden met twee maanden. In dat geval wordt de betrokkene daarvan binnen een maand op de hoogte gesteld. Ook kan de Regio als het verzoek onduidelijk is of om veel gegevens gaat, de betrokkene verzoeken om zijn/haar verzoek te specificeren.
Wanneer betrokkenen bij één van de medische RVE's (GGD, J&G, RAV, Sturing/CenA Team) verzoeken om inzage in hun medisch dossier of medisch dossier van hun kinderen en zij zich in algemene termen beroepen op de AVG, kan de Regio een verificatievraag stellen of het betrokkene alleen om zijn/haar

persoonsgegevens te doen is, of om de inhoud van het volledige medisch dossier. In dat laatste geval kan de Regio het verzoek alsnog opvatten als een inzageverzoek op grond van de Wgbo. De Regio kan daarin zodoende ook enigszins sturend optreden.

8.6.3 Beslissing op verzoek

In de beslissing laat de Regio weten of en hoe aan het verzoek zal worden voldaan. In het geval de Regio niet – of gedeeltelijk – aan het verzoek voldoet, wordt dit altijd gemotiveerd in het besluit. Zo is het bijvoorbeeld niet toegestaan om gegevens van andere personen in te zien.

Zie bijlage 5 voor Werkproces inzageverzoeken en overige verzoeken ogv art. 15 t/m art. 18 AVG.

8.6.4 Uitvoering van verzoek

Het uitvoeren van het verzoek hoeft niet per se binnen de beslistermijn plaats te vinden. De daadwerkelijke verwijdering of de afspraak op kantoor om het resultaat van het inzageverzoek in ontvangst te nemen, moet echter wel zo spoedig mogelijk plaatsvinden. Vóór afgifte van het resultaat van het inzageverzoek moet (wederom) de identiteit van de betrokkene worden gecontroleerd.

8.7 Klachten

Indien de betrokkene van mening is dat de AVG, de UAVG of het privacybeleid niet wordt nageleefd, dient hij/zij zich te wenden tot de klachtenfunctionaris van de Regio via klachten@regiogv.nl.
Ook kan men een klacht indienen bij de Functionaris Gegevensbescherming (via fg@regiogv.nl).
Voor de afhandeling van klachten met een privacycomponent die bij de klachtenfunctionaris worden ingediend, wordt de FG zo nodig om advies gevraagd. Klachten die bij de FG binnenkomen, worden door de FG zelf afgedaan. Ook is er een mogelijkheid een klacht in te dienen bij de Autoriteit Persoonsgegevens.

9. Geautomatiseerde verwerkingen

9.1 Geautomatiseerde besluitvorming

Geautomatiseerde verwerkingen waarbij besluiten worden genomen over zaken die (aanzienlijke) gevolgen kunnen hebben voor personen, komen bij de Regio niet voor.

9.2 Onderzoek

De Regio wil haar taken goed uitvoeren. Om te weten wat beter kan, gebruikt de Regio informatie van inwoners voor onderzoek. De Regio zorgt ervoor dat onderzoeksresultaten niet te herleiden zijn tot individuele personen. Onderzoek vindt bijvoorbeeld plaats door data-analyse waarbij geen gebruik wordt gemaakt van het BSN.

9.3 Cameratoezicht

De Regio maakt gebruik van cameratoezicht in en rond haar gebouwen en in de parkeergarage onder het gebouw aan de Burgemeester de Bordesstraat. Ook zijn de vrachtwagens van de GAD uitgerust met één of meerdere camera's. Voor het cameratoezicht heeft de Regio een actuele risicoanalyse (DPIA) voor handen.

Zie bijlage 5 voor Regeling Cameratoezicht.

10. Overgangs- en slotbepalingen

10.1 Geldigheid privacybeleid

Onverminderd eventuele wettelijke bepalingen is dit beleid van kracht gedurende de hele looptijd van de verwerking van de persoonsgegevens.

10.2 Inwerkingtreding, evaluatie en wijziging

10.2.1 Inwerkingtreding

Dit beleid treedt in werking, na vaststelling door het bestuur, onder gelijktijdige intrekking van het voorafgaande Reglement Bescherming Persoonsgegevens (MyCorsa 11.0004190). In tegenstelling tot het huidige Reglement bescherming persoonsgegevens wordt dit privacybeleid niet gepubliceerd. Dat hoeft niet omdat het een intern stuk is.

10.2.2 Evaluatie

Er wordt door de Regio jaarlijks geëvalueerd of het privacybeleid nog volstaat. Hierbij wordt gekeken naar zaken als actualiteit, volledigheid, voldoende bekendheid bij alle medewerkers en of het beleid goed werkt. Hiertoe zullen de FG en de aandachtsfunctionarissen privacy steekproeven kunnen uitvoeren (zoals clean desk rondes). De evaluatie wordt uitgevoerd met de bevindingen van een doorlopende monitoring.
Deze monitoring vindt op drie manieren plaats:
- incident-gebaseerd (bijvoorbeeld n.a.v. een klacht van een betrokkene of een datalek),
- cyclisch volgens de PDCA-methode (aangezien regels, technologie en maatschappelijke opvattingen voortdurend aan verandering onderhevig zijn, zal ook steeds bekeken dienen te worden of het privacybeleid nog volstaat); en
- periodiek (privacytoets als beheermaatregel).

10.2.3 Wijziging

Wanneer de jaarlijkse evaluatie, gewijzigde wet- en regelgeving of veranderingen in de maatschappij hiertoe noodzaken, wordt het privacybeleid herzien. Het Dagelijks Bestuur wordt geïnformeerd over kleine wijzigingen. Bij grote aanpassingen wordt het privacybeleid opnieuw ter vaststelling aan het Dagelijks Bestuur voorgelegd. Dit privacybeleid kan zonder voorafgaande waarschuwing door de Regio worden gewijzigd. Wijzigingen treden in werking vanaf het moment dat ze op het intranet zijn geplaatst.

10.3. Slotartikel

Deze regeling kan aangehaald worden als het Privacybeleid Regio Gooi en Vechtstreek d.d. 8 juli 2021 met kenmerk 21.0004032

Vragen?
Bij vragen over dit beleid kan contact worden opgenomen via fg@regiogv.nl.

Bijlagen

Bijlage 1 Afwijkingen privacybeleid voor zover Wet politiegegevens van toepassing is

5.1.2 Grondslagen

Voor de BOA's die strafrechtelijk handhavend optreden, is de AVG niet van toepassing. Het kader voor het verwerken van persoonsgegeven bij het uitvoeren van deze werkzaamheden wordt gevormd door het Besluit politiegegevens buitengewoon opsporingsambtenaren in combinatie met de Wet politiegegevens en het Besluit politiegegevens. Kortweg wordt deze combinatie van regelgeving aangeduid met Wet politiegegevens (hierna: Wpg) omdat deze wet de meeste relevante bepalingen bevat. In het kader van de Wpg wordt gesproken van politiegegevens i.p.v. persoonsgegevens.

Op basis van de volgende grondslagen in de Wpg verwerkt de BOA voor het strafrechtelijke werk politiegegevens:
- Dagelijkse politietaak (art. 8): politiegegevens kunnen worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak. Bij de Regio betreft dit handhaving van wetten en regels, hulpverlening, surveillance en eenvoudige opsporingsonderzoeken.
- Uitgebreidere opsporingsonderzoeken en veelplegersdossiers (art. 9): politiegegevens kunnen gericht worden verwerkt voor onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval. Denk hierbij aan het verzamelen van gegevens over een bepaalde persoon of naar aanleiding van een specifieke gebeurtenis.

5.1.3 Verwerkte persoonsgegevens

Een BOA kan als dat nodig is meerdere soorten persoonsgegevens verzamelen, afhankelijk van het soort onderzoek en het doel, zoals:
- personalia (naam, voornaam, adres, geboortedatum)
- kenteken
- financiële gegevens
- bijzondere persoonsgegevens, zoals gezondheidsgegevens.

De informatiesystemen voor het strafrechtelijk BOA-werk van de Regio maken gebruik van basisregistraties van overheidsinstellingen met publiekrechtelijke taken, zoals:
- Basisregistratie Personen (BRP) van de Rijksdienst voor identiteitsgegevens (RvIG)
- Kentekenregister van de (Rijksdienst voor het Wegverkeer) RDW
- Basisregistraties Adressen en Gebouwen (BAG) van het Kadaster
- Handelsregister van de Kamer van Koophandel (KvK)
- Verzuimmeldingen en onderwijsregistratie in en uitschrijvingen van Dienst uitvoering Onderwijs.

Uit deze basisregistraties kan de Regio ook persoonsgegevens halen. Wanneer de Regio deze gegevens heeft verwerkt zijn het voor de Regio politiegegevens geworden.

Sommige persoonsgegevens worden verzameld op grond van het Wetboek van Strafvordering. Volgens het Wetboek van Strafvordering is de BOA verplicht om de identiteit van een verdachte vast te stellen. De Wet identiteitsvaststelling verdachten, veroordeelden en getuigen en het daarbij horende besluit geven aan welke gegevens daarvoor moeten worden gebruikt. Op grond hiervan worden verwerkt de naam, voornaam, geboorteplaats- en datum, het adres (zoals vermeld in de gemeentelijke

basisadministratie) en iemands feitelijke verblijfplaats. In speciale gevallen worden ook bijzondere categorieën persoonsgegevens verzameld.

Voor details van de verwerkte persoonsgegevens per verwerking, zie bijlage 2 Register van gegevensverwerkingen.

5.1.4 Betrokkenen

De Wpg verplicht om in de systemen een onderscheid te maken tussen de verschillende categorieën van betrokkenen die kunnen voorkomen. Dit zijn in ieder geval verdachten, slachtoffers, derden (zoals getuigen) en veroordeelden.

7.2 Beveiliging

Politiegegevens en andere persoonsgegevens (die onder de AVG vallen) moeten gescheiden worden opgeslagen. Bij RBL wordt op dit moment bekeken hoe dat ingeregeld kan worden.
Vanuit de Wpg is daarnaast het uitvoeren van een jaarlijkse interne audit en een 4-jaarlijkse externe privacy audit verplicht.

7.8 Delen met derden

Naast de BOA's is de Wpg ook van toepassing op de politie, Koninklijke Marechaussee en de rijksrecherche. Daarnaast is de Wpg van overeenkomstige toepassing op de verwerking van persoonsgegevens door de vier bijzondere opsporingsdiensten:
- De Fiscale Inlichtingen- en Opsporingsdienst (FIOD),
- De Inspectie Sociale Zaken enWerkgelegenheid, Directie Opsporing (ISZW-DO)
- De Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport (ILT/IOD)
- De Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Waren Autoriteit (NVWA-IOD)

Het motto voor de BOA's en die organisaties die aan de Wpg moeten voldoen is "delen tenzij". Dat betekent dat de BOA's in bepaalde gevallen verplicht zijn om politiegegevens beschikbaar te stellen aan die andere organisaties en andersom. Dit motto geldt niet voor instanties die niet aan de Wpg zijn gebonden.
De BOA mag gegevens uitsluitend verstrekken aan andere partijen als daar een wettelijke basis voor is. Denk hierbij aan het Openbaar Ministerie, Raad voor de Kinderbescherming of de gemeente. Gegevens mogen niet altijd voor een ander doel worden gebruikt dan waarvoor zij zijn verzameld.

Op basis van de volgende grondslagen in de Wpg en het Besluit politiegegevens verstrekt de BOA persoonsgegevens:

Verstrekking aan gezagsdragers (art. 16): Op basis van dit artikel moet de BOA politiegegevens verstrekken aan het Openbaar Ministerie en de korpschef voor disciplinaire onderzoeken.

Verstrekking aan inlichtingendiensten (art. 17): Politiegegevens worden verstrekt voor zover dit voortvloeit uit de Wet op de inlichtingen- en veiligheidsdiensten 2017.

Verstrekking aan derden structureel (art. 18): Als er structureel politiegegevens aan derden worden verstrekt, moet dat zijn vastgelegd in een Algemene maatregel van bestuur. Het Besluit politiegegevens is zo'n Algemene maatregel van bestuur. Daar staat in artikel 4:1-4:4 aan wie de

gegevens structureel kunnen worden verstrekt. Hiertoe behoort o.a. de verstrekking aan Halt-bureaus en de Raad voor de Kinderbescherming.

Verstrekking aan derden incidenteel (art. 19): Politiegegevens kunnen in bijzondere gevallen worden verstrekt aan personen of instanties. De gegevens moeten dan nodig zijn voor één van de volgende doelen:
- Het voorkomen en opsporen van strafbare feiten;
- Het handhaven van de openbare orde;
- Hulp verlenen aan hen die dat behoeven;
- Het uitoefenen van toezicht op het naleven van de regelgeving.

Verstrekking aan derden structureel voor samenwerkingsverbanden (art. 20): De Regio heeft met sommige partijen een samenwerkingsverband ten behoeve van de BOA's. Politiegegevens kunnen aan deze partijen worden verstrekt als daar een zwaarwegend algemeen belang voor is. Hierbij kan worden gedacht aan zowel publieke als private partijen, zoals gemeenten, woningbouwverenigingen, de belastingdienst, banken en scholen.

Verwerking voor wetenschappelijk onderzoek en statistiek (art. 22): Politiegegevens kunnen worden verwerkt voor beleidsinformatie, wetenschappelijk onderzoek of statistiek zolang de gebruikte resultaten geen persoonsgegevens bevatten. Het gaat dan om geanonimiseerde bestanden.

Rechtstreekse verstrekking (art. 23): Het verstrekken van politiegegevens aan het Openbaar Ministerie en de korpschef kan rechtstreeks gedaan worden. Dit betekent dat deze geautomatiseerd (via een systeem) kunnen worden verstrekt.

Rechtstreekse verstrekking aan inlichtingen- en veiligheidsdiensten (art. 24): De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) kunnen politiegegevens rechtstreeks geautomatiseerd vergelijken als dat noodzakelijk is voor de uitvoering van hun taak.

7.10 Bewaren van persoonsgegevens

De Wet politiegegevens maakt onderscheid tussen verwijderen en vernietigen van gegevens. Als gegevens worden verwijderd, zijn zij nog niet definitief weg. Ze komen als het ware achter een digitaal schot te staan en zijn niet meer in te zien. Alleen als mocht blijken dat de BOA's de gegevens nodig hebben voor een klachtenprocedure of omdat er verantwoording over moet worden afgelegd, dan kunnen ze worden opgevraagd.
Bij RBL is op dit moment de situatie dat nog alles zichtbaar blijft tot het moment dat de leerlingen archiefleerlingen zijn (leerlingen boven de 23).

Als er een groot opsporingsonderzoek moet worden verricht wat een grote impact heeft op de rechtsorde, dan mogen deze gegevens opnieuw verwerkt, en dus ook geraadpleegd, worden. Dit kan alleen als de officier van justitie daar opdracht voor geeft.
Vernietigen is een definitieve handeling. De gegevens zijn niet meer terug te halen

Doel verwerking	Verwerken	Verwijderen	Vernietigen
Dagelijkse politietaak (artikel 8)	Tot 5 jaar na de datum van eerste verwerking	Na 5 jaar	5 jaar na verwijdering
Recherche-onderzoeken (artikel 9)	Zolang het onderzoek loopt	Een half jaar na afloop van het onderzoek + max. een half jaar om te kijken of er aanleiding is voor een nieuw onderzoek	5 jaar na verwijdering

8.2 Welke rechten hebben betrokkenen?

- Recht op inzage (art. 25):
Betrokkenen mogen vragen of de Regio politiegegevens van hen verwerkt. Als die gegevens er zijn, kunnen ze worden ingezien. Er wordt dan informatie verstrekt over in ieder geval:

- Doelen en rechtsgrond van de verwerking;
- De betrokken categorieën van politiegegevens;
- De vraag of deze politiegegevens gedurende een periode van vier jaar voorafgaande aan het verzoek zijn verstrekt en informatie over de ontvangers of categorieën ontvangers. Met name ontvangers in derde landen of internationale organisaties;
- De voorziene periode van opslag. Of, als dat niet mogelijk is, de criteria voor het bepalen van de bewaartermijn;
- Het recht om te vragen om rectificatie, vernietiging of afscherming van de verwerking van politiegegevens;
- Het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens;
- De herkomst van de politiegegevens.

- Recht op rectificatie en vernietiging van politiegegevens (art. 28): betrokkenen hebben het recht onjuiste politiegegevens te rectificeren of, indien nodig, aan te vullen. Als politiegegevens feitelijk onjuist, onvolledig, niet nodig voor het doel of in strijd met een wettelijk voorschrift worden verwerkt, kan een verzoek worden ingediend om deze gegevens te verbeteren, aan te vullen, te verwijderen, af te schermen of te markeren.

- Het recht op overdraagbaarheid van gegevens, dataportabiliteit is een recht onder AVG en komt niet voor in de Wet politiegegevens.

De beslissing op zowel het verzoek uit artikel 25 als 28 Wpg is een besluit in de zin van de Algemene Wet Bestuursrecht. Betrokken kunnen hiertegen in beroep gaan. Ook kan men zich wenden tot de Autoriteit Persoonsgegevens en vragen om bemiddeling of advies. Tegelijkertijd kan beroep worden ingesteld.

Bijlage 2 Register van gegevensverwerkingen

In het Register van gegevensverwerkingen geeft de Regio informatie geeft over alle voorkomende verwerkingen binnen de organisatie. De inventarisatie en actualisatie van het register van gegevensverwerkingen vindt doorlopend plaats. Separaat wordt aan het Dagelijks Bestuur bij het voorstel tot vaststelling van dit beleid een momentopname gestuurd van het register. Voor een actuele versie zie MyCorsa 19.0014889.

Bijlage 3 Verwijzingen naar de verschillende privacyverklaringen op de websites van de Regio

Algemene privacyverklaring Regio
https://www.regiogv.nl/privacyverklaring/

Specifieke verklaringen op organisatieonderdelenwebsites:
https://www.gad.nl/privacyverklaring/
https://www.gad.nl/wp-content/uploads/sites/8/2018/08/Privacy-protocol-GAD.pdf
https://www.visitgooivecht.nl/nl/privacyverklaring
https://www.ggdgv.nl/contact/privacy/
Diverse verwijzingen op GGD-website (https://www.ggdgv.nl/mijn-gezondheid/infectieziekten/coronavirus/) naar GGD GHOR voor corona privacyverklaringen
https://www.ggdgv.nl/wp-content/uploads/sites/2/2020/09/5.-Privacyverklaring-GM-VO-2020-GV.pdf
https://www.veiligthuisgv.nl/over-ons/privacy-en-rechten/
https://www.ravflgv.nl/privacyverklaring/
https://www.jggv.nl/wp-content/uploads/sites/9/2019/10/privacy-en-digitaal-dossier-jeugd-en-gezin.pdf (folder)

Specifieke verklaringen op onderwerpwebsites:
https://www.blijfgezondgv.nl/privacyverklaring/
https://www.30dagengezonder.nl/privacybeleid/
https://www.vervoergv.nl/privacyverklaring/ (Vervoer Gooi en Vechtstreek heeft een eigen privacybeleid maar de verklaring is hier voor de volledigheid opgenomen)

Verklaringen op onderwerpwebsites die verwijzen naar de algemene privacyverklaring:
https://www.hierfixjenix.nl/privacyverklaring/
https://www.verwijsindexgv.nl/privacyverklaring/
https://www.pleegoudergv.nl/privacyverklaring/
https://www.herstelnetwerk.nl

Bijlage 4 Beschrijvingen/verantwoordingen van verwerkingen die de Regio uitvoert maar waarvoor de grondslag niet volkomen duidelijk is

In deze verantwoordingen wordt ingegaan op de grondslagen om de verwerkingen uit te voeren en welke passende maatregelen daarbij zijn getroffen.

- Onderbouwing bepaalde verwerkingen RBL
- Onderbouwing verwerkingen HMD
- Onderbouwing verwerkingen CenA Team
- Onderbouwing verwerkingen tegengaan mensenhandel
- Onderbouwing verwerkingen peutermonitor
- Onderbouwing verwerkingen Veilig Verder

PM De inhoud van deze bijlage wordt in een volgende versie van het privacybeleid toegevoegd.

