



Privacy (be)spreekuur Zorg en Veiligheid

Hans Versteeg, 13 en 14 mei 2020

Privacyverklaring

De IBD stelt Zoom privacyvriendelijk in (*privacy by default*)

Tijdens de interactieve webinars maakt de IBD:

- gebruik van **wachtwoorden** om aan vergaderingen deel te nemen.
- gebruik van **unieke vergader ID's** om vergaderingen af te scherm.
- geen gebruik van:
 - “cloud recording” en neemt de videoconferentie niet op.
 - “local Recording”
 - “automatically Transcribe Cloud Recordings”
 - “attendee attention tracking”

Even voorstellen

- Naomi (IBD) moderator
- Privacy adviseurs IBD introduceren thema's en helpen bij beantwoording vragen



Doelen *bespreekuur*

- **Informatieoverdracht en deling → Samen privacy issues bespreken**
- Deelnemers stellen en beantwoorden vragen
- Contacten onderhouden en nieuwe contacten maken
- Input ophalen voor FAQs en Privacy Producten op de IBD website

Corona en Privacy

Via deze pagina informeert de IBD gemeenten met veelgestelde vragen, nieuwsberichten, publicaties en relevante links over hoe Corona impact kan hebben op privacy. Gemeenten kunnen onderling expertise en vragen uitwisselen op het [Coronaforum](#). Voor algemene informatie en vragen over Corona die niet te maken hebben met informatiebeveiliging en of privacy, kunt u terecht op de [VNG website](#) en voor privacy gerelateerde vragen kunt u mailen naar privacy@vng.nl.

De IBD organiseert daarbij tweewekelijks online Privacy (be)Spreekuren voor gemeentelijke FG's en PO's (de eerste waren op 31 maart en 1 april). Houd de [agenda](#) in de gaten om u aan te melden voor de volgende besprekuren. [De presentatie van deze besprekuren kunt u hier downloaden.](#)

Q&A

De onderstaande Q&A's worden regelmatig aangevuld aan de hand van input die we in deze periode van gemeenten ontvangen. De vragen zijn per onderwerp genummerd. Om die reden vindt u de nieuwste vragen

Spelregels





Programma

Toelichting (10.30 – 11.15 uur)

1. Achtergrond en kenmerken zorg & veiligheid domein
2. Grondslagen voor gegevensverwerking, juridische basis
3. De werkwijze in de praktijk
4. Nieuwe wetgeving
5. Bredere context: relatie met o.a. sociaal domein, radicalisering, ondermijning

En discussie! (11.15 uur – 12.00 uur)



1. Achtergrond zorg en veiligheid

Zorg en veiligheidshuizen



- 34 regio's
- Doel: veiligheid en leefbaarheid: minder overlast, minder criminaliteit, en minder maatschappelijke uitval
- Netwerkorganisatie, samenwerking tussen verschillende partijen uit zorg én veiligheid
- Ondersteuning professionals op casusniveau
- Kenmerk doelgroep: multiproblematiek
- Persoonsgerichte aanpak én gezamenlijke aanpak

Werkwijze zorg en veiligheidshuis



Aanpak multiproblematiek



1. Er is sprake van meerdere problemen
2. De problematiek kan leiden tot crimineel en/of overlastgevend gedrag
3. Samenwerking tussen partijen is noodzakelijk om effectief te kunnen zijn
4. De problematiek wordt beïnvloed door en heeft impact op het (gezin)systeem en/of de sociale leefomgeving
5. Ernstige lokale of gebiedsgebonden veiligheidsproblematiek, die vraagt om een ketenoverstijgende aanpak

Kwetsbare personen – gevoelige gegevens

Het gaat om gevoelige persoonsgegevens:

- Vanwege de herkomst
 - Justitiële gegevens
 - Medische gegevens
 - Politiegegevens
- Vanwege de gevolgen
 - Mogelijk inperking van rechten
 - Volgen / monitoren van mensen

Waarom JenV dit niet alleen kan | **Gezamenlijke opgave**



(ex-gedetineerden)

Complexiteit mbt gegevensuitwisseling

- Grondslag niet vanuit de AVG maar vanuit de materiewetten
- Materiewetten gericht op één domein of problematiek, weinig oog voor verbinding tussen domeinen en problematieken
- Regels over gegevensdeling gericht op bilaterale uitwisseling, en voorziet niet in multilaterale situaties
- Als de situatie en ieders rol duidelijk is kom je er vaak wel uit, de onduidelijkheid zit in de fase dat je nog moet verkennen of je überhaupt iets moet samen
- Wettelijke beroepsgeheimen en tuchtrecht en 'zelfgekozen beroepsgeheimen'
- Gebrek aan regie bij het Rijk op het onderwerp



Drie wielen om aan te draaien

1. Beter uitvoerbare Wetgeving en regie op het thema bij het Rijk
2. Inrichten van de samenwerking, de gegevensuitwisseling en de borging van de privacy door organisaties
3. Kennis en kunde van de professionals

Daar waar organisaties wel investeren in een goede inrichting en organisatie van de samenwerking, gegevensdeling en privacy, zie je dat er vertrouwen en begrip ontstaat en 'de privacy' veel minder als een belemmering wordt ervaren.



2. Juridische grondslag

Scope afbakening

- Grondslag voor gegevensverwerking gaat over: ondersteuning van individuen (evt. met het (gezins)systeem daaromheen) op casusniveau.
- De analyse en de grondslag gaat **niet** over:
 - Beleidsinformatie, statistiek
 - Voorspellende informatie obv (groeps)kenmerken, profiling
 - Geautomatiseerde besluitvorming
 - (Grootschalige) monitoring en toezicht
 - Fraudebestrijding en handhaving

Voor deze onderwerpen zijn aparte juridische analyses nodig voor het gebruik van persoonsgegevens. Dat valt buiten het bestek van dit (be)spreekuur.