Bijlage 5 Verwijzingen naar al vastgestelde stukken in MyCorsa

- Gedragscode integriteit, na Wnra (MyCorsa 19.0015780)
- Rollen, taken en verantwoordelijkheden privacy (MyCorsa 19.0011739)
- Strategisch Informatiebeveiligingsbeleid Regio Gooi en Vechtstreek van 2019 tot en met 2022 (MyCorsa 19.0013516)
- Aanwijzing Functionaris Gegevensbescherming en daarbij behorende bevoegdheden conform AVG (MyCorsa 18.0004540)
- Aanwijzing plaatsvervangend Functionaris Gegevensbescherming en daarbij behorende bevoegdheden conform AVG (MyCorsa 19.0010461)
- Voorstel uitrol e-learning privacy (MyCorsa 21.0000089)
- Werkproces inzageverzoeken en overige verzoeken ogv art. 15 t/m art. 18 AVG (MyCorsa 19.0011233)
- Stroomdiagram werkproces voor verzoeken op grond van de AVG. Inzage- en vernietigingsverzoeken (MyCorsa 19.0011234)
- Interne procedure afhandeling meldingen datalekken AVG (MyCorsa 19.0013519)
- Handreiking beoordeling datalekken AVG (MyCorsa 19.0013574)
- Goed Geordend Overzicht van Informatie (GGO) Regio Gooi en Vechtstreek 2020 (MyCorsa 20.0002778)
- Regeling Cameratoezicht (MyCorsa 19.0000296)
- Regeling Bescherming persoonsgegevens (document van HR, MyCorsa 19.0015785)

Regio Gooi en Vechtstreek

MEMO

Interne procedure afhandeling meldingen datalekken AVG

Algemeen	
Aan	CMT
Van	[redacted]
Datum	21 oktober 2019
Verspreiden	Nee
Kenmerk	19.0013519

Inleiding

Sinds 1 januari 2016 is er met de Wet meldplicht datalekken een verplichting voor organisaties om datalekken zorgvuldig af te handelen. Met de inwerkingtreding van de Algemene Verordening Gegevensbescherming (AVG) is het afhandelen van datalekken ook een Europese verplichting geworden. Deze plicht om datalekken goed af te handelen betekent voor de Regio onder meer dat zij als verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens bij informatieveiligheidsincidenten met persoonsgegevens moet beoordelen of er sprake is van een datalek.
Als vast is gesteld dat inderdaad sprake is van een datalek (in de AVG inbreuk in verband met persoonsgegevens geheten) moet vervolgens mogelijk worden gemeld aan de Autoriteit Persoonsgegevens (AP) en de gedupeerde (in de AVG betrokkene). Ook bestaat er een verplichting alle datalekken vast te leggen in een datalekkenregister. Het register geeft inzicht in het aantal en de soorten datalekken dat heeft plaatsgevonden binnen de organisatie en dient ook als controlemiddel voor de AP of de organisatie aan de meldplicht heeft voldaan.
Datalekken kunnen zich in de gehele organisatie voordoen, maar de kans is het grootst daar waar veel met persoonsgegevens wordt gewerkt, zoals bij P&O en de uitvoerende RVE's.
Het onterecht niet aanmerken als datalek, het onterecht niet melden aan AP of betrokkene en het niet (op de juiste wijze) registreren van datalekken kan aanleiding zijn tot het opleggen van boetes door de AP aan de Regio.
In dit document worden de intern te zetten processtappen ten aanzien van een mogelijk datalek beschreven.
Voor de beoordeling of sprake is van een datalek en zo ja, om vervolgens te bepalen wat er moet gebeuren, wordt verwezen naar de Handreiking beoordeling datalekken AVG.

De procedure

In deze paragraaf wordt beschreven welke stappen achtereenvolgens gezet moeten worden als bij de Regio bekend wordt dat er sprake is of is geweest van een (mogelijk) datalek.
Allereerst is een overzicht opgenomen waarin de meest voorkomende stappen in relatie tot de actoren in een 'swimlane' schematisch zijn weergegeven.
Daarna volgt een tweede overzicht waarin de stappen voor interne en Regio-overstijgende opschaling in een 'swimlane' zijn weergegeven. Deze stappen zijn apart gevisualiseerd omdat opschaling zich niet vaak zal voordoen maar de kenbaarheid voor de organisatie (w.o. het bestuur) wel heel belangrijk is.

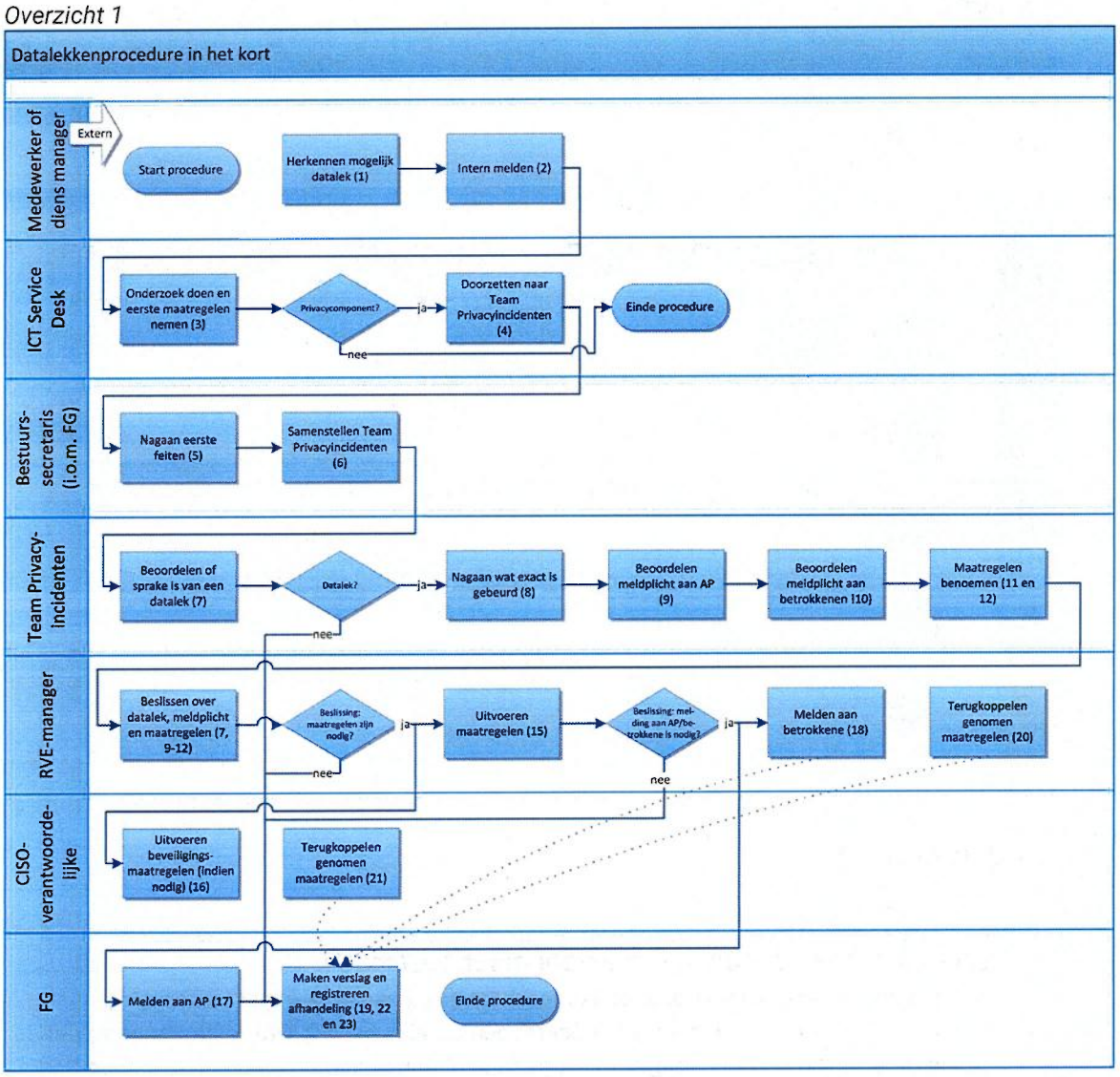
Na de schema's worden de stappen in detail uitgewerkt (waarbij de nummers van de stappen corresponderen met de nummers in de overzichten).
De processtappen zijn een uitwerking van de volgende aandachtspunten bij een datalek:

- Herkennen van mogelijk datalek
- Interne melding
- Eerste maatregelen door ICT (bij betrokkenheid device)
- Samenstelling van het Team Privacyincidenten
- Beoordelen datalek
- Overzicht verkrijgen
- Beoordelen meldplichtigheid aan AP
- Beoordelen meldplichtigheid aan betrokkene
- Maatregelen benoemen
- Interne en Regio-overstijgende opschaling
- Uitvoeren van maatregelen
- Daadwerkelijk melden
- Registratie van het datalek

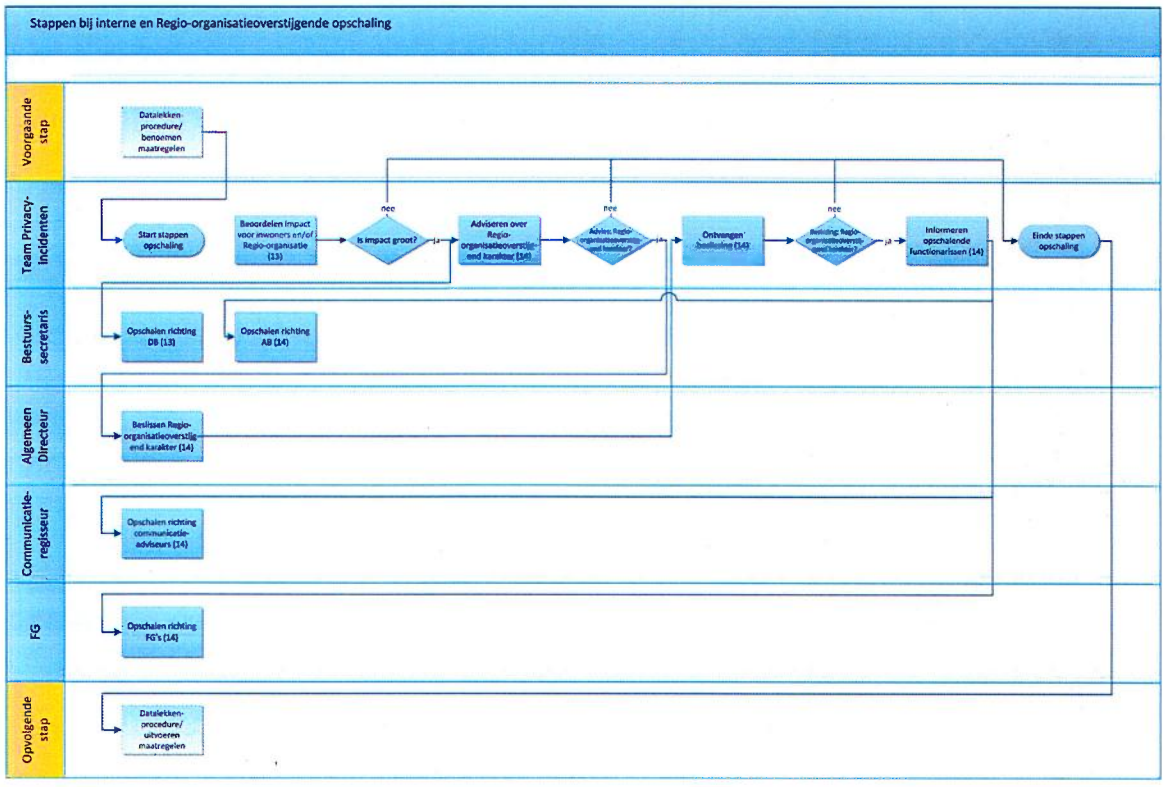
Algemeen

Het grootste deel van de onderstaande processtappen dient plaats te vinden voordat 72 uren zijn verstreken nadat bekend is geworden dat sprake is van een datalek.
In het algemeen is van belang dat er discreet met een datalek wordt omgegaan, zowel voor wat betreft de aanmelder als degene van wie de persoonsgegevens zijn gelekt. Van de gedupeerde persoon wordt in de beschrijving van het datalek niet de naam (en indien mogelijk ook geen andere identificerende gegevens) vermeld. Er is in het Document Management Systeem een vertrouwelijkheidsniveau (niveau datalekkenteam) voor het datalekkendossier (incl. brief aan betrokkene).
De rol van de betreffende RVE-manager bij beoordelen van een datalek is essentieel. De beslissing dat het een datalek is, dat al dan niet gemeld moet worden en het formuleren van de maatregelen ligt bij de verwerkingsverantwoordelijke, en dat is de RVE-manager. Uiteraard zullen de overige leden van het Team Privacyincidenten hier een advies over geven. Als de omstandigheden dit toelaten/vereisen (n.a.v. kennisniveau manager, specifieke omstandigheden van het lek) kan dit advies wat directiever van aard zijn. Indien manager advies niet overneemt, wordt dat geregistreerd. De FG kan eventueel escaleren via de lijn Algemeen Directeur – DB – AB.
Jaarlijks worden de datalekken en de werking van deze procedure geëvalueerd. De uitkomst van de evaluatie wordt gebruikt om het privacybewustzijn van de organisatie en deze procedure verder aan te scherpen.
Verder zal binnen de Regio de term datalek, vanwege de negatieve bijklank, zoveel mogelijk worden vervangen door de term privacyincident.

Overzicht 1


Datalekkenprocedure in het kort
Medewerker of diens manager
Extern
Start procedure
Herkennen mogelijk datalek (1)
Intern melden (2)
ICT Service Desk
Onderzoek doen en eerste maatregelen nemen (3)
Privacycomponent?
ja
nee
Doorzetten naar Team Privacyincidenten (4)
Einde procedure
Bestuurs-secretaris (i.o.m. FG)
Nagaan eerste feiten (5)
Samenstellen Team Privacyincidenten (6)
Team Privacy-Incidenten
Beoordelen of sprake is van een datalek (7)
Datalek?
ja
nee
Nagaan wat exact is gebeurd (8)
Beoordelen meldplicht aan AP (9)
Beoordelen meldplicht aan betrokkenen (10)
Maatregelen benoemen (11 en 12)
RVE-manager
Beslissen over datalek, meldplicht en maatregelen (7, 9-12)
Beslissing: maatregelen zijn nodig?
ja
nee
Uitvoeren maatregelen (15)
Beslissing: melding aan AP/betrokkene is nodig?
ja
nee
Melden aan betrokkene (18)
Terugkoppelen genomen maatregelen (20)
CISO-verantwoordelijke
Uitvoeren beveiligings-maatregelen (indien nodig) (16)
Terugkoppelen genomen maatregelen (21)
FG
Melden aan AP (17)
Maken verslag en registreren afhandeling (19, 22 en 23)
Einde procedure

Overzicht 2



Stap voor stap

Herkennen, interne melding en eerste maatregelen ICT

1. Een **medewerker** van de Regio constateert dat er sprake is geweest van een informatieveiligheidsincident dat mogelijk een datalek betreft. Ook is het mogelijk dat de constatering door een **manager** wordt gedaan of van buiten de organisatie van de Regio (bijv. via een inwoner of ICT-leverancier) komt.
2. De betrokken **medewerker** of diens **manager** meldt het (vermoeden van een) datalek z.s.m. intern bij de ICT servicedesk telefonisch op nummer 035-6926200 of per e-mail op meldpuntdatalek@regiogv.nl.
3. **ICT** stelt vast of er sprake is van omstandigheden waarbij elektronica (iPad, desktop, laptop Ericom Blaze, smartphone, USB-stick) betrokken is. Hierbij valt te denken aan een hack, malware of diefstal. Ook kan het zijn dat het een louter "fysiek datalek" (verlies of diefstal papieren dossier) betreft.
   Hiervoor start ICT een onderzoek. Hierbij wordt gekeken of er een afzonderlijk apparaat bij betrokken is. Zo ja, dan zal het betreffende apparaat zo spoedig mogelijk geïsoleerd worden van de elektronische systemen binnen de Regio.
   ICT onderneemt indien nodig nog andere acties die noodzakelijk zijn gelet op de aard van de melding. Denk hierbij aan het op afstand lokaliseren en/of wissen of versleutelen van een laptop, tablet, of smartphone of het op afstand blokkeren van de toegang tot een medewerkersaccount of clouddienst.
4. Indien **ICT** vermoedt dat het informatieveiligheidsincident een privacycomponent heeft, geeft zij de melding door aan het Team Privacyincidenten via de bestuurssecretaris (06-52578064).

Samenstellen van Team Privacyincidenten

5. De **bestuurssecretaris** of de **FG** gaat t.b.v. het overleg met het Team alvast de eerste feiten na bij de manager of medewerker
6. **Bestuurssecretaris** bepaalt (in overleg met de FG) de samenstelling van het Team en de wijze van afdoening en roept het Team bij elkaar. Samenstelling van het Team en aanpak hangen af van de ernst van het lek zowel voor de Regio als voor gedupeerde. Bij applicatie/systeemfouten is een grondigere afdoening nodig dan bij menselijke fouten. Wijze van aanpak kan variëren van schriftelijk (via mail) afdoen in kleinste samenstelling tot in volledige bezetting[1] bijeenkomen. Bij datalekken die wat complexer zijn en waarbij niet direct alle feiten boven tafel komen, is het gewenst nogmaals met het Team bij elkaar te komen op het moment dat alle feiten helder zijn.

Beoordelen of sprake is van een datalek en of gemeld moet worden

7. Het **Team Privacyincidenten** beoordeelt aan de hand van de Handreiking beoordeling datalekken AVG of er sprake is van een 'inbreuk in verband met persoonsgegevens', ofwel een datalek. Dit is 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 en adviseert de **RVE-manager** die beslist. Deze beoordeling moet zo spoedig mogelijk worden uitgevoerd. Als er wordt besloten dat geen sprake is van een datalek dan wordt het dossier m.b.t. het gemelde (mogelijke) datalek gesloten. Wordt er daarentegen besloten dat van een datalek wél sprake is, dan begint de termijn van 72 uren voor melden aan de AP vanaf nu te lopen.
8. Het **Team Privacyincidenten** gaat m.b.v. de Handreiking beoordeling datalekken AVG na wat er exact gebeurd is. Als de melding door de manager is gedaan of van buiten de Regio komt, dan loopt de afhandeling en terugkoppeling volledig via de manager. Indien de medewerker zelf heeft gemeld dan is hij of zij zelf de contactpersoon. De aanmelder wordt bedankt voor de melding. Bij de inventarisatie wordt o.a. bekeken welke persoonsgegevens zijn betrokken, wat de omvang van het datalek is en wie toegang hebben gekregen tot de persoonsgegevens. Hiervoor houdt de betrokken medewerker/manager zich beschikbaar en verleent alle medewerking die redelijkerwijs verwacht mag worden. De **RVE-manager** en de **CISO-verantwoordelijke** verstrekken de benodigde informatie. De verkregen informatie is nodig voor de vervolgstappen.
9. Het **Team Privacyincidenten** beoordeelt m.b.v. de Handreiking beoordeling datalekken AVG of het datalek gemeld moet worden aan de AP. Indien het Team dat wenselijk vindt, wordt de communicatieregisseur op de hoogte gesteld (als die niet al deel uitmaakt van het Team) van het feit dat gemeld gaat worden. Het Team adviseert de **RVE-manager** die beslist. Er moet binnen 72 uur worden bepaald of het datalek moet worden gemeld aan de AP en zo ja, moet ook binnen die termijn de melding zijn gedaan. Regel is dat er moet worden gemeld tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor rechten en vrijheden van natuurlijke personen.
10. Ook beoordeelt **Team Privacyincidenten** m.b.v. de Handreiking beoordeling datalekken AVG of het datalek gemeld moet worden aan de betrokkene. Indien gewenst wordt de communicatieregisseur erbij betrokken (als die niet al deel uitmaakt van het Team). Het Team

---

[1] Het volledige Team bestaat uit de FG, de CISO-verantwoordelijke, één van de juridisch adviseurs en de bestuurssecretaris. Per datalek wordt de betrokken manager aan het team datalekken toegevoegd. De bestuurssecretaris kan per geval bepalen dat andere personen aan het Team worden toegevoegd. De communicatieregisseur wordt erbij betrokken als de bestuurssecretaris het aannemelijk vindt dat er een melding aan AP (en betrokkene) gedaan moet worden.
Als een lid van het datalekkenteam de dupe is van het datalek of het datalek heeft veroorzaakt, wordt de beoordeling zonder deze persoon gedaan en wordt zo nodig het vertrouwelijkheidsniveau naar boven bijgesteld (bijv. alleen betreffende manager en FG).

adviseert de **RVE-manager** die beslist. De betrokkene moet worden geïnformeerd als het risico voor rechten en vrijheden van natuurlijke personen hoog is.

Maatregelen benoemen

11. Het **Team Privacyincidenten** formuleert (naast de maatregelen die ICT al heeft genomen) de maatregelen die direct getroffen moeten worden om het datalek te beëindigen en de schade te beperken en adviseert de **RVE-manager** die beslist.[2]
    Voorbeelden van maatregelen om schade bij een datalek te beperken zijn:
    - Een gepubliceerd bestand offline halen.
    - Een verkeerde ontvanger vragen om een bevestiging dat de gegevens uit een brief of e-mail zijn vernietigd. Hoewel je op basis van zo'n bevestiging niet 100% zeker weet dat de gegevens vernietigd zijn, is het handig dit mee te nemen in de risico-inschatting.
12. Het **Team Privacyincidenten** formuleert voorstellen ter voorkoming van herhaling en adviseert de **RVE-manager** die beslist.

Interne en Regio-organisatieoverstijgende opschaling

13. Bij datalekken met mogelijk grote impact voor inwoners en/of de Regio-organisatie is het van belang dat het bestuur snel op de hoogte wordt gebracht. Het **Team Privacyincidenten** beoordeelt of deze mogelijk grote impact aanwezig is.
    Overwegingen om te bepalen dat er grote impact is voor inwoners en/of de Regio-organisatie zijn:
    - betrokkenheid meerdere RVE's
    - maatschappelijke onrust / impact
    - (dreigende) verstoring van functioneren van de Regio
    - gevaar voor veiligheid medewerkers / inwoners
    - bedreiging van reputatie
    - betrokkenheid meerdere externe partners
    - opschaling vanuit overheidszijde
    - noodzaak grootschalige inzet
    - (verwachte) mediaaandacht

    Grote impact voor inwoners (en trouwens ook voor de Regio-organisatie) is er bijvoorbeeld wanneer volledige dossiers van inwoners voor onbevoegden toegankelijk zijn. Mogelijk grote impact voor de Regio-organisatie zelf kan aan de orde zijn wanneer de reputatie van de Regio in het geding is. Denk hierbij aan een in de landelijke media breed uitgemeten datalek dat zich vervolgens bij de Regio op een zelfde wijze voordoet.
    De **bestuurssecretaris** draagt zorg voor opschaling richting DB.
14. Als het datalek (naast grote impact voor inwoners en/of de Regio-organisatie) ook een Regio-organisatieoverstijgend karakter heeft, moet mogelijk opgeschaald worden richting de Regiogemeenten. Het **Team Privacyincidenten** beoordeelt of al dan niet sprake is van een datalek met een Regio-organisatieoverstijgend karakter en adviseert de Algemeen Directeur. De **Algemeen Directeur** beslist en koppelt de beslissing terug aan het Team Privacyincidenten.
    Om het Regio-organisatieoverstijgende karakter in te schatten wordt gekeken of het datalek afstraalt op de Regiogemeenten. Hiervan kan sprake zijn bij een datalek dat zich voordoet rondom taken waarvan de uitvoering deels bij de Regio en deels bij gemeenten ligt (zoals bij de taken van Inkoop en Contractbeheer). Of ten aanzien van taken waarvan niet helder is of de Regio daarvoor alleen of samen met Regiogemeenten verantwoordelijk is (zoals nieuwe taken waarvan de opdracht aan de Regio nog niet goed vast is gesteld).
    Als de beslissing is dat het datalek een Regio-organisatieoverstijgend karakter heeft, zorgt het

[2] Team Privacyincidenten kan daarnaast voorstellen doen m.b.t. doen van aangifte en melden bij de verzekering, etc.

Team Privacyincidenten ervoor dat de **bestuurssecretaris** overgaat tot opschaling richting AB en de Regiogemeenten (op welk niveau is afhankelijk van de omstandigheden van het geval). Ook wordt de **communicatieregisseur** geïnformeerd die zorgt voor opschaling richting communicatieadviseurs van de Regiogemeenten en de **FG** zorgt voor opschaling richting FG's van de Regiogemeenten. In communicatie naar de buitenwereld heeft de communicatieregisseur van de Regio een coördinerende rol. Communicatieadviseurs vanuit de Regiogemeenten stemmen hun werkzaamheden m.b.t. het datalek af met de communicatieregisseur van de Regio. De Regio is verantwoordelijk voor de afhandeling van het datalek. Dit vanwege het praktische aspect dat de Regio waarschijnlijk het best op de hoogte is van de situatie, maar ook vanwege de veronderstelde verwerkingsverantwoordelijkheid van de uitgevoerde taak. Dit betekent o.a. dat de Regio de melding aan AP en betrokkenen verzorgt.

Uitvoeren van maatregelen

15. De **RVE-manager** treft de maatregelen waartoe hij/zij na advies van het Team heeft besloten. Maatregelen die onmiddellijk genomen moeten worden, hebben de eerste aandacht.
16. De **CISO-verantwoordelijke** treft de vereiste beveiligingsmaatregelen (indien nodig).

Daadwerkelijk melden

17. De **FG** draagt zorg voor melding aan de AP via https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken. Er moet een kopie van de melding worden opgeslagen. Melding vindt onverwijld plaats, zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking. Ook als nog niet alle informatie bekend is, moet zo mogelijk binnen 72 uur een voorlopige melding worden gedaan. Deze kan later worden aangevuld of ingetrokken. In zo'n geval kan het Team vóór aanvulling of intrekking nogmaals bij elkaar komen.
18. De FG stelt een tekst op voor mededeling aan betrokkene(n)[3]. Deze tekst wordt voorgelegd aan de communicatieregisseur. De tekst die FG en communicatieregisseur samen hebben opgesteld wordt aan de RVE-manager gestuurd. Als FG en communicatieregisseur het niet eens zijn over de tekst, beslist RVE-manager. De **RVE-manager** draagt zorg voor het mededelen aan betrokkene(n). De mededeling kan bijv. in een e-mail of brief aan betrokkenen worden gestuurd. Overwogen kan worden om de betrokkene eerst telefonisch op de hoogte te stellen. Afhankelijk van de omstandigheden van het geval kan telefonisch informeren voldoende zijn. Een vooraf door FG en communicatieregisseur opgestelde belinstructie is dan wel van belang.
    Indien een eigen medewerker de dupe is van het datalek wordt, voordat een brief aan gedupeerde medewerker wordt gestuurd, de manager van gedupeerde medewerker op de hoogte gesteld, die de gedupeerde medewerker mondeling inlicht. Daarbij wordt de gedupeerde medewerker aangeboden actief te worden betrokken bij door de organisatie te treffen maatregelen.

Registratie

19. De **FG** zorgt (samen met het Team Privacyincidenten) voor het maken van een verslag (waarvoor een Word-sjabloon beschikbaar is) met daarin het feitenrelaas, de beoordeling en de maatregelen.
20. De **RVE-manager** laat per mail weten hoe en wanneer de geformuleerde maatregelen zijn uitgevoerd.

---

[3] De mededeling bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van het datalek, contactgegevens van de FG, de waarschijnlijke gevolgen van het datalek en de voorgestelde en getroffen maatregelen. Ook wordt aangegeven welke maatregelen betrokkene zelf kan nemen om de negatieve gevolgen te beperken.

21. De **CISO-verantwoordelijke** laat per mail weten hoe en wanneer de benodigde beveiligingsmaatregelen zijn uitgevoerd.
22. De **FG** registreert het in stap 19 bedoelde verslag en i.v.t. de melding aan AP en betrokkenen in het Document Management Systeem.
23. De **FG** neemt het gemelde informatieveiligheidsincident (waaronder naast de gemelde ook de niet-gemelde datalekken) met relevante kenmerken[4] op in het register van incidenten en datalekken dat de Regio op grond van de AVG in het Document Management Systeem bijhoudt.

Afronding

24. De **bestuurssecretaris** legt, indien naar zijn oordeel nodig, na afloop het verslag en de eventuele aanbevelingen voor aan de Algemeen Directeur. De Algemeen Directeur tekent voor gezien.

[4] In het register staat aangegeven of het een informatieveiligheidsincident of datalek betreft, een beschrijving van de inbreuk, het betrokken organisatieonderdeel, de mogelijke gevolgen van de inbreuk, de getroffen corrigerende maatregelen en of hiervan een melding is gedaan aan de AP en betrokkenen (plus inhoud van die melding). Ook staat aangegeven of de FG is betrokken bij afhandeling en of de RVE-manager het advies van het Team Privacyincidenten heeft opgevolgd en zo niet, waarom niet. De betrokkenheid van derde partijen die bij het datalek een rol hebben gehad wordt vermeld. Ten slotte is opgenomen een vermelding van de vindplaats van de documentatie aangaande verslag, melding aan AP en betrokkenen en de bevestiging van RVE-manager (en indien van toepassing van de CISO-verantwoordelijke) van daadwerkelijk genomen hebben van corrigerende (en preventieve) maatregelen.

Regio
Gooi en Vechtstreek

Strategisch Informatiebeveiligingsbeleid Regio Gooi en Vechtstreek

Van 2019 tot en met 2022

Ons kenmerk	19.0013516
Versie	0.4
Datum	30 oktober 2019
Contactpersoon	
E-mail	@regiogv.nl

Gemeente Blaricum · Gemeente Eemnes · gemeente goorsemaren · Hilversum Mediastad · Gemeente Huizen · Gemeente Laren · Gemeente Weesp · Wijdemeren

INHOUD

Versiebeheer 1

Inleiding 2

Leeswijzer 2
Wat is informatiebeveiliging? 2
Ambitie en visie van de Regio op het gebied van informatieveiligheid 2

Strategisch beleid 3

Doel 3
Ontwikkelingen 3
Standaarden informatiebeveiliging 3
Plaats van het strategisch beleid 4
Scope informatiebeveiliging 4
Uitgangspunten 4

Organisatie, taken & verantwoordelijkheden 6

Aansturing: Algemeen Directeur en Centraal Management Team (CMT) 6
Uitvoering: RVE- managers 6
Controle en verantwoording 7

Versiebeheer

Versie	Datum	Door	Wijzigingen
0.1	11 09 2019		
0.2	24 09 2019		Feedback.
0.3	29 10 2019	CMT	Ingestemd
0.4			Instemming DB

Inleiding

Dit document beschrijft het strategische informatiebeveiligingsbeleid van de Regio Gooi en Vechtstreek ('Regio') voor de jaren 2019 tot en met 2022.
Deze document is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Informatiebeveiligingsbeleid 2019-2022' zet de Regio een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de Regio te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG.

Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Regio Informatiebeveiligingsplan (vastgesteld door het CMT) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de RVE-managers, de CISO, het dreigingsbeeld van de IBD en de uitkomsten van relevante audits. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de Regio en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie.

Ambitie en visie van de Regio op het gebied van informatieveiligheid

De komende jaren zet de Regio in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de Regio en de basis voor het beschermen van rechten van burgers, werknemers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken.

Het proces van informatiebeveiliging is niet alleen gericht op het beschermen van informatie, maar is tegelijkertijd een 'enabler'. Het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, innovatieve manieren van werken.
De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Ook gaat het niet alleen over ICT; verantwoord en bewust gedrag van medewerkers is essentieel voor informatieveiligheid.

Strategisch beleid

Doel

Het doel van deze beleidsnota is het presenteren van het 'Strategisch Informatiebeveiligingsbeleid voor de jaren 2019 tot en met 2022'. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP).

Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende:

De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG. Dat wil zeggen dat de RVE-managers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit betekent dat bij het maken van keuzes op voorhand én daarna een afweging maakt en informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

De 10 principes voor informatiebeveiliging (zie bijlage)

De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de organisatie zichzelf oplegt. De principes zijn als volgt:

1. Bestuur en management bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de Regio organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen van de Regio, dan kan dit directe gevolgen hebben voor inwoners, medewerkers, ondernemers en partners van de Regio. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

Dreigingsbeeld Informatie Beveiligings Dienst

Het Dreigingsbeeld van de Informatie Beveiligings Dienst (IBD) geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

Informatie uit incidenten en inbreuken op de beveiliging

De Regio kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017 en de toepassing daarvan bij de Regio. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 (en eventueel ook NEN-ISO/IEC 7510:2017 genomen.

Voor de ondersteuning van de Regio bij het formuleren en realiseren van haar informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[1] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van een risicoanalyse voor het opstellen van een beveiligingsplan. De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

Plaats van het strategisch beleid

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.
Dit document beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligingsplan van de Regio'.

Scope informatiebeveiliging

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van de Regio en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit strategisch Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af. Voor zover van toepassing kunnen specifieke beveiligingseisen gelden op grond van bijzondere wet- en regelgeving. Deze worden in aanvullende documenten geformuleerd.

Uitgangspunten

Het bestuur en management spelen een cruciale rol bij het uitvoeren van dit strategische informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de Regio heeft, de risico's die de Regio hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het management geeft een duidelijke richting aan informatiebeveiliging en laat zien dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele Regio. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de Regio en de relevante landelijke en Europese wet- en regelgeving.

Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:
- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.

---

[1] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.

- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Het waarborgen van de naleving van dit beleid.

Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:
- Alle informatie en informatiesystemen zijn van belang voor de Regio, bepaalde informatie is van vitaal en kritiek belang. Het Dagelijks Bestuur is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de Regio hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, study en act' vormen samen het managementsysteem van informatiebeveiliging.
- De Regio stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Invulling van de uitgangspunten
Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:
- Het Dagelijks Bestuur van de Regio stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De Algemeen Directeur (met instemming van het CMT) stelt jaarlijks het informatiebeveiligingsplan vast.
- De Algemeen Directeur (daarbij gesteund door het CMT) is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De Algemeen Directeur (daarbij gesteund door het CMT) is verantwoordelijk voor het vragen om informatie bij de RVE-managers en ziet erop toe dat de RVE-managers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan de Algemeen Directeur met kopie aan het CMT.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen voor zover aanwezig.
- De RVE-managers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Alle medewerkers van de Regio worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
- De RVE-managers zien er op toe dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.

- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. RVE-managers kunnen quickscans informatiebeveiliging uitvoeren om deze risico-afwegingen te kunnen maken, daarbij gefaciliteerd door de CISO.

Randvoorwaarden
Belangrijke randvoorwaarden zijn:
- De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
- Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een informatiebeveiligingsplan opgesteld onder leiding van de CISO, gebaseerd op:
  - de uitkomsten van eventuele audits;
  - het dreigingsbeeld van de IBD;
  - De door de RVE-managers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD).

In dit model is het lijnmanagement verantwoordelijk voor de eigen processen, inclusief de informatiebeveiliging daarvan.
De tweede lijn (CISO, security officers indien aanwezig) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt.
In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

Aansturing: Algemeen Directeur en Centraal Management Team (CMT)

De Algemeen Directeur (met instemming van het CMT) zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een RVE-manager. De Algemeen Directeur zorgt dat de RVE-managers zich verantwoorden over de beveiliging van de informatie die onder hen berust.

De Algemeen Directeur (met instemming van het CMT) stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De Algemeen Directeur (met instemming van het CMT) draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO van de Regio GV. De Algemeen Directeur (met instemming van het CMT) autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de Regio gezien als een integraal onderdeel van risicomanagement.

Uitvoering: RVE- managers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle RVE-managers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. RVE-managers rapporteren aan de Algemeen Directeur (met kopie aan het CMT) over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het CMT overleg.

Taken van de RVE-managers in het kader van informatiebeveiliging zijn:
- Het leveren van input voor wijzigingen op maatregelen en procedures.

- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

Voorbereiding en coördinatie van het overleg ligt bij de CISO.

Controle en verantwoording

Dit Strategisch Beleid is een verantwoordelijkheid van het Dagelijks Bestuur van de Regio. Het Dagelijks Bestuur, de Algemeen Directeur, het CMT en de RVE-managers zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De Algemeen Directeur (daarbij gesteund door het CMT) is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan het Dagelijks Bestuur. De Algemeen Directeur (daarbij gesteund door het CMT) rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische onderwerpen die aanvullend zijn op dit strategische beleid.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking waarmee het Dagelijks Bestuur aangeeft in hoeverre de Regio voldoet aan de afspraken die gemaakt zijn en welke eventuele verbetermaatregelen die de Regio gaat treffen.

Middels deze verantwoording wordt het Algemeen Bestuur van de Regio geïnformeerd. Deze essentiële betrokkenheid van het bestuur laat zien dat de Regio informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

GGD Gooi en Vechtstreek					
Maatregelen	**Maatregelen geimplementeerd**	**Toelichting GGD**	**Risico**	**Mitigerende maatregelen**	
Intern informatievoorziening rechten betrokkenen	Deels	Ik weet niet wat GGD hier al zelf voor heeft gemaakt (check Kim/Wenda) maar gebruik kan worden gemaakt van de informatie in de privacyverklaring van de Regio (https://www.regiogv.nl/privacyverklaring/) en het privacybeleid, hst. 8 (MyCorsa 21.0004032) dat 8 juli waarschijnlijk door het bestuur wordt vastgesteld. Specifiek voor GGD Contact is er een privacyverklaring waarna de GGD ook op de website verwijst: https://ggdcontact.nl/nl/privacy	Belemmering uitoefenen rechten van betrokkenen	GGD voldoet deels aan de maatregel. Er is een privacyverklaring en beleid voor de regio.	privacybeleid inmiddels vastgesteld
Plausabiliteitscheck		Check bij GGD	Onrechtmatige toegang tot gegevens van betrokkenen	Plausabiliteitscheck wordt opgenomen in de werkinstructie/ e-learning GGD Contact.	
Overeenkomsten		Algemeen bekend (neem ik aan?) dat dat via juridisch adviseurs verloopt, volgens mij geen proces, Check bij juridisch adviseurs	Ontbreken verwerkersovereenkomsten	GGD voldoet waarschijnlijk deels aan de maatregel. Dit moet nagevraagd worden bij de juridische adviseurs van Gooi en Vechtstreek.	We hebben hiervoor het mandaatbesluit, een apart proces hiervoor is niet nodig.
Audit/controle derde partijen	Nee		Ontbreken verwerkersovereenkomsten	GGD voldoet niet aan de maatregel. GGD dient een proces te implementeren voor het controleren op de toepassing van privacymaatregelen bij derden.	Verklaringen van toereikendheid worden inmiddels al opgevraagd bij verwerkers voor enkele andere organisatieonderdelen. Voor GGD Corona kan dit ook gemakkelijk worden ingeregeld.
Monitoring e-learning bco-medewerkers	Ja	Medewerkers worden in eerste instantie gewezen op het feit dat de E-learning aanwezig is. Verder zijn er rollen toegekend in academy van coach waardoor medewerkers worden gecheckt op het hebben uitgevoerd van de e-learning. Consequenties voor het niet uitvoeren van de E-learning zal uiteindelijk een verwijdering van het BCO proces zijn.	Toegang door derden in de GGD contact door ontbreken beveiliging bij toegang tot applicatie	GGD voldoet aan de maatregel.	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Afwijkingen referentie DPIA		DPIA v. 1.1 is gedeeld met GGD. Bij de FG zijn geen lokale afwijkingen bekend. Check door GGD zelf.	Verwerking van de klachten door GGD blijkt niet-noodzakelijk	Als verwerkingsverantwoordelijke dienen afwijkingen op de referentie DPIA te worden verwerkt. Indien dit niet tijdig wordt gedaan is het risico dat afwijkingingen in het bco-proces van de GGD andere risico's met zich meenemen die niet in de DPIA worden meegenomen en mogelijk ook niet gemitigeerd.	Ik neem aan dat we dus niet afwijken van de landelijke referentie DPIA vwb de uitvoering?
Intern privacybeleid	Deels	Het nieuwe intern privacybeleid van de Regio wordt 8 juli als het goed is vastgesteld door het bestuur. Nu hebben we nog een gedateerd Reglement Bescherming Persoonsgegevens (MyCorsa [redacted]	Geen intern privacybeleid	GGD voldoet deels aan de maatregel. Het interne privacybeleid is verouderd maar wordt geupdate.	privacybeleid inmiddels vastgesteld
Datelekbeleid	Ja		Het niet tijdig/correct reageren op datalekken	GGD voldoet aan de maatregel.	
Datalekkenregister	Ja		Het niet tijdig/correct reageren op datalekken	GGD voldoet aan de maatregel.	
Actueel verwerkingsregister	Ja	Het verwerkingsregister (myCorsa 19.0014889) wordt doorlopend bijgewerkt. De verwerkingen ihkv GGD Contact zitten er nog niet volledig in.	Verwerkingsregister niet volledig/compleet/up to date	GGD voldoet aan de maatregel.	
Procedure aanvragen betrokkenen	Ja	Beleid rechten van betrokkenen is te vinden in hst 8 Privacybeleid (MyCorsa 21.0004032). De procedure is beschreven in Werkproces inzageverzoeken en overige verzoeken ogv art. 15 t/m art. 18 AVG (MyCorsa 19.0011233). Specifiek voor verwijderverzoeken rondom coronaverwerkingen is er een procedurebeschrijving gemaakt door de juridisch adviseurs die door GGD (Kim, Wenda) verder is aangescherpt. Check bij hen.	Het niet tijdig/correct reageren op verzoeken van betrokkenen	GGD voldoet aan de maatregel.	
Bewaar- en verwijder proces	Deels	Selectielijst intergemeentelijke organen 2020 waarop wordt toegezien door Pieter-Bas. Een bewaartermijnenbeleid is er volgens mij niet. Check bij PB.	Het niet tijdig verwijderen/archiveren van gegevens.	GGD voldoet deels aan de maatregel. De GGD dient een bewaartermijnenbeleid op te stellen.	Hiervoor heeft [redacted] nog een update

[redacted]

Van: [redacted]
Verzonden: dinsdag 22 maart 2022 11:25
Aan: [redacted]
Onderwerp: FW: Reminder: Update Autorisatiematrix GGD Contact en verzoek tot aanmaken AD groepen
Bijlagen: Rollenmatrix GGD Contact Nov 2021 GGD V1.8.pdf; 20211206 Beschrijving contextbeheer&dossierkwaliteit - GGD Contact[29].pdf

---

Van: [redacted]
Verzonden: donderdag 13 januari 2022 16:34
Aan: [redacted]
CC: [redacted]
Onderwerp: FW: Reminder: Update Autorisatiematrix GGD Contact en verzoek tot aanmaken AD groepen

Hoi [redacted]

Zouden jullie naar onderstaande kunnen kijken?
Het betreft wederom een nieuwe rol in BCO portaal.
In ieder geval alle Dagcoördinatoren en Context coördinatoren mogen deze rol toebedeeld krijgen.
Voor de volledigheid hieronder de namen:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Groet,

[redacted]
Coördinator Bron- en contactonderzoek
Afdeling Infectieziektenbestrijding

GGD
Gooi en Vechtstreek

Burgemeester de Bordesstraat 80, 1404 GZ Bussum
Postbus 251, 1400 AG Bussum
(035) 692 64 00 | ggdgv.nl | bco@ggdgv.nl

[redacted]

Van: [redacted]
Verzonden: dinsdag 22 maart 2022 11:25
Aan: [redacted]
Onderwerp: FW: Toegang tot BCO-Portaal

Van: [redacted]
Verzonden: donderdag 30 december 2021 15:21
Aan: [redacted]
CC: E-mail Corona <corona@ggdgv.nl>; [redacted]
Onderwerp: RE: Toegang tot BCO-Portaal

Beste [redacted]

Dit is het BCO portaal en iedereen (alle rollen) moeten daartoe toegang hebben. De dag coördinatoren moeten ook de rol werkverdeler hebben.

Ik begrijp net van [redacted] dat hij niet in de infectieziektemailbox kan. De rest van de nieuwe wel. Kan jij deze toegang regelen?

Dank je wel alvast,

Gr [redacted]

Van: [redacted]
Verzonden: woensdag 29 december 2021 07:59
Aan: [redacted]
Onderwerp: Toegang tot BCO-Portaal

Hoi,

Voor de toegang tot het BCO-Portaal zijn 2 rollen opgenomen op het netwerk waar mensen aan toegevoegd kunnen worden:

- DBCO-Gebruiker
- DBCO-Werkverdeler

Nu zie ik, naar aanleiding van het feit dat Isabelle er niet in kon, dat iedereen op persoonlijke naam aan de rol DBCO-gebruiker. Ik vraag me af of het niet zo is dat BCO'ers toegang moet hebben tot BCO-portaal. Geldt dit alleen voor medewerkers BCO? Of ook voor medewerkers BCO admin? En medewerkers BCO context? En de dagcoordinatoren BCO?

Als jij aangeeft welke toegang moeten hebben, dan laat ik het aanpassen naar de functie in plaats van op persoonlijke naam (en gaat het in de toekomst automatisch goed).

Groetjes, [redacted]

[redacted]

Van: [redacted]
Verzonden: dinsdag 22 maart 2022 11:24
Aan: [redacted]
Onderwerp: FW: Vraag over de rol DBCO-Werkverdeler

Van: E-mail Corona
Verzonden: woensdag 17 november 2021 13:54
Aan: [redacted]
Onderwerp: RE: Vraag over de rol DBCO-Werkverdeler

Ha[redacted]

Ze mogen allemaal deze rol krijgen en dus inderdaad deze rol koppelen aan medewerker admin BCO :-)

Van: [redacted]
Verzonden: woensdag 17 november 2021 12:46
Aan: E-mail Corona <corona@ggdgv.nl>
Onderwerp: Vraag over de rol DBCO-Werkverdeler

Hoi,

Ik weet niet of ik bij jullie aan het juiste adres ben of dat ik dit aa[redacted]moet vragen, maar ik heb een paar vragen over het volgende: de rol DBCO-Werkverdeler.

- Ik zie in de Active Directory dat de mensen die er in zitten allemaal medewerker admin BCO zijn met uitzondering van[redacted]en[redacted]Nu weet ik niet of[redacted]deze rol ook moeten hebben?
- Daarnaast zijn er een drietal functieiwijzigingen ingevoerd ([redacted]) waarbij de genoemde mensen medewerker admin BCO moeten worden. Hebben zij ook de rol DBCO-werkverdeler nodig?

Als nu allemaal ook de rol DBCO-werkverdeler krijgen, dan kan deze rol worden gekoppeld aan medewerker admin BCO. Zo niet, dan graag bij elke keer dat iemand medewerker admin BCO wordt daarbij aangeven of de rol DBCO-werkverdeler ook nodig is.

ik hoop dat jullie het snappen wat ik schrijf, zo niet, bel me dan op 211 :-)

Groetjes,[redacted]

[redacted]

Van: [redacted]
Verzonden: dinsdag 22 maart 2022 10:27
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Inventarisatie voldoen aan Wob-verzoek GGD-datalek

Dag[redacted]

In GGD Contact (oftewel BCO-Portaal) zijn een aantal rollen gedefinieerd en tevens opgenomen in de Active Directory.

De rollen DBCO-Gebruiker en DBCO-Werkverdeler zijn gekoppeld aan de functie die iemand uitvoert.

De rollen BCO-GGD-Medische Supervisie en BCO-GGD-Gesprekscoach zijn toebedeeld aan 2 personen.
De rol BCO-GGD-Dossierkwaliteit is gekoppeld aan 11 mensen, dus niet gekoppeld aan een bepaalde functie.
De rol BCO-GGD-Contextbeheerder is gekoppeld aan de functie BCO Teamcontext.

Mocht je nog wat meer willen weten, dan hoor ik dat graag.

Groetjes,[redacted]

Sent: woensdag 20 mei 2020 10:07:24
To:
Cc:
Subject:

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

Van:
Datum: 19 mei 2020 om 10:28:10 CEST
Aan:
Onderwerp: Aanbod Bender

Zoals telefonisch besproken hierbij kort ons voorstel.

Van 1 juni t/m 31 augustus, een vaste basis van vier kandidaten, zie profielen in de bijlagen.

Naast een vaste basis stel ik voor om op 1 juni te starten met drie extra kandidaten. Die je waar nodig kunt op- en afschalen. Voor het opschalen wij hebben vijf werkdagen nodig dit ivm training en autorisatie van ICT systemen. Voor afschalen hanteren wij normaal gesproken een termijn van één maand. Gezien de omvang en maatschappelijke impact van het bron- en contactonderzoek hanteren wij nu een termijn van twee weken.

Onderstaand een overzicht van de kandidaten en de geldende tarieven, deze zijn exclusief BTW en thuiswerk faciliteiten (telefoon en laptop). Alle kandidaten beschikken over de volgende competenties en vaardigheden: HBO werk- en denkniveau, communicatief zeer vaardig en ICT-vaardig.

Naam:

Tarief:

Beschikbaar: Per direct

Uren per week: 32 uur

Naam:

Tarief:

Beschikbaar: Per direct

Uren per week: 36 uur

Naam:

Tarief:

Beschikbaar: Per direct

Uren per week: 32 uur

Naam:

Tarief:

Beschikbaar: Per direct

Uren per week: 36 uur

Naam:

Tarief:

Beschikbaar: Per direct

Uren per week: 32 uur

Naam:

Tarief:

Beschikbaar: Per direct

Uren per week: 36 uur

Naam:

Uren per week: 36 uur

Alle bovengenoemde kandidaten zijn zeven dagen per week inzetbaar in diensten van acht uur per dag. De werkzaamheden worden vanuit huis uitgevoerd hiervoor zijn bepaalde autorisaties nodig. Kan jij aangeven met welke programma's er gewerkt dient te worden?

De kandidaten worden vooraf getraind middels een e-learning en gezamenlijke zoom-meeting dit neemt ongeveer een dagdeel in beslag, welke voor rekening komt van de GGD Gooi- en Vechtstreek.

Tot slot hoop ik je met bovenstaand voorstel een passend aanbod te hebben gedaan en hoop ik dat ik de kans krijg om te laten zien wat we voor de GGD kunnen betekenen.

Laten wij deze week even telefonisch-contact hebben om het voorstel te bespreken.

Voor nu een fijne werkdag gewenst.

--
Met vriendelijke groet,

Manager Wonen

Benden voor jou

ARBEIDSOVEREENKOMST VOOR BEPAALDE TIJD

DE ONDERGETEKENDEN:

1. Regio Gooi en Vechtstreek, gevestigd te 1404 GZ Bussum, aan de Burgemeester de Bordesstraat 80, hierbij rechtsgeldig vertegenwoordigd door de Manager .....(RVE vermelden), mevr./dhr. .....(naam vermelden), hierna te noemen: "Werkgever",

en

2. .....(gegevens werknemer vermelden), hierna te noemen: "Werknemer",

PARTIJEN ZIJN HET VOLGENDE OVEREENGEKOMEN:

Artikel 1 Duur van de overeenkomst

1. Werknemer treedt met ingang van ..... in dienst van Werkgever voor bepaalde tijd. De arbeidsovereenkomst eindigt van rechtswege op .....
2. De eerste maand van de arbeidsovereenkomst geld als proeftijd in de zin van artikel 7:652 van het Burgerlijk Wetboek. Tijdens de proeftijd heeft zowel Werkgever als Werknemer het recht om deze overeenkomst op ieder moment te beëindigen, zonder dat daarvoor opzegging is vereist

Artikel 2 Ontbindende voorwaarde i.v.m. verklaring omtrent gedrag

1. Werknemer overhandigt uiterlijk 10 weken na ondertekening van deze arbeidsovereenkomst, te weten uiterlijk op ....., een Verklaring Omtrent Gedrag (VOG) aan Werkgever.
2. Als Werknemer de VOG niet uiterlijk op ..... aan Werkgever overhandigd heeft, dan eindigt deze arbeidsovereenkomst van rechtswege op voornoemde datum.

Artikel 3 Ontbindende voorwaarde i.v.m. afleggen eed of belofte

1. Werknemer is op grond van artikel 7 Ambtenarenwet 2017 verplicht om de eed of de belofte af te leggen. Werkgever is op grond van artikel 5 lid 1 onder a Ambtenarenwet 2017 verplicht om Werknemer daartoe in staat te stellen. Werknemer moet de eed of de belofte uiterlijk binnen vier maanden na zijn indiensttreding afleggen, te weten uiterlijk op .....
2. Als Werknemer de eed of de belofte niet uiterlijk op ..... afgelegd heeft, dan eindigt deze arbeidsovereenkomst van rechtswege op voornoemde datum.

Artikel 4 Beëindiging - opzegtermijn

Zowel Werkgever als Werknemer kan deze overeenkomst beëindigen door schriftelijke opzegging tegen het einde van de maand met inachtneming van de wettelijke opzegtermijn.

Artikel 5 Functie

1. Werknemer is bij Werkgever werkzaam in de functie van ..... De functie van ..... is toebedeeld aan het generieke functieprofiel ..... waaraan de salarisschaal .. is gekoppeld.

2. Werknemer is verplicht zich als goed werknemer te gedragen. Werknemer zal de overeengekomen werkzaamheden naar zijn beste vermogen verrichten. Hij zal de aanwijzingen en instructies opvolgen die hem door of namens Werkgever zijn gegeven.
3. Werknemer verricht de werkzaamheden hoofdzakelijk vanuit Bussum of vanuit één van de locaties van Regio Gooi en Vechtstreek. Werkgever kan van Werknemer verlangen dat deze andere werkzaamheden (van een vergelijkbaar niveau) uitvoert. Werkgever kan Werknemer eventueel ook overplaatsen naar een andere vestiging. Werkgever zal het voorgaande alleen doen als dat naar zijn mening noodzakelijk is voor een goede vervulling van de binnen zijn organisatie te verrichten activiteiten. Werkgever zal voorafgaand aan dergelijke wijzigingen met Werknemer overleggen.
4. Werknemer geeft wijzigingen in zijn persoonlijke gegevens voor zover deze voor Werkgever redelijkerwijs van belang kunnen zijn, tijdig door. De gevolgen van het niet of niet tijdig doorgeven van wijzigingen komen voor rekening van Werknemer.
5. Werknemer verklaart dat hij bij indiensttreding en/of bij de uitoefening van zijn functie bij Werkgever niet wordt gehinderd door een concurrentie- en/of relatiebeding van één van zijn vorige werkgevers.
6. Werknemer verklaart dat hij geen medische belemmeringen heeft, die aan een goede uitvoering van zijn functie in de weg staan.

Artikel 6 Arbeidsduur en werktijden

1. Werknemer is werkzaam voor .. uur per week
2. Op Werknemer is de standaard of bijzondere regeling voor de werktijden van toepassing
3. Van het verrichten van overwerk/werk buiten het dagvenster is alleen sprake als tot het verrichten daarvan uitdrukkelijk opdracht is gegeven door Werkgever. De hiervoor geldende bepalingen uit het personeelshandboek Regio Gooi en Vechtstreek zijn alsdan van toepassing.

Artikel 7 Salaris, salaristoelagen en IKB

1. Het basissalaris van Werknemer is op basis van een 36-urige werkweek € ..... bruto per maand, schaal .. trede ....

2. Werknemer heeft maandelijks recht op een Individueel Keuzebudget (IKB). De hoogte van het IKB en de besteding wordt bepaald door de Cao SGO en het Personeelshandboek Regio Gooi en Vechtstreek. Werknemer kan het IKB besteden aan de in de Cao SGO en in het personeelshandboek opgenomen doelen.Werknemer stemt in om de loonstrook, jaaropgave en ook overige communicatie over de arbeidsovereenkomst digitaal te ontvangen.

Artikel 8 Vakantie-uren

1. Werknemer heeft elk kalenderjaar recht op betaalde vakantie. Werknemer heeft recht op wettelijke vakantie-uren en bovenwettelijke vakantie-uren per kalenderjaar conform Cao SGO en het personeelshandboek. Als de werknemer in deeltijd werkt, geldt het recht op betaalde vakantie naar rato van het dienstverband.
2. Aanvullende verlofaanspraken zijn van toepassing voor zover deze zijn opgenomen in het personeelshandboek en op werknemer van toepassing zijn.
3. Werkgever stelt de tijdstippen van de vakantie vast na overleg met Werknemer.
4. Als Werknemer bij het einde van het dienstverband een negatief saldo vakantiedagen heeft, verrekent Werkgever dit saldo met de laatste salarisbetaling en/of de eindafrekening. Als bij het einde van het dienstverband sprake is van een positief saldo, dan betaalt Werkgever de niet genoten vakantiedagen uit, tenzij Partijen hierover andere afspraken maken.

Artikel 9 Pensioen

Werknemer bouwt pensioen op bij de Stichting pensioenfonds ABP. De voorwaarden zijn vastgelegd

in het ABP pensioenreglement. Dit reglement is van toepassing zoals het op dit moment luidt en in de toekomst zal komen te luiden.

Artikel 10 Bedrijfseigendommen

1. Bedrijfseigendommen die door Werkgever aan Werknemer ter beschikking zijn gesteld voor de functie uitoefening en verder alle correspondentie, aantekeningen, tekeningen, modellen, geautomatiseerde bestanden en andere dragers van gegevens etc. die betrekking hebbende op de bedrijfsaangelegenheden, blijven eigendom van Werkgever.
2. Werknemer moet de in lid 1 bedoelde zaken en gegevens op eerste verzoek van Werkgever, maar in elk geval bij het einde van de arbeidsovereenkomst bij Werkgever inleveren.
3. Werknemer mag geen bedrijfsdocumenten- of informatie als bedoeld in dit artikel mee naar huis nemen of naar zijn privé e-mailadres sturen als dat voor de uitoefening van zijn werkzaamheden niet noodzakelijk is

Artikel 11 Nevenwerkzaamheden

1. In aanvulling op de verplichting die op grond van artikel 8 lid 1 onder a en lid 2 onder a Ambtenarenwet 2017 op Werknemer rust, geldt voor Werknemer hetgeen in dit artikel is bepaald.
2. Het is Werknemer verboden om gedurende zijn dienstverband, direct of indirect, als werknemer of als zelfstandige in welke vorm dan ook, voor een andere werkgever of andere opdrachtgever werkzaam te zijn. Werknemer moet zich ook onthouden van het doen van zaken voor eigen rekening. Deze twee verboden gelden niet als Werkgever voorafgaand schriftelijk toestemming heeft gegeven aan Werknemer.
3. Het aanvaarden van onbetaalde nevenfuncties is Werknemer toegestaan, mits hij daarvan tevoren schriftelijk mededeling doet aan Werkgever en mits Werkgever schriftelijk te kennen heeft gegeven tegen aanvaarding van een dergelijke nevenfunctie geen bezwaar te hebben.

Artikel 12 Geheimhouding

Werknemer verplicht zich zowel tijdens als na afloop van de arbeidsovereenkomst strikte geheimhouding te betrachten over alle aangelegenheden betreffende Werkgever, waarvan het vertrouwelijke karakter geacht kan worden bekend te zijn.

Artikel 13 Ziekte bij of na uitdiensttreding

1. Als Werknemer ziek is op het moment dat hij uit dienst gaat of binnen vier weken na het einde van de arbeidsovereenkomst ziek wordt én op dat moment geen WW-uitkering ontvangt of niet werkzaam is bij een andere werkgever, meldt Werknemer zich onmiddellijk ziek bij Werkgever conform de bij Werkgever geldende regels.
2. Als sprake is van een situatie als bedoeld in lid 1, moet Werknemer:
   a. gehoor geven aan een oproep van de bedrijfsarts en/of arbeidsdeskundige van Werkgever;
   b. aan Werkgever alle informatie verstrekken die hij op grond van de Ziektewet of Wet WIA aan Werkgever als eigenrisicodrager of aan het UWV moet verstrekken;
   c. alle verplichtingen nakomen die volgen uit de Ziektewet en de Wet WIA;
   d. meewerken aan een namens Werkgever aangeboden re-integratietraject of proefplaatsing;
   e. een (vervroegde) IVA-uitkering aan vragen indien en zodra de bedrijfsarts dit mogelijk acht.
3. De in lid 2 genoemde verplichtingen blijven bestaan zolang Werknemer arbeidsongeschikt blijft en een Ziektewetuitkering ontvangt. Als Werknemer volledig hersteld is dan eindigen de verplichtingen, tenzij Werknemer binnen vier weken na hersteldmelding opnieuw arbeidsongeschikt raakt.

Artikel 14 Wijziging

1. Werkgever mag eenzijdig de inhoud van de arbeidsovereenkomst met Werknemer wijzigen.
2. Werkgever zal de in lid 1 omschreven bevoegdheid alleen gebruiken wanneer hij daarbij een zodanig zwaarwegend belang heeft dat de belangen van Werknemer bij ongewijzigde voortzetting van de arbeidsovereenkomst daarvoor naar maatstaven van redelijkheid en billijkheid moeten

wijken.
3. Werkgever zal een eenzijdige wijziging van de arbeidsovereenkomst twee maanden voorafgaand aan de ingang van de wijziging schriftelijk aan Werknemer mededelen.

Artikel 15 Ambtenarenwet 2017

1. Voor Werkgever en Werknemer gelden de rechten en verplichtingen die voortvloeien uit de Ambtenarenwet 2017.
2. Overtreding daarvan kan leiden tot een sanctie uit het Burgerlijk Wetboek of een reden vormen voor beëindiging van de arbeidsovereenkomst.

Artikel 16 Cao SGO en het Personeelshandboek Regio Gooi en Vechtstreek

1. Op deze arbeidsovereenkomst is de Cao Samenwerkende Gemeentelijke Organisaties (Cao SGO) van toepassing, zoals deze nu luidt en in de toekomst zal komen te luiden. Door ondertekening van deze overeenkomst verklaart Werknemer zich daarmee akkoord.
2. Op deze arbeidsovereenkomst is de bij Werkgever geldende Personeelshandboek Regio Gooi en Vechtstreek van toepassing, zoals dit nu luidt en in de toekomst zal komen te luiden. Door ondertekening van deze overeenkomst verklaart Werknemer zich daarmee akkoord.

Artikel 17 Toepasselijk recht

1. Op deze overeenkomst is Nederlands recht van toepassing.
2. Als één of meer bepalingen van deze overeenkomst ongeldig of op andere wijze niet verbindend zou(den) zijn, wordt daardoor de geldigheid van de overige bepalingen van deze overeenkomst niet aangetast. Partijen zullen deze overeenkomst dan – voor zover nodig - in gezamenlijk overleg en in de geest van deze overeenkomst aanpassen. Aanpassing betekent dat de niet-verbindende bepalingen worden vervangen door bepalingen die zo min mogelijk verschillen van de betreffende niet-verbindende bepalingen.

Aldus overeengekomen en ondertekend

&DigitaleHandtekening1;	&DigitaleHandtekening2;
Namens het dagelijks bestuur van de Regio Gooi en Vechtstreek,	
.....naam vermelden ---------- functienaam vermelden	.....naam Werknemer

Gedragscode Integriteit Mycorsa nr. 21.0004615

Inleiding
De gedragscode gaat over wat van een integere ambtenaar mag worden verwacht. Een ambtenaar moet zich gedragen als 'goed ambtenaar'. Maar wat is dat, je gedragen als een goed ambtenaar? Door kernwaarden te benoemen en gedragsregels te beschrijven wordt duidelijk wat die ambtelijke integriteit is. Er zijn gedragsregels die bepaalde handelingen verbieden of juist voorschrijven. De gedragsregels kunnen gezien worden als een instrument om te bepalen wat in een bepaalde situatie wel of niet kan. Dit geldt zowel voor situaties op het werk als in de privésfeer. Bij vragen of dilemma's wordt geadviseerd om het gesprek met collega's, leidinggevende of de vertrouwenspersoon aan te gaan. Dit kan zorgen voor meer duidelijkheid en inzicht.

Onder integer gedrag verstaat de Regio Gooi en Vechtstreek een professionele, individuele verantwoordelijkheid om in al het handelen rekening te houden met rechten, belangen en het welzijn van belanghebbenden. De integere ambtenaar is betrouwbaar en professioneel, laat zich niet sturen door eigenbelang en eigengewin. Daarnaast kan hij zich verantwoorden voor de keuzes die hij in zijn werkzaamheden maakt, is hij zorgvuldig en gaat hij respectvol om met collega's, inwoners en andere partijen. De integere ambtenaar handelt altijd met oog voor het publieke belang. Ook van de Regio Gooi en Vechtstreek als werkgever mag integer gedrag worden verwacht. Als werkgever is zij verantwoordelijk voor het scheppen van een veilige cultuur. Hierbij wordt goed gedrag beloond en wordt opgetreden tegen onoorbaar gedrag. Zij neemt de verantwoordelijkheid voor het beschermen van de werknemer tegen verleidingen. Want met elkaar zorgen we voor een integere organisatie.

Reikwijdte
De gedragscode is van toepassing op alle werknemers die werken bij Regio Gooi en Vechtstreek. Onder werknemer wordt in dit verband verstaan: (1) de werknemer in dienst van de Regio Gooi en Vechtstreek en (2) personen die (betaalde of onbetaalde) werkzaamheden voor de Regio Gooi en vechtstreek verrichten, anders dan op basis van een arbeidsovereenkomst.

1. Kernwaarden
Integriteit is een belangrijk onderdeel van het professioneel functioneren van een ambtenaar. Een aantal kernwaarden staan binnen de organisatie voorop. Deze waarden dienen als kapstok om de regels, procedures en beginselen rondom integer gedrag als werknemer van de Regio Gooi en Vechtstreek aan op te hangen.

a. Betrouwbaarheid
Op een ambtenaar moet men kunnen rekenen. Die houdt zich aan zijn afspraken. Kennis en informatie waarover een ambtenaar uit hoofde van zijn functie beschikt, wendt hij aan voor het doel waarvoor die zijn gegeven.

b. Dienstbaarheid
Het handelen van een ambtenaar is altijd en volledig gericht op het belang van de Regio Gooi en Vechtstreek en op de organisaties en burgers die daar onderdeel van uit maken.

c. Functionaliteit
Het handelen van een ambtenaar heeft een herkenbaar verband met de functie die hij vervult.

d. Onafhankelijkheid
Het handelen van een ambtenaar wordt gekenmerkt door onpartijdigheid. Dat wil zeggen dat geen vermenging optreedt met oneigenlijke belangen en dat ook iedere schijn van een dergelijke vermenging wordt vermeden.

e. Openheid
Het handelen van een ambtenaar is transparant, zodat optimale verantwoording mogelijk is. De controlerende organen moeten volledig inzicht hebben in het handelen van de ambtenaar en zijn beweegredenen daarbij.

f. Zorgvuldigheid

Het handelen van een ambtenaar is zodanig dat hij alle organisaties en burgers op gelijke wijze en met respect bejegent. De ambtenaar weegt belangen van partijen op correcte wijze af.

De kernwaarden zijn het fundament voor het gedrag als goed ambtenaar. Onderdelen die daarin genoemd zijn komen terug in de onderstaande gedragsregels.

2. Goed ambtenaarschap

'Goed ambtenaarschap' verwijst naar de verplichting je als ambtenaar te gedragen 'zoals een goed ambtenaar betaamt'. Deze verplichting is neergelegd in artikel 6 Ambtenarenwet 2017 en volgt ook uit artikel 7:611 van het Burgerlijk Wetboek. Daarnaast legt de ambtenaar de eed of de belofte af. Een persoon die niet op basis van een arbeidsovereenkomst of onbetaald werken bij werkgever tekenen een integriteitsverklaring (*bijlage 1*). Deze verklaring gaat over de omgang met informatie, bedrijfsmiddelen en omgangsvormen.

Werknemers worden geacht bij te dragen aan een prettig en veilig werkklimaat, waarin respectvol met elkaar wordt omgegaan. Ook buiten werktijd kan je als werknemer gezien worden door een ander als 'iemand die bij Regio Gooi en Vechtstreek werkt'.

Gedragsregels

- Je beseft dat je onderdeel bent van de overheid. Je dient het algemeen belang en met je handelen versterk je het vertrouwen in de overheid.
- Houd je aan de wettelijke voorschriften en aan algemeen aanvaarde gedragsregels. Je discrimineert niet en verleent geen voorkeursbehandelingen.
- Je hebt respect voor de eigenheid, zelfstandigheid, zelfbeschikkingsrecht en persoonlijke levenssfeer van inwoners, collega's en externen, zowel in verbaal als non-verbaal gedrag.
- Je gaat verantwoord om met middelen van werkgever (gelden, diensten, goederen, kennis). Je vermijdt het maken van onnodige kosten.
- Je beïnvloedt geen geldstromen voor eigen gewin die voor werkgever zijn (fraude).
- Je onthoudt je van ongewenste omgangsvormen - zoals seksuele intimidatie, agressie, geweld en discriminatie. Je bent alert op signalen, misstanden of incidenten bij collega's en in de werksituatie.
- Je dient je representatief en zo te kleden dat het passend is bij de boodschap die werkgever wil uitstralen. Dit betekent dat er geen statement wordt gemaakt voor politieke of religieuze uitlatingen of anderszins. De algemeen directeur of leidinggevende beslist in hoeverre de kleding passend is.
- Je houdt je aan de kledingvoorschriften die horen bij je functie. Draag de aan jou verstrekte veiligheidskleding en volg de veiligheidsregels en voorschriften op.
- Op de werkplek wordt geen alcohol gedronken. Je gebruikt geen alcohol en/of drugs tijdens de uitoefening van je functie (inclusief de pauzetijd). Je schaft tijdens de uitoefening van je functie (inclusief pauzetijd) geen alcohol en/of drugs aan en je bent tijdens de uitoefening van je functie (inclusief pauzetijd) niet onder invloed van alcohol en/of drugs.
- Je maakt je niet schuldig aan vandalisme en vernielt geen eigendommen van werkgever.
- Je mag niet onbevoegd of zonder opdracht van je leidinggevende een dienstvoertuig besturen.

Meer weten? Lees de *Regeling eed of belofte*

3. Vertrouwelijk omgaan met informatie

Het vertrouwelijk omgaan met gevoelige informatie waarborgt de betrouwbaarheid en de geloofwaardigheid van de overheid. Iedereen moeten er op kunnen vertrouwen dat hun privacy wordt gerespecteerd. In veel gevallen werken wij met (bijzondere) persoonsgegevens van inwoners. Het is van groot belang dat wij als organisatie en als individuele werknemer zorgvuldig omgaan met deze informatie. Per specifieke handeling moet de afweging worden gemaakt welke informatie noodzakelijk is. Voorop staat dat het altijd uitlegbaar moet zijn waarom bepaalde informatie is geraadpleegd. Daarnaast dienen wij ons te houden aan de regelgeving over het omgaan met informatie en privacy.

Gedragsregels

- Ga binnen de muren van werkgever zorgvuldig om met (vertrouwelijke) informatie.
- Laat geen privacygevoelige documenten onbeheerd achter. Zorg ervoor dat stukken met vertrouwelijke gegevens veilig zijn opgeborgen als je een werkplek verlaat en zorg ervoor dat je computer netjes is afgesloten.
- Gebruik de toegang tot privacygevoelige informatie enkel en alleen voor het doel waarvoor het is bestemd en wanneer dit voor jouw werkzaamheden noodzakelijk is.
- Je gebruikt financiële informatie en voorkennis van beleid voor de uitoefening van je functie en niet voor andere doeleinden.
- Je 'lekt' geen vertrouwelijke informatie vanuit werkgever naar buiten.
- Je mag geen informatie aan de media verstrekken zonder toestemming van de algemeen directeur.
- Informatie waarover het dagelijks bestuur of algemeen bestuur een geheimhoudingsplicht heeft opgelegd houd je geheim.

4. Nevenwerkzaamheden en financiële belangen

Wanneer een werknemer een functie vervult of gaat vervullen die een raakvlak heeft met de regionale taken, dient de werknemer dit te melden. Het maakt niet uit of het om een betaalde of onbetaalde activiteit gaat. Een raakvlak is in elk geval aanwezig als je werkzaamheden verricht voor een organisatie, instantie of bedrijf dat op een of andere manier banden heeft met werkgever. Na melding van de activiteit/ werkzaamheden wordt er getoetst of er voor werkgever risico's kunnen kleven aan de nevenwerkzaamheden. De toestemming of afwijzing wordt in het personeelsdossier opgenomen. In sommige gevallen zullen risico's ondervangen kunnen worden door daar met elkaar afspraken te maken. Is dat niet mogelijk, dan is ook denkbaar dat werknemer een geheel andere functie gaat uitoefenen of dat nevenactiviteiten verboden worden. Voorbeelden van nevenactiviteiten zijn bestuursfuncties, commissariaten, vrijwilligerswerk, een eigen bedrijf en vennoot- of aandeelhouderschap. Voorbeelden van nevenfuncties en andere privé-activiteiten die niet samengaan met een functie bij Regio Gooi en Vechtstreek:

- In je vrije tijd ben je als barkeeper regelmatig tot laat aan het werk en dit heeft zijn weerslag op de productiviteit overdag;
- Je geeft vanuit een eigen bedrijf adviezen aan inwoners/cliënten, waar je zelf of een collega vervolgens een oordeel over moet uitspreken;
- Je neemt privé deel aan ethisch of politiek omstreden activiteiten;
- Jij of jouw partner hebben financiële belangen in een organisatie waar je ook als werknemer mee te maken hebt.

Belangenverstrengeling kan zich op allerlei manieren voordoen. Bij de beoordeling van de risico's van nevenwerkzaamheden kunnen enkele vragen behulpzaam zijn.

- Is er verwevenheid met het functionele beleidsterrein?
- Bestaat er een risico dat er informatie wordt gebruikt?
- Kunnen er persoonlijke confrontaties in de functie plaatsvinden?
- Hoe is de reputatie van de organisatie, het bedrijf of de branche?
- Hoe zal de buitenwereld tegen de combinatie van functies aankijken?
- Wat is de tijdsbelasting van de nevenwerkzaamheden?

Gedragsregels

- Vraag toestemming voor het uitoefenen van een nevenfunctie of nevenwerkzaamheden. Dit ongeacht het aantal uren.
- Je mag niet zonder toestemming betrokken zijn bij een onderneming, die een bedrijf uitoefent dat aan de beoordeling of toezicht van werkgever is onderworpen.
- Als je een functie vervult waaraan in het bijzonder het risico van financiële belangenverstrengeling of het risico van oneigenlijk gebruik van koersgevoelige informatie verbonden is, geef dan je financiële belangen of bezit van transacties in effecten op, die de belangen van de dienst, voor zover deze in verband staan met je functievervulling, kunnen raken.

- Je mag geen financiële belangen hebben, effecten bezitten en transacties in effecten te verrichten waardoor de goede vervulling van je functie of de goede functionering van de openbare dienst, voor zover deze in verband staat met je functievervulling, niet in redelijkheid zou zijn verzekerd.
- Persoonlijke belangenverstrengeling of de schijn van belangenverstrengeling is niet toegestaan. Meld een eventueel conflict tussen belangen bij je leidinggevende en bespreek eventuele twijfelgevallen.
- Nevenwerkzaamheden kunnen verboden worden wanneer deze in strijd zijn met artikel 8 van de ambtenarenwet 2017.

Meer weten? Lees de *Regeling nevenwerkzaamheden en financiële belangen.*

5. Aannemen van geschenken en gelden

Als werknemer handel je onafhankelijk en onpartijdig. Geef geen voorkeursbehandelingen en vermijdt ook de schijn daarvan. Er wordt geen geld aangenomen en geschenken worden geweigerd tijdens het onderhandelingsproces of lopende de procedure (met uitzondering van geschenken met een 'symboolfunctie').

Gedragsregels

- Accepteer een geschenk alleen als je onafhankelijke opstelling tegenover de gever niet wordt beïnvloed. Ga na of acceptatie van het geschenk verplichtingen schept voor de toekomst en vraag jezelf af hoe de buitenwereld zou kunnen aankijken tegen het aannemen van het geschenk. In veel gevallen levert dit geen probleem op. Denk aan een fles wijn voor een verrichte presentatie, een ceremonieel aan je overhandigd rapport van een bureau of aan bedrijfsattenties, zoals kalenders, pennen, muismatten en hebbedingetjes. Dergelijke geschenken zijn bedoeld als blijk van waardering voor een specifieke inspanning of de goede samenwerkingsrelatie en hoef je niet te melden.
- Een geschenk met een waarde van boven de € 50,- accepteer je niet.
- Aanbiedingen voor privé-werkzaamheden, kortingen op privé-goederen en andere gunsten accepteer je niet.
- Een geschenk dat je hebt gekregen of aangeboden krijgt, meld je bij je leidinggevende. De geschenken, gunsten of gelden zijn eigendom van werkgever. Je leidinggevende bepaalt wat er met het geschenk gebeurt.
- Geld wordt nooit aangenomen, net als geschenken die op je thuisadres worden geleverd. Is een geschenk toch thuis geleverd, bespreek de bestemming met je leidinggevende.
- Je accepteert geen geldbedragen voor verrichte werkzaamheden. Als afgesproken is dat een derden betaalt voor de werkzaamheden, dan gebeurt dat door een factuur van werkgever.
- Vanzelfsprekend vraag je nooit gunsten voor jezelf aan derden.
- In een onderhandelingsfase wordt er nooit een geschenk aangenomen, ook niet als het geschenk een waarde van minder dan € 50,-- vertegenwoordigt.

6. Uitnodigingen voor reizen, congressen, evenementen en diners

De aanwezigheid van werknemers bij bijeenkomsten en evenementen zal doorgaans een directe functionele betekenis hebben voor werkgever: het profileren van werkgever, het delen van ervaringen, het opdoen van kennis, de mogelijkheid waardevolle contacten te leggen of te onderhouden. Ontbreekt die betekenis, dan wordt de uitnodiging afgeslagen.

Als een werknemer wordt uitgenodigd om te spreken op een symposium zullen er, net als bij nevenactiviteiten, afspraken moeten worden gemaakt over de vraag of dat namens werkgever dan wel op persoonlijke titel gebeurt en of het tijdens dan wel buiten werktijd plaatsvindt. Voor een lezing op persoonlijke titel onder werktijd moet verlof gevraagd worden. Voor een lezing namens werkgever mag de medewerker geen geldelijke beloning aanvaarden.

Gedragsregels

- Beoordeel of een uitnodiging relevant is voor werkgever en bespreek de uitnodiging met je leidinggevende.

- Reis niet op kosten van derden. Als deelname aan een reis functioneel is, dan is er sprake van een dienstreis en gelden de algemene regels: er is toestemming nodig van je leidinggevende en de kosten zijn voor werkgever.
- Je neemt verantwoordelijkheid bij informele contacten met derden, zoals recepties en etentjes waar alcohol wordt geschonken. Zorg dat je 'nee' kunt blijven zeggen als het 'nee' moet zijn.

7. Persoonlijk gebruik goederen of diensten

Alle zaken binnen werkgever worden bekostigd met publieke middelen en zijn bestemd voor regionale doeleinden. Daar gaan wij verantwoord mee om. Dit is dan ook de basis voor de regels rondom het gebruik van bedrijfshulpmiddelen, declaraties, kosten van afscheid van werknemer, ons opleidingsbeleid en ons inkoopbeleid of een dienstauto. Ambtelijke integriteit houdt in dat iedereen die werkzaamheden verricht bij werkgever zich ervan bewust is dat hij of zij, ieder in de eigen functie, een grote publieke instelling vertegenwoordigt die het algemeen belang van velen moet behartigen. Dat vraagt dat de werknemer zijn of haar taak verricht op een professionele, verantwoorde en zorgvuldige manier, met aandacht voor dienstbaarheid en de vereiste vertrouwelijkheid.

Gedragsregels

- Je mag geen goederen of diensten van werkgever gebruiken voor privédoeleinden, tenzij je daar toestemming van je leidinggevende voor hebt gekregen.
- Je beheert de aan je beschikbaar gestelde bedrijfsmiddelen 'met goed werknemerschap'.
- Je declareert alleen kosten die je hebt gemaakt.
- Verantwoord gebruik van de middelen van werkgever betekent ook het naleven van de regelingen in het personeelshandboek en de Cao SGO, waaronder de regels met betrekking tot werktijden, ziekte en verlof.
- Je mag geen diensten laten verrichten door collega's in je eigen belang.
- Het is niet toegestaan om via werkgever materialen te bestellen die bestemd zijn voor privé doeleinden.
- Je mag geen kantoorartikelen, verbruiksgoederen of andere eigendommen van werkgever wegnemen of mee naar huis nemen, zonder toestemming van werkgever.
- Je neemt goederen dan wel afvalstoffen die door derden aan werkgever worden aangeboden niet mee, verhandelt deze niet en verkoopt deze niet door.
- Je maakt geen misbruik van technische installaties en voertuigen waarbij personen of materieel in gevaar kunnen komen of schade kan ontstaan (overbruggen van veiligheden).

8. Gebruik telefoon, internet en e-mail

Voor het gebruik van je telefoon, internet en e-mail gelden er regels. Het uitgangspunt is dat internet, e-mail en je telefoon gebruikt wordt voor je werkzaamheden voor werkgever. Dit geldt voor het internetten op locaties, maar ook op de aan jou beschikbaar gestelde apparatuur en je e-mailaccount (benaderd via apparatuur van werkgever of eigen digitale apparatuur). Het is belangrijk dat je in alle openheid laat zien wat je doet. En vraag je je af of je een grens passeert, bespreek het met je leidinggevende. In bepaalde gevallen, zoals bij een vermoeden van een integriteitsschending, het niet gedragen als een goed ambtenaar betaamt of langdurige afwezigheid, is de werkgever gerechtigd om kennis te nemen van de e-mailbox van het zakelijke account van de werknemer.

Gedragsregels voor werknemers

- Het is niet toegestaan sites te bezoeken die pornografisch, racistisch dan wel terroristisch materiaal bevatten of om anderszins dergelijk materiaal te vergaren en of te verspreiden.
- Je mag het e-mailsysteem beperkt gebruiken voor het ontvangen en versturen van niet-zakelijke, persoonlijke mail berichten zowel intern als extern, mits dit niet storend is voor hun dagelijkse werkzaamheden.
- Het registreren van gegevens die tot een persoon herleidbaar zijn wordt tot een minimum beperkt. Hierbij wordt gestreefd naar een maximale bescherming van de privacy van werknemer op de werkplek.

Meer weten? Lees het *Reglement gebruik telefoon, internet en e-mail*

9. Gebruik Social Media

Bijna iedereen gebruikt tegenwoordig wel één of meerdere social media. Als privé persoon of voor je werk. Het verschil tussen die twee kan voor de buitenwereld in bepaalde gevallen niet helemaal duidelijk zijn.

Gedragsregels voor werknemers

- Zet social media in om mensen aan betrouwbare informatie te helpen.
- Wees open en transparant over wie je bent. Als je reageert vanuit je rol of functie bij werkgever, zet er dan ook bij dat je werkt voor werkgever en wat je functie is.
- Geef duidelijk aan of iets je privémening is of dat je reageert vanuit je rol/functie. Wees je ervan bewust dat ook jouw privémening kan afstralen op werkgever.
- Overleg bij twijfel met de communicatieadviseur of je leidinggevende.
- Je deelt geen vertrouwelijke informatie op social media.
- Plaats geen racistische of ongepaste opmerkingen
- Pas geen censuur toe op de mening van anderen
- Werknemers vallen elkaar in het openbaar niet af. Heb je iets op je hart? Ga dan het gesprek persoonlijk of via telefoon/e-mail met je collega of je leidinggevende.

Meer weten? Lees de *Gedragscode Social Media*.

10. Belangen van familieleden, vrienden en ex-collega's

Werknemers gedragen zich onpartijdig en gaan dus niet in op verzoeken van familie of vrienden om 'iets te regelen'. Het inhuren van een ex-werknemer heeft voordelen maar ook nadelen. Een ex-werknemer kan ook misbruik maken van kennis en contacten die hij tijdens de functie bij werkgever heeft opgedaan. Dit kan vervolgens de geloofwaardigheid en integriteit van werkgever schaden. Soms worden bij uitdiensttreding van een collega die voor zichzelf begint afspraken gemaakt over toekomstige opdrachten. Deze praktijken zijn concurrentievervalsend en kunnen de geloofwaardigheid en integriteit van de overheid aantasten.

Gedragsregels

- Wees alert op situaties in je werk waarin je met privérelaties te maken krijgt. Licht je leidinggevende in over aanvragen van offertes van vrienden, familie of bedrijven waarin familie of vrienden werken.
- Voorkom de schijn van vriendjespolitiek en behandel dergelijke aanvragen niet zelf.
- Volg bij het inhuren van ex-werknemers de juiste procedure voor inhuur en aanbesteding. Je moet kunnen motiveren waarom de inhuur van een ex-werknemer als zelfstandige nodig en verantwoord is. Bespreek eventuele risico's met je leidinggevende.

11. Reageren op niet-integere zaken

Van werknemers wordt verwacht dat zij zich volgens deze code gedragen en collega's aanspreken op de overtreding ervan. Indien overtredingen van ernstiger aard zijn of indien het aanspreken van een collega niet helpt, kun je dit melden bij je leidinggevende. Je kunt er ook voor kiezen om integriteitsschendingen te melden bij de vertrouwenspersoon. De vertrouwenspersoon kan werknemers hierin bijstaan. Werknemers hebben het recht om zich vrij te voelen en misstanden intern aan te kaarten. Werknemers kunnen verschillende misstanden signaleren, bijvoorbeeld diefstal van goederen van werkgever door collega's, vriendjespolitiek door de leidinggevende, het achterhouden van informatie voor een bestuurder, luiheid of minimale inzet door collega's. Belangrijk is dat met deze aangelegenheden vertrouwelijk wordt omgegaan. Lekken naar de pers hierover is ongewenst.

Gedragsregels

- Je bent samen met al je collega's verantwoordelijk voor een open en integere cultuur waarin je daadwerkelijk met elkaar bespreekt wat het beste is om te doen. Daarbij is een andere mening of visie geaccepteerd, maar het is belangrijk dat je dat wel op respectvolle wijze met elkaar deelt.
- Afspraken worden nagekomen.
- Ongewenst gedrag zoals pesten, discriminatie, vloeken, roddelen, beledigen, aanstootgevend of (seksueel) intimiderend gedrag is onaanvaardbaar en wordt niet getolereerd.
- Je maakt geen misbruik van macht en positie.

- Spreek eerst je collega aan bij niet-integer of ongewenst gedrag. Is dat niet mogelijk of leidt dat niet tot het gewenste resultaat bespreek dit dan met je leidinggevende of de algemeen directeur. Vermoeden van (ernstige) integriteitsschendingen, fraude of corruptie meld je bij je leidinggevende. Werkgever is verplicht om een reactie te geven op je melding. Wil je niet dat bekend wordt dat je de misstand aankaart, dan kun je een melding doen via de vertrouwenspersoon. Alleen de vertrouwenspersoon is dan op de hoogte van je identiteit.

Meer weten? Lees de *Regeling ongewenst gedrag, melding vermoeden misstanden en vertrouwenspersoon*

12. De leidinggevende draagt het integriteitbeleid uit

De leidinggevende bevordert de integriteitsbewustwording van werknemers en ondersteunt hen in het omgaan met gevoelige en risicovolle situaties. De leidinggevende maakt ongewenst gedrag van een werknemers bespreekbaar, corrigeert en treft indien nodig maatregelen.

Gedragsregels

- Als leidinggevende geef je het goede voorbeeld.
- Je bent open over je manier van werken. Je bent aanspreekbaar op je werkwijze en je houding naar werknemers.
- Je bespreekt twijfels en vragen over integriteit en stimuleert werknemers om dat zelfde te doen.
- Je bent alert op risicogevoelige situaties waarin werknemers terecht kunnen komen en draagt bij aan hun weerbaarheid.
- Je spreekt werknemers aan op dubieus gedrag, maakt afspraken en treft indien nodig maatregelen.

13. Wettelijke verplichtingen gezondheidszorg

Wet op de Beroepen in de Individuele Gezondheidszorg (BIG)

De medische en paramedische werknemers (artsen, verpleegkundigen, doktersassistenten, en screeners) gedragen zich en handelen overeenkomstig de formuleringen gesteld in de Wet BIG, in het bijzonder de passages die handelen over bevoegdheid, deskundigheid en bekwaamheid. Artsen en verpleegkundigen vallen onder de wet BIG en dienen bij indiensttreding een kopie van hun registratie in het BIG-register te overleggen. De inspanningen voor herregistratie zijn de verantwoordelijkheid van de artsen en verpleegkundigen.

Wet geneeskundige behandelingsovereenkomst (WGBO)

Werknemers van het organisatieonderdeel RVE GGD gaan een behandelovereenkomst aan met de cliënt in de zin van de WGBO. Dat betekent dat zowel de werknemer als de cliënt rechten en plichten hebben. Het is de plicht van de werknemer informatie te verstrekken, een medisch dossier bij te houden en de privacy van de cliënt te bewaren.

Wet medisch-wetenschappelijk onderzoek

Bij het uitvoeren van cliëntgebonden of cliëntgerelateerd onderzoek moet nagegaan worden of het onderzoek onder de reikwijdte valt van de Wet medisch-wetenschappelijk onderzoek. Dat is het geval als naast de onderzoeksdoelstellingen ook wetenschappelijke doelstellingen aan een enquête worden verbonden. Indien dit het geval is, dient het onderzoek getoetst te worden door een erkende medisch-ethische commissie.

14. Betrokkenheid bij casuïstiek

Casuïstiek waarbij werknemers direct of indirect betrokken zijn, wordt voor behandeling ondergebracht bij een andere regio, tenzij daar eigenlijk geen praktische mogelijkheden voor zijn. Dat geldt bijvoorbeeld voor meldingen bij Veilig Thuis waar werknemers bij zijn betrokken, of voor casuïstiek in het kader van de forensische geneeskunde (lijkschouw, arrestantenzorg). Het geldt in principe niet voor kinderen die in zorg zijn bij Jeugd en Gezin, of voor meldingen in het kader van de infectiezektebestrijding.

15. Sancties

In situaties waarin vastgesteld wordt dat een werknemer niet-integer heeft gehandeld, wordt dit beschouwd als strijdig met het bepaalde in artikel 6 Ambtenarenwet 2017. In dit artikel wordt beschreven dat een ambtenaar gehouden is zich te gedragen als een goed ambtenaar. Niet-integer gedrag wordt bestraft op een wijze als opgenomen in het Sanctiebeleid. Het openbaar maken van een overtreding zonder verdere acties kan in dit verband ook als sanctie worden gezien. Voor werkgever zijn ook personen werkzaam die geen arbeidsovereenkomst met de organisatie hebben. Als deze personen niet-integer handelen, treft werkgever passende maatregelen. Hiervoor wordt per individueel geval door werkgever een beslissing genomen. Daarbij besluit werkgever ook of er, al dan niet middels een civiele procedure, een schadevergoeding wordt gevorderd. Bij ernstige integriteitschendingen zal werkgever een onafhankelijk onderzoek laten instellen. Welke sanctie er wordt opgelegd, hangt af van verschillende omstandigheden. De aard en de ernst van de overtreding spelen een rol. Maar ook is van belang of het een eerste overtreding betreft of dat je al vaker in de fout gegaan bent.

Bijlage 1 Integriteitsverklaring

Hierbij verklaart ondergetekende kennis te hebben genomen van de regels met betrekking tot integriteit zoals vastgelegd in de Gedragscode Integriteit.

Ten overstaan van de manager van organisatieonderdeel _____ verklaar ik het volgende:

1. Ik heb noch direct noch indirect, in welke vorm dan ook, valse informatie verstrekt in verband met het verkrijgen van mijn overeenkomst.

2. Ik heb voor het verkrijgen van mijn overeenkomst aan niemand iets geschonken of beloofd en dat zal ik ook niet gaan doen.

3. Ik zal recht doen aan en handelen in overeenstemming met de grondwet en andere wetten.

4. Ik zal mij inzetten voor het welzijn en de rechten van alle deelnemende gemeenten van de Regio Gooi en Vechtstreek.

5. Ik zal in contacten met inwoners en vertegenwoordigers van bedrijven en maatschappelijke organisaties een betrouwbare vertegenwoordiger van de Regio Gooi en Vechtstreek zijn.

6. Ik zal onpartijdig handelen en democratische beginselen en procedures respecteren.

7. Ik ben loyaal ten opzichte van de bestuursorganen van de Regio Gooi en Vechtstreek en het door hen vastgestelde beleid.

8. Ik zal geen misbruik maken van mijn positie.

9. Ik zal zorgvuldig omgaan met informatie.

10. Ik zal handelen in overeenstemming met de geldende Gedragscode Integriteit.

Het bovenstaande verklaar ik,

_____(voorletters, voorvoegsel(s) en achternaam)

__(handtekening)

Bussum_____(datum)

Regio
Gooi en Vechtstreek

Integriteitsverklaring

Hierbij verklaart ondergetekende kennis te hebben genomen van de regels met betrekking tot integriteit zoals vastgelegd in de Gedragscode Integriteit.

Ten overstaan van de manager van organisatieonderdeel RVE GGD, team AGZ/Corona verklaar ik het volgende:

1. Ik heb noch direct noch indirect, in welke vorm dan ook, valse informatie verstrekt in verband met het verkrijgen van mijn overeenkomst.

2. Ik heb voor het verkrijgen van mijn overeenkomst aan niemand iets geschonken of beloofd en dat zal ik ook niet gaan doen.

3. Ik zal recht doen aan en handelen in overeenstemming met de grondwet en andere wetten.

4. Ik zal mij inzetten voor het welzijn en de rechten van alle deelnemende gemeenten van de Regio Gooi en Vechtstreek.

5. Ik zal in contacten met inwoners en vertegenwoordigers van bedrijven en maatschappelijke organisaties een betrouwbare vertegenwoordiger van de Regio Gooi en Vechtstreek zijn.

6. Ik zal onpartijdig handelen en democratische beginselen en procedures respecteren.

7. Ik ben loyaal ten opzichte van de bestuursorganen van de Regio Gooi en Vechtstreek en het door hen vastgestelde beleid.

8. Ik zal geen misbruik maken van mijn positie.

9. Ik zal zorgvuldig omgaan met informatie.

10. Ik zal handelen in overeenstemming met de geldende Gedragscode Integriteit.

Het bovenstaande verklaar ik,

_____(voorletters, voorvoegsel(s) en achternaam)

_____(handtekening)

_____(plaatst) _____(datum)

Van:
Verzonden:
Aan:
Onderwerp: VOG

Opvolgingsmarkering: Opvolgen
Markeringsstatus: Gemarkeerd

Artikel 10 Overige voorwaarden
3. Voor de uitvoering van de dienstverlening zoals omschreven in artikel 2 en overeenkomstig artikel 30 lid 4 van Algemene inkoopvoorwaarden, garandeert Contractant dat hij/zij in het bezit is van een geldige Verklaring Omtrent Gedrag (VOG) als bedoeld in artikel 28 van de Wet justitiële en strafvorderlijke gegevens (WJSG), en overlegt deze verklaring(en) aan Opdrachtgever.

4. In navolging van artikel 30 lid 2 van de Algemene inkoopvoorwaarden stelt Opdrachtgever, voordat de uitvoering van de dienstverlening zoals omschreven in artikel 2 een aanvang neemt, de identiteit vast aan de hand van een geldig identiteitsbewijs van Contractant.
Het identiteitsbewijs (paspoort of identiteitskaart, geen rijbewijs) dient door Contractant persoonlijk te worden overlegd aan Opdrachtgever.

5. Opdrachtgever verstrekt aan Contractant de 'gedragscode integriteit' inclusief een integriteitsverklaring. Contractant dient te handelen in overeenstemming met deze gedragscode en verklaart dit door persoonlijke ondertekening van de integriteitsverklaring.

Groetjes

Regio
Gooi en Vechtstreek

De Regio blijft doorwerken tijdens de coronacrisis. Wie dat kan, doet dat thuis. Maar let op: voor cybercriminelen is deze crisis een kans om gevoelige data buit te maken. En een foutje is snel gemaakt, waardoor gevoelige gegevens op straat kunnen komen te liggen. Volg onderstaande richtlijnen en voorkom dat er gegevens over inwoners of collega's in verkeerde handen vallen.

Door het naleven van deze regels kunnen we zo zorgvuldig en zo veilig mogelijk thuis werken met middelen die door de Regio beschikbaar zijn gesteld (smartphone, laptop) of met eigen apparatuur.

1. Werk bij voorkeur met de middelen die door de Regio beschikbaar zijn gesteld, zoals iPhone, iPad en laptop;
2. Indien eigen apparatuur wordt gebruikt (computer, laptop, privételefoon), dan mag op de schijven hiervan geen bedrijfsinformatie en gevoelige (persoons)informatie worden opgeslagen;
3. Werk voor wat betreft vak-applicaties zoveel mogelijk binnen de beveiligde werkomgeving via Ericom Blaze. Kun je in je werk volstaan met enkel de mail dan is het dringend verzoek om dat zoveel mogelijk via webmail te doen;
4. Gebruik altijd je werkmailadres en werktelefoonnummer (indien beschikbaar) voor zakelijke communicatie;
5. Wees voorzichtig met het gebruik van (video)chatdiensten. Bellen en SMS is nog steeds het makkelijkst en veiligst. Over de mogelijkheden om online te vergaderen (waaronder videobellen) is al eerder een stappenplan gecommuniceerd waarin eerst naar de veiligste opties moet worden gekeken en pas in laatste instantie naar de minst veilige opties.
6. Bewaar het gebruikerswachtwoord om in je je laptop te komen niet op een briefje op of in de laptop maar leer het uit je hoofd;
7. Sla geen documenten lokaal op je laptop op, zeker niet als je huisgenoten van dezelfde laptop gebruik maken. Andersom: bescherm jezelf en je huisgenoten tegen het uitlekken van persoonlijke documenten als de laptop weer terug moet naar ICT.
8. Ga zorgvuldig om met mobiele apparatuur: niet onbeheerd achterlaten in bijvoorbeeld een vervoermiddel of een ruimte waarin andere personen aanwezig zijn;
9. Indien de werkplek wordt verlaten en er andere mensen in de woning aanwezig zijn, dien je Ericom Blaze (tijdelijk) af te sluiten;
10. Gegevens die je verwerkt namens de Regio zijn vertrouwelijk, dus niemand kijkt mee/luistert mee. Wees net als altijd extra voorzichtig met bijzondere persoonsgegevens, zoals medische gegevens;
11. Laat eventueel in bezit zijnde fysieke documenten van de Regio niet onbeheerd en berg ze goed op. Wil je ze vernietigen, neem ze dan t.z.t. weer mee naar de Regio en gooi ze in de daarvoor bestemde zilveren papiercontainers;
12. Neem geen fysieke documenten/dossiers met persoonsgegevens mee naar huis, tenzij het praktisch echt niet uitvoerbaar is om dit op een andere manier te doen, bijvoorbeeld door te digitaliseren/scannen. Desnoods maak je gebruik van een versleutelde USB-stick (te verkrijgen bij de ICT servicedesk);
13. Let op phishingmails/sms-jes. Dit zijn berichten die door kwaadwillenden aan mensen worden gestuurd om hen aan de hand van een actueel thema (zoals nu corona) te verleiden persoonlijke gegevens te verstrekken. Krijg je berichten die je niet verwacht of die van een onbekende afzender zijn? Klik dan niet op links in deze berichten, open geen bijlagen en vul geen gegevens in. Zie hierover ook dit eerdere bericht op de Binnenband;
14. Wees voorzichtig met het gebruik van cloud- of opslagdiensten, zeker wanneer deze gratis zijn. Want het zou kunnen dat zo'n dienst juist gratis is omdat de aanbieder je gegevens gebruikt voor andere doeleinden of omdat geen aandacht is besteed aan beveiliging.
15. Zorg dat je altijd goed bereikbaar bent voor je collega's (en externen/derden) voor vragen en overleg.
16. Probeer te voorkomen dat een datalek ontstaat met deze tips.
17. Neem je verantwoordelijkheid voor informatiebeveiliging als er toch iets fout gaat of als je verdachte zaken ziet en meld dit direct bij de ICT Service Desk (via (035) 692 62 00 of meldpuntdatalek@regiogv.nl) of maak een melding via de Binnenband.

GGD
Gooi en Vechtstreek

21 januari 2022

Onderwerp: Account sharing

Beste collega's,

Bij GGD GHOR Nederland is een security operations center (SOC) actief dat ieders activiteiten in CoronIT volgt. Bij verdachte of niet te plaatsen activiteiten worden wij hiervan op de hoogte gesteld en wordt hier onderzoek naar gedaan door het SOC. Helaas is gebleken dat dit team er niet voor niets is. Het verstrekken van QR codes zonder vaccinatie en opzoeken BN'ers is helaas iets wat in het land voorkomt.

We willen jullie er daarom nogmaals op wijzen dat je uitsluitend onder je eigen accounts mag werken. Dit geldt niet alleen voor CoronIT, maar ook voor je Regio account, HPZone enz. Dit is ter bescherming van jezelf; als iemand iets op jouw account doet wat niet is toegestaan dan is het lastig aan te tonen dat jij het niet was.

Als jullie integer om blijven gaan met de toegang tot gegevens die jullie hebben, dan hoeven jullie je geen zorgen te maken.

Groet,
Ook namens [redacted]

[redacted]

GGD Gooi en Vechtstreek | Postbus 251, 1400 AG Bussum
Burgemeester de Bordesstraat 80, 1404 GZ Bussum | T: (035) 692 62 22 | info@ggdgv.nl
KvK 32170415 | IBAN NL40 BNGH 0285 0321 94 | BIC BNGHNL2G | BTW NL 0019.37.194.B01

Security & Privacy

Privacy beleid regio
Het privacy beleid van de Regio Gooi en Vechtstreek is te vinden op de binnenband
Nb; De belangrijkste aandachtspunten verschijnen binnenkort per RVE – worden dan toegevoegd aan dit document.

Privacy beleid BCO Portaal/GGD Contact
Het privacy beleid van GGD Contact is te vinden op de Academy van GGD GHOR NL in de e-learning werken met GGD Contact - onderdeel 4 van hoofdstuk Beveiliging en Privacy.

Nb; De eerste keer dat je inlogt bij BCO Portaal zie je de kennisgeving dat je activiteiten gelogd worden. Om verder te gaan klik je op OK. Er wordt vastgelegd dat je akkoord bent met de monitoring en logging van je activiteiten in het BCO Portaal

Veilig thuiswerken
Richtlijnen voor veilig thuiswerken staan op de binnenband

Datalek
Signaleer je een datalek? meld dat dan direct via de binnenband en de teamcoördinator.

Privacy & Security Training.
De Privacy & Security training is te vinden via een beveiligde Microsoft teams form link en is een verplicht onderdeel van het inwerk traject. De E-learning bestaat uit drie onderdelen en 15 vragen.

1. Privacy & Security
2. Clean desk policy en datalek
3. BCO Security Rules

De belangrijkste vragen zijn:

- Voor wie geldt de Privacywetgeving?
- Wie moet de AVG naleven?
- Wat is de procedure voor het melden van een datalek?

Landelijke/Regionale werkinstructie.
Landelijke werkinstructies staan op de Academy van GGD GHOR NL en de dagcoördinatoren zetten actuele versies op de H:\schijf. De teamcoördinator verstuurt wekelijks updates van procedures in de weekmail.

Inwerkproces nieuwe BCO medewerkers

Algemeen
Nieuwe medewerkers starten bij voorkeur op woensdag
Nieuwe medewerkers starten bij voorkeur met 2 of meer personen.

Thuis afronden vóór eerste inwerkdag

- E-learning Bron & contactonderzoek bij Covid-19
- E-learning Bron & Contactonderzoek gespreksvoering
- Doorlezen Werkinstructie

Kantoor Bussum
Dag 1
Ochtend; starterstraining door [redacted] - Specifiek aandacht voor Security & Privacy
Middag; inwerken door vaste medewerker volgens vast document

Dag 2
Ochtend; Voltooien E-learning Privacy & Security
Middag; inwerken door vaste medewerker volgens vast document

Dag 3
Ochtend; Voltooien E-learning GGD Contact
Middag; inwerken door vaste medewerker volgens vast document

Opvolgende 2 weken; werkzaam op kantoor in Bussum

- Ontvangst van een druppel via [redacted]
- Ontvangst van laptop/mobiel via ICT
- Inlogcodes voor mail/HPzone lite/ Coron IT
- Evaluatie gesprek met [redacted]

Documenten/e-learnings vooraf

FUNCTIENAAM	VERPLICHTE SCHOLING voor start
Vaccinatie medewerker	https://landelijkeleeromgeving.nspoh.nl/login/index.php - E-learning COVID-19 vaccinatie - E-learning COVID-19 vaccins voorbereiden en toedienen - E-learning COVID-19 vaccinaties registreren in CoronIT - Regionaal handboek laatste versie inclusief medische lijn
Callcenter medewerker	- Document handige websites - Veel gebruikte telefoonnummers - Werkwijze Callcenter - Updates en werkafspraken
BCO medewerker	https://lci.rivm.nl/COVID-19-bco - Landelijke werkinstructie LCI
Teststraat medewerker	https://landelijkeleeromgeving.nspoh.nl/login/index.php - E-learning landelijke opleiding Bemonsteraars in de teststraat PCR test - E-learning CoronIT voor testen

Stappenplan E-learnings GGD GHOR NL

1. Ga naar de link: https://landelijkeleeromgeving.nspoh.nl/login/index.php
2. Klik op 'nieuw account maken'.
3. Voer je e-mailadres, voornaam, achternaam, wachtwoord en GGD Gooi en Vechtstreek in
4. Klik op 'maak mijn nieuwe account aan'.
5. Ga naar de inbox van je opgegeven e-mailadres. Check eventueel je SPAM.
6. Klik op de link in je e-mail of kopieer de link en plaats hem in de internetbalk.
7. Klik op 'ga door' en kies het juiste thema.
8. Selecteer de juiste training(en) en doorloop de e-learning(s) voor je eerste werkdag.

Gedragscode integriteit lezen en integriteitsverklaring invullen
Retour aan corona@ggdgv.nl en doorsturen naar po@regiogv.nl moet binnen zijn alvorens te kunnen starten op locatie

VOG (functieprofiel 45) moet binnen zijn alvorens te kunnen starten op locatie

Verder inwerkprocedure 'on the job' zodra inloggegevens bekend zijn kan op locatie gestart worden met inwerken.

- Privacy & Security
- CoronIT

Specifiek voor BCO

- HPZone/Lite
- BCO Portaal

GGD
Gooi en Vechtstreek

Richtlijnen voor veilig thuiswerken (versie 2.0)

De Regio blijft doorwerken tijdens de coronacrisis. Wie dat kan, doet dat thuis. Maar let op: voor cybercriminelen is deze crisis een kans om gevoelige data buit te maken. En een foutje is snel gemaakt, waardoor gevoelige gegevens op straat kunnen komen te liggen. Volg onderstaande richtlijnen en voorkom dat er gegevens over inwoners of collega's in verkeerde handen vallen.

Door het naleven van deze regels kunnen we zo zorgvuldig en zo veilig mogelijk thuis werken met middelen die door de Regio beschikbaar zijn gesteld (smartphone, laptop) of met eigen apparatuur.

1. Werk bij voorkeur met de middelen die door de Regio beschikbaar zijn gesteld, zoals iPhone, iPad en laptop;
2. Indien eigen apparatuur wordt gebruikt (computer, laptop, privételefoon), dan mag op de schijven hiervan geen bedrijfsinformatie en gevoelige (persoons)informatie worden opgeslagen;
3. Werk voor wat betreft vak-applicaties zoveel mogelijk binnen de beveiligde werkomgeving via Ericom Blaze. Kun je in je werk volstaan met enkel de mail dan is het dringend verzoek om dat zoveel mogelijk via webmail te doen;
4. Gebruik altijd je werkmailadres en werktelefoonnummer (indien beschikbaar) voor zakelijke communicatie;
5. Wees voorzichtig met het gebruik van (video)chatdiensten. Bellen en SMS is nog steeds het makkelijkst en veiligst. Over de mogelijkheden om online te vergaderen (waaronder videobellen) is al eerder een stappenplan gecommuniceerd waarin eerst naar de veiligste opties moet worden gekeken en pas in laatste instantie naar de minst veilige opties.
6. Bewaar het gebruikerswachtwoord om in je je laptop te komen niet op een briefje op of in de laptop maar leer het uit je hoofd;
7. Sla geen documenten lokaal op je laptop op, zeker niet als je huisgenoten van dezelfde laptop gebruik maken. Andersom: bescherm jezelf en je huisgenoten tegen het uitlekken van persoonlijke documenten als de laptop weer terug moet naar ICT.
8. Ga zorgvuldig om met mobiele apparatuur: niet onbeheerd achterlaten in bijvoorbeeld een vervoermiddel of een ruimte waarin andere personen aanwezig zijn;
9. Indien de werkplek wordt verlaten en er andere mensen in de woning aanwezig zijn, dien je Ericom Blaze (tijdelijk) af te sluiten;
10. Gegevens die je verwerkt namens de Regio zijn vertrouwelijk, dus niemand kijkt mee/luistert mee. Wees net als altijd extra voorzichtig met bijzondere persoonsgegevens, zoals medische gegevens;
11. Laat eventueel in bezit zijnde fysieke documenten van de Regio niet onbeheerd en berg ze goed op. Wil je ze vernietigen, neem ze dan t.z.t. weer mee naar de Regio en gooi ze in de daarvoor bestemde zilveren papiercontainers;
12. Neem geen fysieke documenten/dossiers met persoonsgegevens mee naar huis, tenzij het praktisch echt niet uitvoerbaar is om dit op een andere manier te doen, bijvoorbeeld door te digitaliseren/scannen. Desnoods maak je gebruik van een versleutelde USB-stick (te verkrijgen bij de ICT servicedesk);
13. Let op phishingmails/sms-jes. Dit zijn berichten die door kwaadwillenden aan mensen worden gestuurd om hen aan de hand van een actueel thema (zoals nu corona) te verleiden persoonlijke gegevens te verstrekken. Krijg je berichten die je niet verwacht of die van een onbekende afzender zijn? Klik dan niet op links in deze berichten, open geen bijlagen en vul geen gegevens in. Zie hierover ook dit eerdere bericht op de Binnenband;
14. Wees voorzichtig met het gebruik van cloud- of opslagdiensten, zeker wanneer deze gratis zijn. Want het zou kunnen dat zo'n dienst juist gratis is omdat de aanbieder je gegevens gebruikt voor andere doeleinden of omdat geen aandacht is besteed aan beveiliging.
15. Zorg dat je altijd goed bereikbaar bent voor je collega's (en externen/derden) voor vragen en overleg.
16. Probeer te voorkomen dat een datalek ontstaat met deze tips.
17. Neem je verantwoordelijkheid voor informatiebeveiliging als er toch iets fout gaat of als je verdachte zaken ziet en meld dit direct bij de ICT Service Desk (via (035) 692 62 00 of meldpuntdatalek@regiogv.nl) of maak een melding via de Binnenband.

[redacted]

4 maart 2021

Melden datalekken

Wat is een datalek?
We spreken van een datalek als sprake is van toegang tót of vernietiging, wijziging of vrij komen ván persoonsgegevens zonder dat dit de bedoeling is. Ook als redelijkerwijs niet kan worden uitgesloten dat dit gebeurd is, is sprake van een datalek. Een persoonsgegeven betreft informatie die direct over iemand gaat óf naar deze persoon te herleiden is. Voorbeelden van persoonsgegevens zijn het burgerservicenummer, naam, adres en geboortedatum, maar ook medische informatie en geloofsovertuiging. Meest in het oog springend zijn datalekken naar derden buiten onze organisatie. Maar ook tussen collega's onderling kan sprake zijn van lekken. Denk hierbij aan de onbedoelde inzage in iemands personeelsdossier door een onbevoegde. Datalekken ontstaan (ook bij de Regio) in de meeste gevallen door handelen van medewerkers en niet door onvoldoende technische beveiliging. Meest voorkomend zijn de gevallen waarin derden die geen toegang tot die gegevens mogen hebben, toch toegang hebben gekregen. Vaak gaat het om digitale bestanden die per ongeluk beschikbaar zijn of zijn toegestuurd aan onbevoegden. Maar een verloren of gestolen geprint dossier is evengoed een datalek.

Voorbeelden van mogelijke datalekken zijn:

- kwijtraken van een brief met persoonsgegevens bij de post
- verzenden van persoonsgegevens naar een verkeerd e-mailadres
- versturen van te veel (onnodige) gegevens aan derden
- kwijtraken van een onbeveiligde USB-stick met persoonsgegevens
- diefstal van een laptop, iPad e.d. met persoonsgegevens
- een malware besmetting

Tips voor voorkomen datalekken:

- Laat je spullen niet onbeheerd op je bureau achter.
- Laat je laptop niet in de auto achter.
- Lock je computer met 'Windows vlaggetje L' als je je werkplek verlaat
- Bewaar persoonsgegevens niet langer dan nodig. Wat je niet hebt, kun je ook niet lekken. Verwijder de databestanden die je niet meer nodig hebt. Denk hierbij ook aan papieren documenten, gooi deze weg in de papierkliko op het werk en níet thuis bij het oud papier.
- Deel alleen gegevens die voor de ontvanger noodzakelijk zijn om het werk uit te voeren. Denk er bij het versturen van Excel documenten aan dat je alleen de relevante kolommen/werkbladen meestuurt.
- Controleer vóór het versturen nog even het opgestelde mailtje:
  o Kloppen de geadresseerden?
  o Heb je de juiste bijlage bijgevoegd?
  o Is het gevoelige informatie die je naar buiten de organisatie verstuurt? In dat geval gebruik je Zivver.
- Wees alert bij de printer:
  o papier op? Loop dan niet weg maar vul direct het papier bij, anders komt je opdracht er mogelijk bij een ander uit.
  o storing tijdens het printen? Geef dan aan ICT Servicedesk door dat de printopdracht gevoelige gegevens bevat.

Wat te doen bij een datalek?

- Merk je dat er mogelijk sprake is van een datalek dan moet je dit direct melden bij ICT Servicedesk. Dat kan telefonisch: **(035) 692 62 00**, via meldpuntdatalek@regiogv.nl of gebruik het formulier hieronder. De collega's van ICT ondernemen dan actie.
  Vervolgens beoordeelt het Team Privacyincidenten (nieuwe naam!) of het daadwerkelijk een datalek is en of het datalek extern gemeld moet worden bij de toezichthouder, de Autoriteit Persoonsgegevens, en eventueel ook bij degene wiens gegevens het betreft. Dit is het geval als er een (hoog) risico voor personen is.

Het is niet erg om een datalek intern te melden. De organisatie wordt er vaak scherper van. Bij twijfel schroom niet en meld het mogelijke datalek! De handreiking 'Beoordeling datalekken AVG en 'Memo Interne procedure afhandeling meldingen datalekken AVG' staan op de Binnenband of zijn op te vragen bij [redacted] (corona@ggdgv.nl)

Tips ter voorkoming van datalekken

Een datalek ontstaat gemakkelijk bij onachtzaamheid. Hier vind je tips om dat te voorkomen.

In het algemeen
De onderstaande tips vinden vooral hun oorsprong in onze Bruikleenovereenkomst. Het is hoe dan ook verstandig deze nog eens door te lezen en je te houden aan de daarin gestelde richtlijnen.

Zakelijke apparatuur in bruikleen?
Het spreekt voor zich dat je zorgvuldig omgaat met apparatuur die door de werkgever aan jou in bruikleen is gegeven. Beschadiging en verlies/diefstal die jou is aan te rekenen, zijn voor eigen rekening.

Gebruik je een iPad, iPhone of andere Smartphone?
Zorg ervoor dat het apparaat met een pincode is beveiligd. Bij nieuwere typen van dergelijke apparaten kan ook een vingerafdruk of gezichtsherkenning worden ingesteld. Maak ook op je privé-smartphone gebruik van dergelijke beveiligingsmiddelen, zeker als je daarop ook je zakelijke e-mail synchroniseert.

iPad of iPhone verloren of gestolen?
Een verloren of gestolen iPad of iPhone kan op afstand worden gewist zodra het apparaat verbinding maakt met Internet. Team ICT kan dat voor je verzorgen maar nog beter is het om dat zelf te doen zodat er minder tijd verloren gaat. Op het Serviceplein bij Handleidingen staat hoe je dat moet doen.

Gebruik je USB-sticks?
Gebruik geen USB-sticks die privé eigendom zijn. Mocht het nodig zijn om op deze manier zakelijke bestanden te vervoeren, gebruik dan een beveiligde stick. Deze is via het Serviceplein aan te vragen en bevat een beveiligde zone waarin je zakelijke bestanden kunt plaatsen. Een USB-stick raak je gemakkelijk kwijt (in een pc laten zitten, vergeten mee te nemen of verloren), vandaar dat extra oplettendheid hierbij geboden is.

Privacy?
Op zakelijke laptops mogen natuurlijk geen privacy-gevoelige gegevens achterblijven. Dit geldt ook voor de leenlaptops die je via het Serviceplein voor korte tijd kunt reserveren. Mocht het voor het werk toch noodzakelijk zijn om bestanden lokaal op te slaan, gebruik dan de speciaal voor dat doel ingerichte beveiligde zone. Daar kun je alleen bij als je het juiste wachtwoord kent. Verwijder na gebruik alle gegevens die je op de laptop hebt opgeslagen uit de mappen 'Mijn documenten', 'Downloads' en van het bureaublad etc.

Deel je privacygevoelige gegevens?
Maak geen gebruik van onveilige websites zoals Dropbox, WeTransfer of Google Cloud om privacygevoelige gegevens met externe partijen te delen. Gebruik hiervoor het NAS systeem waarmee je zowel kunt verzenden als ontvangen. Meer informatie hierover is aan te vragen bij de ICT Servicedesk. Op niet al te lange termijn wordt de software Zivver bedrijfsbreed geïmplementeerd waarmee veilig mailen en meesturen van grote bestanden mogelijk is. Houd de berichtgeving hierover in de gaten).

Installeren van software
Op in bruikleen gegeven apparatuur mag uiteraard geen software worden toegevoegd. Ontbreekt benodigde software, dan neem je contact op met ICT.

Pas op met e-mail
Zowel zakelijk als privé: open geen e-mail waarvan je de herkomst niet kent en klik niet op linkjes of onbekende bijlagen. Het is niet logisch dat je e-mails van bijvoorbeeld banken of internetproviders op je zakelijk mailadres ontvangt; die bevatten meestal ransomware, virussen of pogingen tot phishing. Het bekende TV-programma 'Opgelicht' heeft een goede gratis app met dezelfde naam gemaakt die hierbij behulpzaam is. Je ontvangt dan waarschuwingen voor valse mail of websites die tot doel hebben jou inloggegevens te ontfutselen. Tenslotte: gebruik je zakelijke e-mail adres niet voor privé doeleinden zoals inloggen bij webwinkels of het ontvangen van vakantie-aanbiedingen.

Q&A WOB-/WOO-VERZOEK
De termijn om aan het Woo-verzoek te voldoen loopt t/m woensdag a.s. (1 juni). De publicatie van in elk geval de GGD GHOR-stukken zal dan plaatsvinden. Ook zullen veel GGD'en dan eigen stukken publiceren. Onderstaand een woordvoeringslijn vanuit GGD GHOR Nederland die ook kan helpen bij het beantwoorden van vragen over het proces, onze mening over ICAM, de inhoud van documenten die we openbaar maken. De regionale GGD'en beantwoorden vragen die zij hierover krijgen zelf. Als er inhoudelijke vragen zijn over GGD GHOR-stukken of over dit proces dan kan GGD GHOR Nederland deze vragen beantwoorden. Belangrijkste is dat we woordvoering onderling afstemmen, zodat we elkaar niet verrassen of in verlegenheid brengen. En te concentreren op de eigen afwegingen en niet te oordelen over anderen en/of te reageren op mogelijke verschillen. Bij twijfel graag overleggen met woordvoering landelijk. (Jacqueline Toonen: 06-15189751).

UITLEG WERKWIJZE AFHANDELING WOB-/WOO-VERZOEK
We maken onderscheid tussen het proces voor:
A) de documentatie die GGD GHOR NL voor GGD'en verzamelt: dit zijn de stukken die GGD GHOR NL heeft gedeeld met alle GGD'en; en
B) de documentatie die GGD'en zelf verzamelen. Uiteraard worden alleen de stukken waarin VWS belanghebbende is voorgelegd.

Samenvatting proces A
- De GGD GHOR-documentatie is beoordeeld op i) binnen de scope van het Wob/Woo-verzoek valt; (ii) of een document potentieel schadelijk is, en zo ja; (iii) welke uitzondering eventueel van toepassing is op het betreffende (onderdeel van) document en welke motivering daarbij past. Afhankelijk van die beoordeling kan de verstrekking van documenten achterwege blijven, dan wel kunnen onderdelen daarvan worden gelakt.
- GGD Zeeland is de partij die de GGD GHOR-documentatie online plaatst, zodat andere GGD'en alleen maar naar die publicatie en de motivering van GGD Zeeland hoeven te verwijzen. De beoordeling van die documenten (wel/niet/gedeeltelijk verstrekken) wordt daarmee in principe door iedereen overgenomen.

Samenvatting proces B
- Voor regionale GGD-stukken maken GGD'en zelf een afweging, aan de hand van een referentiebeoordeling die is uitgevoerd op het dossier van GGD Zeeland. Dit dossier biedt een voorbeeld van welke (type) stukken wel/niet/gedeeltelijk openbaar moeten worden gemaakt en waarom.
- Het kan zijn dat GGD'en de deadline van 1 juni niet halen, of slechts een gedeelte van de stukken kunnen verstrekken. Ofwel door tijdnood, ofwel omdat een andere partij nog om een zienswijze moet worden gevraagd op de publicatie van de stukken (dwz: bij een

zienswijze wordt een partij die in stukken genoemd wordt gevraagd of/waarom deze er bezwaar tegen heeft dat de info in een bepaald document openbaar wordt.) In dat geval zullen zij deelbesluiten gaan nemen. De rest volgt dan later op een door de regionale GGD te bepalen tijdstip.

Q&A WOO-VERZOEKEN

Wat is er aan de hand?
Op 15 februari 2022 kreeg elke GGD een Wob-verzoek (vanaf 1 mei 2022 heet dit een Wet Open Overheid-verzoek) van Stichting ICAM naar aanleiding van de datadiefstal uit CoronIT. Elke GGD heeft een eigen verantwoordelijkheid en bevoegdheid om invulling te geven aan het Woo-verzoek. GGD GHOR Nederland kreeg ook dit Wob-verzoek maar valt niet onder de werkingssfeer en gaat daardoor zelf geen stukken verstrekken. Wel coördineert GGD GHOR Nederland op verzoek van de DPG'en de afhandeling van dit Woo-verzoek en wordt daarbij juridisch bijgestaan door van Doorne. Dat doet GGD GHOR Nederland vanwege het belang van alle GGD'en om dit verzoek op consistente wijze te behandelen. De termijn om aan het Woo-verzoek te voldoen loopt t/m woensdag 1 juni 2022. De publicatie van in elk geval de GGD GHOR-stukken (via GGD Zeeland) zal dan plaatsvinden. Ook zullen veel GGD'en nog eigen stukken publiceren.

Stichting ICAM?
Stichting ICAM zegt op te komen voor de belangen van groepen mensen die schade lijden door toedoen van grote organisaties. Een procesfinancier (Liesker Procesfinanciering) financiert de collectieve rechtszaak die ICAM wil aanspannen. Burgers kunnen zonder kosten deelnemen, op basis van een no cure no pay-regeling. In ons geval stelt ICAM op te komen voor burgers die ten tijde van de datadiefstal (januari 2021) in de corona-systemen stonden geregistreerd. Deze burgers zouden onvoldoende beschermd zijn tegen inbreuken op hun privacy door "de overheid". De zaak wordt inhoudelijk behandeld door een team van het bureau SOLV Advocaten onder leiding van Douwe Linders. De procesfinancier krijgt een vergoeding voor zijn kosten als de zaak slaagt. Deze vergoeding bedraagt 20% van de schadevergoeding die Stichting ICAM voor gedupeerden weet te innen en is gemaximeerd op vijf keer de door de procesfinancier geïnvesteerde som.

Stichting ICAM spreekt het ministerie van Volksgezondheid, Welzijn en Sport (VWS) aan: "Gedurende de corona pandemie hebben de GGD'en hun uiterste best gedaan om alles in goede banen te leiden. Het ging echter mis bij het beveiligen van de IT-systemen waarin persoonsgegevens van 6,5 miljoen Nederlandse burgers zijn opgeslagen. Het ministerie van VWS had de leiding over de

bestrijding van de corona pandemie en heeft opdracht gegeven tot de ingebruikname van de slecht beveiligde IT-systemen."

Werken jullie mee aan de WOO-verzoeken van Stichting ICAM?
Stichting ICAM heeft verschillende verzoeken om informatie bij de GGD'en en GGD GHOR Nederland neergelegd, waaronder een Wob verzoek d.d. 15-02. Dit verzoek heeft zij overigens ook aan de veiligheidsregio's en gemeenten gedaan. De GGD'en werken mee aan dit Wob verzoek en trachten zo zorgvuldig mogelijk dit verzoek af te wikkelen. Vanwege de grote hoeveelheid gevraagde documentatie is uitstel aan ICAM gevraagd tot 1 juni. Op die datum zal een (groot) deel van de gevraagde documentatie verstrekt worden.

Heel veel documenten worden niet verstrekt/zijn grotendeels weggelakt. Waarom is dat?
We hebben met de grootst mogelijke zorgvuldigheid invulling proberen te geven aan het Wob verzoek. Gezien de enorme reikwijdte van het verzoek zullen zeer veel documenten verstrekt worden. De documenten die niet verstrekt worden vallen ofwel niet onder de reikwijdte van het verzoek of vallen onder een uitzonderingsgrond zoals gedefinieerd in de Woo. Onderdelen van documenten zijn gelakt conform de bepalingen daarover in de Woo.

Geven we zo niet onvoldoende openheid van zaken?
Als GGD zijn we meer dan bereid om openheid van zaken te geven. Vanuit die grondhouding hebben we het Wob verzoek van ICAM in behandeling genomen en bij iedere categorie van opgevraagde documenten beschouwd welke documenten onder de reikwijdte vallen en verstrekt dienen te worden.

Het decentrale systeem en de decentrale infrastructuur?
Het zal inmiddels niemand meer verrassen als we stellen dat de decentrale infrastructuur die de GGD'en kenmerkt, niet altijd even effectief was om een pandemie te bestrijden. Dat gold zeker ook voor de IT-systemen en datastromen waarlangs gewerkt is. Dat was echter hetgeen voor handen was en waarmee we gewerkt hebben teneinde besmettingen, ziekte en ziekenhuisopname zoveel mogelijk te voorkomen.

Wat vinden jullie van de massaclaim die Stichting ICAM heeft neergelegd?
GGD GHOR en GGD'en werden eind januari 2021 geconfronteerd met datadiefstal uit corona-systemen. Er is direct aangifte bij de politie en melding bij AP gedaan en de beveiliging van de systemen en data is verder geïntensiveerd. Een jaar politieonderzoek naar de verdachten van de datadiefstal toont aan dat gegevens van circa 1250 Nederlanders uit CoronIT gestolen zijn. Richting deze 1250 burgers

hebben wij een financieel gebaar gemaakt. Grootschalige databestanden noch de handel erin heeft de politie niet aangetroffen.
Wij zijn dan ook verbaasd dat stichting ICAM voor zo'n grote groep een schadevergoeding claimt. En verontwaardigd dat zij stelt dit vanuit een ideëel doel te doen; namelijk een betere beveiliging van de data van burgers. De stichting had er ons inziens beter aan gedaan haar zogenaamde ideële doel op een andere wijze te realiseren in plaats van met een massaclaim van 3,2 miljard met een keihard verdienmodel voor de procesfinancier daarachter. Het ideële doel, komen tot betere bescherming van persoonsgegevens, is bovendien al lang in het vizier van de GGD'en die daar het belang volledig van inzien. Immers hebben wij maar één doel; de gezondheid en veiligheid van Nederlanders bevorderen in én buiten crisistijd met alle waarborgen die daarbij horen.

Wat vinden jullie van dit soort claimstichtingen die duidelijk rendement willen zien op hun investeringen? Wij vinden het vooral van belang de daadwerkelijk betrokken burgers bij de datadiefstal te informeren en richting hen een financieel gebaar te maken. Dat past bij de maatschappelijke verantwoordelijkheid die we als organisatie hebben en voelen.

Wat hebben jullie gedaan na de ontdekking van de datadiefstal?
We hebben direct onderzoek ingesteld. Vervolgens contact opgenomen met de politie, aangifte gedaan en een melding gedaan bij de Autoriteit Persoonsgegevens. Ook hebben wij controles uitgevoerd in onze systemen én toegang verstrekt aan de politie om de opsporing zo goed mogelijk plaats te kunnen laten vinden. Wij controleren op verschillende manieren hoe onze medewerkers omgaan met de informatie in onze systemen. Indien we daar onregelmatigheden in zien, nemen we maatregelen. Ook beschermen we ons tegen aanvallen op onze systemen van buitenaf. De betrokkenen van wie de gegevens zijn ingezien, gestolen en mogelijk verkocht zijn allemaal via een brief door ons geïnformeerd.

Waarom starten jullie met een verouderd systeem?
In het voorjaar 2020 heerste angst in Nederland en werd alles in het werk gesteld om grip op het virus te krijgen. Het laten testen en uitvoeren van bron- en contactonderzoek waren dé instrumenten om het virus in beeld te krijgen en te bestrijden. Daar is alles voor in het werk gesteld. Snelheid was letterlijk van levensbelang. HPZone was het systeem dat voor handen was waarmee in Nederland al jaren werd gewerkt in het licht van infectieziektebestrijding. Een systeem dat niet ontwikkeld noch geschikt was voor dermate grote opschaling en gebruik. Een alternatief voor bron- en contactonderzoek was echter niet voor handen. In samenspraak met het RIVM en VWS is

daarnaast, toen duidelijk werd dat de GGD'en de uitvoering van het grootschalig testen op zich moesten nemen, CoronIT, ontwikkeld. Voor beide systemen is ervoor gezorgd dat alle medewerkers overal bij konden zodat indexen snel over hun testuitslag geïnformeerd konden worden en hun contacten konden worden geïnformeerd om zo de verspreiding van het virus in de kiem te smoren. Maximale opschaling was in die begin fase het devies. Later zijn hierop aanpassingen gepleegd waarbij onder andere rechten van medewerkers beperkt zijn en de monitoring is geïntensiveerd. En nog later is zelfs besloten om HPzone uit te faseren en te gaan vervangen door GGD Contact.
Alle medewerkers die toegang hadden tot deze systemen zijn geïnformeerd dat ze werken met gevoelige data, hebben scholing ontvangen, geheimhoudingsverklaring getekend, en wisten dat oneigenlijk gebruik strafbaar was. Sommige medewerkers/uitzendkrachten hebben toch misbruik gemaakt van de situatie deels uit naïviteit, deels heel bewust voor eigen gewin, dat is uiteraard zeer kwalijk.

Welke maatregelen hebben jullie genomen?
Export- en printfuncties zijn direct beperkt en de loggingprocedures zijn geïntensiveerd en aangescherpt, waarbij inmiddels ook geautomatiseerde controle plaatsvindt op de logging. Bij GGD Contact, het door het ministerie van VWS, GGD GHOR Nederland en alle GGD'en aangewezen vervangend systeem voor HPZone Lite, zijn informatiebeveiliging en privacy integrale onderdelen geweest van de ontwikkeling en implementatie. GGD GHOR heeft de Autoriteit Persoonsgegevens middels de door haar gevraagde voortgangsrapportage nader geïnformeerd over de verbeteringen die doorgevoerd zijn.

Kunt u garanderen dat de gegevens van mensen nu veilig bij u zijn?
Geen enkele organisatie kan 100% garantie geven. Dataveiligheid en privacy zijn integrale onderdelen van onze werkprocedures. Het is een doorlopend proces waarbij we continu de veiligheid van onze systemen analyseren en verbeteren. We spannen ons maximaal in om de data van alle Nederlanders goed te beschermen en beveiligen tegen onrechtmatige inzage en misbruik.

Klopt het dat de Autoriteit Persoonsgegevens (AP) onderzoek heeft gedaan n.a.v. de datadiefstal?
Ja, dat klopt. GGD GHOR Nederland heeft kennis genomen van de bevindingen die voortkomen uit het onderzoek van de AP naar de datadiefstal van begin 2021. Net als de AP is ook GGD GHOR Nederland van mening dat persoonsgegevens zo goed mogelijk moeten worden beschermd. GGD GHOR Nederland heeft dan ook werk gemaakt van de aanbevelingen van de AP en de AP daarvan in kennis gesteld.

Hoe stelt GGD GHOR Nederland vast dat de Autoriteit Persoonsgegevens (AP) geen handhavingsbevoegdheden gebruikt, waaronder het opleggen van een boete?
De AP heeft aan GGD GHOR Nederland aangegeven geen handhavingstraject te starten, maar vraagt wel om een voortgangsrapportage op te leveren. Deze rapportage is eind februari 2022 aan de AP verstrekt.

Welke conclusies trok de Autoriteit Persoonsgegevens (AP) in haar onderzoek?
De AP signaleerde op basis van uitgebreid en intensief onderzoek een aantal verbeterpunten. Zo kwam het onder meer met de aanbeveling om de toegangsbeveiliging en de autorisatieprocessen verder aan te scherpen en de afspraken tussen partijen inzake de informatiebeveiliging te verbeteren. Daarnaast deed de AP aanbevelingen ten aanzien van de beveiliging en de vervanging voor de systemen HPZone en HPZone Lite. Zie hier de link (klik hier) naar ons websitebericht van 9 november 2021.

Wat vinden jullie ervan dat er datadiefstal heeft plaatsgevonden?
We betreuren het dat er datadiefstal uit onze systemen heeft plaatsgevonden. Iedere dag werkten we met vele collega's om Nederlanders te testen, te vaccineren en bron- en contactonderzoek uit te voeren. Het waarborgen van de dataveiligheid is daar onlosmakelijk mee verbonden. Nederlanders moeten erop kunnen vertrouwen dat hun data bij de GGD-organisaties in veilige handen zijn. Het is ook goed dat er vanuit de rechter een krachtig signaal is uitgegaan naar diegenen die zich schuldig aan de datadiefstal hebben gemaakt. Wij tolereren niet dat medewerkers misbruik maken van het systeem waartoe ze voor hun werkzaamheden bij de GGD'en toegang hebben. Indien een overtreding ontdekt wordt, wordt hier direct op geacteerd hetgeen kan leiden tot aangifte en ontslag op staande voet.

Vragen over systemen

Uit welke systemen is er sprake geweest van datadiefstal?
Tot nu toe is uit politieonderzoek alleen gebleken dat er uit CoronIT gegevens gestolen zijn. Dit is het administratiesysteem voor het testen en vaccineren en de communicatie hierover. Dus wanneer u een afspraak maakt voor een COVID-19-test via het callcenter, de COVID-19-test website of een arts, komen uw persoonsgegevens in CoronIT. Ook, wanneer u een afspraak maakt voor een vaccinatie.

Zijn mijn gegevens wel veilig bij jullie?
Geen enkel IT-systeem is onfeilbaar. Wij doen alles wat in ons vermogen

ligt om ervoor te zorgen dat gegevens van mensen die zich laten testen of vaccineren in veilige handen zijn. Daarom hebben we ook na dit incident maatregelen genomen om dit soort incidenten in de toekomst te voorkomen. Het gaat om de volgende maatregelen:

- Wij hebben maatregelen genomen om te voorkomen dat GGD-medewerkers gegevens makkelijk uit de systemen kunnen halen zonder daartoe bevoegd te zijn;
- Wij hebben de politie de noodzakelijke toegang gegeven tot onze systemen om de daders op te sporen;
- Wij hebben onderzoek gedaan op internet naar mogelijk te koop aangeboden persoonsgegevens;
- Wij hebben een specialistisch team samengesteld en extra controlemaatregelen genomen. Zo kunnen we continu nagaan of onze medewerkers op een zorgvuldige manier omgaan met de persoonsgegevens.

Zijn de systemen voor testen, bron- en contact onderzoek en vaccineren strikt gescheiden?
Gegevens van testen en vaccineren bevinden zich in CoronIT. De medische gegevens die bij vaccinaties worden vastgelegd zijn afgeschermd en niet zichtbaar voor medewerkers die zich met testen bezighouden. Wel is er een koppeling waardoor een testuitslag altijd te zien is, wanneer iemand in het systeem kijkt bij een vaccinatie afspraak. Dit is zo ingericht omdat het nodig kan zijn om te bepalen of iemand gevaccineerd kan worden. De gegevens van het bron- en contactonderzoek bevinden zich in HPZone.

Hoeveel Nederlanders staan er in CoronIT en HPzone?
Op het moment dat de datadiefstal werd geconstateerd (januari 2021) stonden in CoronIT gegevens van circa ca. 5,5 miljoen mensen en in HPZone gegevens van circa 1 miljoen personen.

Hoeveel medewerkers hebben toegang tot CoronIT?
In totaal ging het in de piekperiode om ca. 35.000 medewerkers. Zowel bij de GGD'en als bij bedrijven die gecontracteerd zijn voor de COVID-19-bestrijding.

Wat doen de medewerkers in CoronIT en HPZone?
Medewerkers van het callcenter die telefoontjes ontvangen kunnen via CoronIT testafspraken en vaccinatieafspraken maken. Verder kunnen de medewerkers die uitgaande telefoontjes plegen de testuitslagen zien, zodat ze die kunnen meedelen. Bron- en contactonderzoekers leggen alle gegevens rondom een besmetting vast in HPZone.

CoronIT

Wat is er precies gestolen uit CoronIT?
Uit politieonderzoek naar de verdachten van de datadiefstal is gebleken dat de gegevens van circa 1.250 personen onbevoegd zijn ingezien, gestolen en mogelijk verkocht. Uit het onderzoek blijkt dat het gaat om gegevens van personen die bij een GGD een coronatest hebben laten doen of zich bij een GGD hebben laten vaccineren. Deze gegevens bevatten onder meer naam, geboortedatum, adres, telefoon, e-mailadres, Burgerservicenummer (BSN) en nationaliteit. De personen om wie het gaat zijn door ons geïnformeerd.

Is het normaal dat zoveel medewerkers toegang hebben tot deze gegevens? En, waarom is dit nodig?
Wij willen het coronavirus zo goed mogelijk bestrijden. Daarbij zijn veel medewerkers betrokken. Elke callcenter medewerker die telefoontjes aanneemt (inbound) moet afspraken kunnen maken. En iedere callcenter medewerker die mensen belt (outbound) moet uitslagen door kunnen geven als deze binnen zijn. Dit alles om te zorgen dat een besmet persoon zo snel mogelijk kennis heeft van diens besmetting en daarmee nieuwe besmettingen kan voorkomen.

Welke verbetermaatregelen zijn er genomen?
Direct na de datadiefstal in januari 2021 zijn er, zoals de Autoriteit Persoonsgegevens ook in haar eindbrief heeft vastgesteld, direct verdere verbetermaatregelen genomen ter bescherming van de persoonsgegevens die door de GGD-organisaties worden verwerkt in het kader van de bestrijding van de coronapandemie. De toegang tot de Corona applicaties is enkel en alleen mogelijk indien een medewerker getekend heeft voor zijn of haar (arbeids-)overeenkomst, een geheimhoudingsbeding en een door het ministerie van Justitie verstrekte Verklaring Omtrent Gedrag (VOG) heeft overlegd. Ook zijn de werkinstructies en de trainingen op het gebied van de verwerking en bescherming van persoonsgegevens verder aangescherpt. Om mensen goed te helpen is het noodzakelijk dat sommige medewerkers alle inwoners die in het systeem staan, kunnen opvragen. De gebruiker ziet alleen die gegevens die hij of zij op dat moment voor zijn werk nodig heeft. Wanneer een medewerker misbruik maakt van zijn of haar rechten geldt een zerotolerance beleid en zal, na onderzoek, aangifte bij de politie worden gedaan. Daarnaast zijn er verdere technische en functionele aanpassingen gedaan in de Corona-applicaties.

Wat betekent het beperken van de snelheid waarmee testen en bron- en contactonderzoek kan worden uitgevoerd?
Het testen en bron- en contactonderzoek loopt onverminderd door. Dat

is immers nodig om de pandemie te bestrijden. Wel hebben we een aantal extra waarborgen ingebouwd om datadiefstal te voorkomen. Deze waarborgen zijn echter niet van invloed op de doorlooptijd om een test- of vaccinatieafspraak te maken of de testuitslag te krijgen, noch op de doorlooptijd van het bron- en contactonderzoek.

HPZone

Waarom starten jullie met een verouderd systeem?
In het voorjaar 2020 heerste angst in Nederland en werd alles in het werk gesteld om grip op het virus te krijgen. Het laten testen en uitvoeren van bron- en contactonderzoek waren dé instrumenten om het virus in beeld te krijgen en te bestrijden. Daar is alles voor in het werk gesteld. Snelheid was letterlijk van levensbelang. HPZone was het enige systeem dat voorhanden was om in maart 2020 in vliegende vaart mee aan de slag te gaan. We hebben aan het begin geconstateerd dat HPZone niet geschikt was voor grote opschaling, maar een alternatief was niet voor handen. Bovendien bewust zo ingericht dat alle medewerkers overal bij konden zodat indexen en hun contacten snel geïnformeerd konden worden om verspreiding van het virus in de kiem te smoren. Er zijn aanpassingen gepleegd, maar we wisten ook dat een nieuw systeem nodig was.
Al die medewerkers zijn geïnformeerd dat ze werken met gevoelige info, hebben scholing ontvangen, geheimhoudingsverklaring getekend, wisten dat oneigenlijk gebruik strafbaar was.
Sommige medewerkers/uitzendkrachten hebben toch misbruik gemaakt van de situatie deels uit naïviteit, deels heel bewust voor eigen gewin, dat is uiteraard zeer kwalijk.

Klopt het dat er datasets uit HPZone zijn aangeboden?
We hebben signalen ontvangen dat datasets zouden zijn aangeboden, maar hebben niet kunnen vaststellen dat ze gestolen of verhandeld zijn. Een jaar na dato heeft de politie dat ook niet vast kunnen stellen. Uit politieonderzoek is alleen gebleken dat de gegevens van circa 1.250 personen onbevoegd zijn ingezien, gestolen en mogelijk verkocht.

Hoe kan het dat er sprake is van het exporteren van een dataset?
Voor CoronIT geldt hier het volgende: CoronIT beschikte niet over een exportfunctie, maar wel over een printfunctie om een lijst met personen die een afspraak had af te drukken. Die functie werd, afhankelijk van de locatie, voor verschillende doeleinden gebruikt. Onder andere door de portier/verkeersregelaar om te controleren of mensen die aankomen een afspraak hebben. Zo kon voorkomen worden dat mensen zonder afspraak in de keten kwamen en voor vertraging zorgen. Ook werd deze functie gebruikt om een noodlijst aan te leggen zodat in geval van uitval

van het systeem testgegevens op de lijst konden worden vastgelegd, zodat die na de storing geregistreerd konden worden.

Er zijn geen indicaties dat deze functie is misbruikt. Echter, omdat de kans bestond dat met het bekend worden van deze printfunctie het risico's op misbruik toe zou kunnen nemen, hebben we de printfunctie in CoronIT op maandag 25 januari 2021 uitgeschakeld. GGD'en kunnen als ze dat willen nu lijsten maken vanuit een beveiligde omgeving.

De exportfunctie van HP Zone maakte het mogelijk om een selectie van de gegevens in HP Zone te downloaden als lijst in bijvoorbeeld Microsoft Excel. De persoon die de export uitvoerde, kon variabelen selecteren (voorbeelden: leeftijd, postcode, testuitslag) en criteria toepassen om benodigde analyses te kunnen uitvoeren (voorbeeld: leeftijd >65). Deze lijsten werden gebruikt ten behoeve van de werkverdeling (door de supervisoren van het bron- en contactonderzoek), om analyses te doen en om rapportages te maken om zicht te houden op het virus (voorbeeld: clusteranalyse). Ook werden dergelijke lijsten gebruikt om de prestaties van de organisatie te monitoren (voorbeeld: analyse tijdigheid bron- en contactonderzoek ten behoeve van artsen, epidemiologen en data-analisten).

Klopt het dat die functie is uitgezet?
Ja, de belangrijkste exportmogelijkheden zijn uitgezet. En er zijn aanpassingen doorgevoerd in de overige exportmogelijkheden. De rechten voor gebruik van de resterende, benodigde exportfunctionaliteit zijn aan minder mensen toegekend op basis van beperktere rollen. Op 30 januari 2021 is de printfunctionaliteit in HPZone en HP Zone Lite uitgezet. Dit geldt voor zowel 'overzichten' als de individuele dossiers. Er kunnen geen persoonsgegevens worden geëxporteerd of geprint uit HPZone en HPZone Lite. Er geldt alleen een uitzondering voor het printen en exporteren van gepseunonimiseerde gegevens voor een zeer beperkt aantal daartoe geautoriseerde personen die de rol van "admin" of "coördinator" hebben", en waarbij de gepseunonimiseerde export voor statistische en onderzoeksdoeleinden is bedoeld. Deze prints en exports worden gelogd. Ook de weergave van de zoekresultaten is verder beperkt in de Corona applicaties. Bovendien kan een medewerker alleen toegang krijgen tot alle Corona applicaties indien zijn GGD-account geactiveerd is door de betreffende GGD.

HP Zone en HP Zone Lite. Wat is het verschil?
HPZone is een systeem dat wordt gebruikt voor infectiebestrijding van alle typen infectieziekten. Bij de uitbraak van het coronavirus is dit systeem ook hiervoor gebruikt. Met het uitbreiden van het aantal medewerkers, is HPZone Lite ontwikkeld om ervoor te zorgen dat zij alleen toegang hadden tot de COVID-19 data.

Waarom hebben jullie HP Zone Lite geïmplementeerd (in augustus 2020)?
HPZone Lite is bedoeld om grote aantallen medewerkers makkelijk te laten werken aan bron- en contactonderzoek. In de eerste golf liepen GGD-regio's over en konden andere GGD-regio's hen niet helpen. Dat hebben we opgelost in HPZone Lite, door het systeem zo in te richten dat GGD'en elkaar wel konden helpen. Hierdoor konden veel meer bron- en contactonderzoekers hun werk doen en kon het bron en contactonderzoek sneller worden opgestart zodat we voorkwamen dat positief geteste mensen en hun directe contacten weer anderen besmetten.

Kan een medewerker van GGD Groningen in een bron-en contactonderzoek casus van GGD Regio Utrecht?
Nee, GGD-medewerkers kunnen alleen bij de gegevens van hun eigen GGD. Het is wel zo dat bron- en contactmedewerkers van een GGD soms tijdelijk toegang krijgen tot gegevens van een andere GGD om te ondersteunen bij hoge druk. Verder is er een landelijke schil van BCO-medewerkers. Deze landelijke BCO-medewerkers werken vaak voor meerdere GGD'en en hebben dus toegang tot de gegevens van deze GGD'en. De procedures voor het toegang geven en -na afronding van werkzaamheden- ontnemen van die toegang is voor landelijke BCO-medewerkers en GGD-medewerkers aangescherpt. Dit is aangescherpt naar aanleiding van de datadiefstal.

Wanneer gaan jullie een ander systeem invoeren voor het bron- en contactonderzoek?
GGD Contact is het door het ministerie van het ministerie van VWS, GGD GHOR Nederland en alle GGD'en aangewezen als vervangend systeem voor HPZone Lite en is bij alle GGD'en en landelijke partners geïmplementeerd. GGD Contact voldoet aan alle moderne eisen op het gebied van privacy- en informatiebeveiliging. GGD Contact is ontwikkeld door het Ministerie van VWS en wordt gebruikt voor het bron- en contactonderzoek (BCO) door de GGD'en en de landelijke partners. Bij GGD Contact, het door het ministerie van VWS, GGD GHOR Nederland en alle GGD'en aangewezen vervangend systeem voor HPZone Lite, zijn informatiebeveiliging en privacy integrale onderdelen geweest van de ontwikkeling en implementatie.

Persoonlijke gegevens

Welke informatie van mensen staat in CoronIT en HP Zone?
In CoronIT staan onder andere naam, adres, woonplaats, telefoonnummer/e-mailadres, BSN, geslacht, geboortedatum, test- en/of vaccineerafspraken en testresultaten. Contra-indicaties en COVID-19 klachten.

In HP Zone staan naam, adres, woonplaats, telefoonnummer, geslacht, geboortedatum en BSN van een persoon. Verder wordt in HP Zone ook de informatie uit de bron- en contactonderzoek gesprekken vastgelegd. Dit is onder andere: noodzakelijke medische gegevens (bijvoorbeeld klachten/symptomen en huisarts), waar iemand is geweest en met wie hij/zij in contact is geweest. Ook wordt informatie vastgelegd van bron(nen) en nauwe contacten.

De gegevens zoals geregistreerd in CoronIT zijn opgenomen in de privacyverklaring CoronIT. Hetzelfde geldt voor HP Zone, deze zijn terug te vinden in de privacyverklaring van bron- en contactonderzoek in het kader van COVID-19.

Waarom zijn persoonlijke gegevens zoals BSN, geboortedatum, telefoonnummer en e-mailadres nodig voor het maken van een test- of vaccinatieafspraak?
Volgens de Wet op de geneeskundige behandelovereenkomst (WGBO) zijn we verplicht om een geboortedatum uit te vragen en vast te leggen bij een te testen of te vaccineren persoon. Zo weten we zeker dat wij te maken hebben met de juiste persoon. Het telefoonnummer is nodig om contact op te kunnen nemen in het geval een test- of vaccinatieafspraak niet door kan gaan. Bijvoorbeeld bij slechte weersomstandigheden of als het vaccineren ineens wordt stilgelegd zoals bij AstraZeneca tijdelijk aan de orde was. Het e-mailadres is nodig om per e-mail een test- of vaccinatieafspraak te kunnen bevestigen. En, wenselijk op het moment dat er onverhoopt een verkeerd telefoonnummer is geregistreerd om iemand te kunnen bereiken.

De wet Aanvullende bepalingen verwerking persoonsgegevens in de zorg bepaalt dat wij het BSN-nummer moeten uitvragen. De GGD'en zijn wettelijk verplicht om het **BSN-nummer** te verwerken. Indien burger deze gegevens niet wil geven, vindt er geen vaccinatie plaats.

Welke gegevens van een persoon kunnen de medewerkers inzien?
Dat hangt van de rol van de gebruiker af. De gebruiker ziet alleen die gegevens die hij of zij op dat moment voor zijn werk nodig heeft. Voor mensen die werken bij het callcenter dat testafspraken maakt zijn bijvoorbeeld de gezondheidsverklaringen die voor vaccinaties worden ingevuld niet zichtbaar. Registratie van bijwerkingen is alleen toegankelijk voor mensen met medische autorisatie.

Staan de gegevens van alle Nederlanders in CoronIT en HP Zone?
Nee, in CoronIT staan alleen de gegevens van personen die een test- of vaccinatie afspraak bij een GGD hebben gemaakt. In HP Zone staan alleen de gegevens van de personen die een positieve COVID-19 test hebben ontvangen en van mensen die als huisgenoot of als nauw contact uit bron- en contactonderzoek kwamen.

Hoe lang blijven mijn persoonsgegevens bewaard?
Wij houden ons aan de wettelijke termijnen die hiervoor gelden. Wij verwijderen uw persoonsgegevens als deze niet langer noodzakelijk zijn. Voor HPzoneLite geldt een maximale bewaartermijn van 5 jaar, voor data in CoronIT 20 jaar. We bewaren persoonsgegevens in ieder geval voor de gehele duur van de pandemie.