Handvat gegevensuitwisseling zorg en veiligheid

- Juridische analyse van wat kan en mag
- Opgesteld door alle ketenpartijen gezamenlijk
- Geeft mbt gegevensuitwisseling:
 - de randvoorwaarden aan gegevensuitwisseling
 - Zorgvuldigheidseisen daarbij
 - Spelregels voor samenwerking
- Redenering is gemaakt voor zorg & veiligheidshuizen, maar breder toepasbaar



Verwerkingsverantwoordelijke

- Positie van het zorg- en veiligheidshuis of samenwerkingsverband:
 - Géén zelfstandige identiteit, géén eigen wettelijke taak
 - Samenwerking obv een convenant en privacyprotocol
 - Gezamenlijke verwerkingsverantwoordelijkheid (art. 26 overeenkomst)
- Ondersteuning door model samenwerkingsconvenant, model privacyprotocol
- Openstaande vraag: hoe kunnen FG's van deelnemende partijen hun toezichthoudende rol vervullen?

Grondslag voor gegevensuitwisseling

- Grondslag voor de verwerking:
 - Art. 6.1.e, 6.3 AVG: taak algemeen belang (N.B. art. 6.1.a toestemming is uitdrukkelijk niet een voldoende grondslag!)
 - In combinatie met specifieke taak uit materiewet (Wmo, Jeugdwet, PBW, WPG, Gemeentewet etc.)
 - Verwerking van bijzondere gegevens (art. 9 AVG) of strafrechtelijke gegevens (art. 10 AVG) op grond van de materiewet
 - Gebruik BSN en identificerende gegevens obv materiewetten
 - Het delen van gegevens gebeurt op grond van ieders eigen taak, er is géén gemeenschappelijke taak in de wet gedefinieerd
 - Extra eisen ivm verenigbaarheid van doelen (art. 6.4 AVG)
 - Rekening houdend met aanvullende eisen (medisch) beroepsgeheim (WGBO, materiewetten)

Belangen en vuistregels bij gegevensuitwisseling

- **A- belangen**: noodzakelijk voor een taak van de **verstrekker**
 - Toegestaan op basis van materiewet van de verstrekker
 - Aanvullende grond nodig bij wettelijke geheimhouding (bijv. medisch, jeugdhulp)
- **B-belangen**: noodzakelijk voor een taak van **zowel de verstrekker als de ontvanger**
 - Toegestaan op basis van materiewet van de verstrekker en van de ontvanger
 - Aanvullende grond nodig bij wettelijke geheimhouding
- **C-belangen**: de uitwisseling is noodzakelijk voor een taak van de ontvanger
 - Alleen toegestaan bij i) specifieke wettelijke bepaling, ii) toestemming, iii) bij een noodsituatie ('conflict van plichten' of bijv. art. 23 AVG)
 - Bij wettelijke geheimhouding of specifieke doelbinding iha niet toegestaan
- **Wettelijke bepaling tot verstrekken**: belangen doen er niet zo veel toe
 - Uitwisseling iha algemeen toegestaan
 - Aanvullende wettelijke eisen en/of basisbeginselen (art. 5 AVG) wel van toepassing



3. Werkwijze in de praktijk

Stappenplan beoordeling gegevensverwerking

1. Wat zijn de taken en werkzaamheden van de deelnemende organisaties?
2. Wat zijn de activiteiten en doelen voor de gegevensverwerking?
3. Welke gegevens zijn daarvoor noodzakelijk?
4. Beoordeel de juridische basis:
 - Taken uit materiewetten en AVG-eisen
 - Gebruik van bijzondere persoonsgegevens
 - Gebruik van strafrechtelijke gegevens
 - Gebruik van nummers en BSN
 - Evt. doorgifte naar derde landen
 - Specifieke geheimhoudingsverplichtingen

Hoe maak je een begin?

1. Begin bij de praktijk

- Wat willen we bereiken/weten/doen en gaat het om beleidsinformatie, casusbehandeling, vroegsignalering
- Hoe willen we dat gaan doen?
- Wie hebben we daarvoor nodig en vanuit welke taak of rol?
- Hoe ziet onze werkwijze er uit: fasen in het werkproces en doelen per fase
- Wat voor gegevens hebben we dan in elke fase nodig en waarom
- Hoe is de samenwerking en privacy geborgd (convenanten, protocol) pof wat is het plan daarvoor?

2. Juridische analyse, inrichtingsaspecten, vuistregels voor de professional

- Mogelijkheden en randvoorwaarden (beleid en juridisch)
- Zorgvuldige inrichting van de gegevensverwerking (beleid en management)
- Praktische handvatten voor de professionals



Werkwijze op organisatieniveau

- Bepalen samenwerkingspartners
 - Convenantpartners
 - Schilpartners
- Maak convenant: afspraken over wijze van samenwerken, verdeling verantwoordelijkheden e.d.
- Maak privacyprotocol: zie stappenplan
- Sturing door Stuurgroep

Werkwijze op casusniveau: 4 fasen



1. Aanmelding: door één van de partners
2. Triage: beoordelen
 - Is er sprake van multiproblematiek?
 - Is samenwerking noodzakelijk?
 - Valt het doel binnen doel van het samenwerkingsverband?
3. Casusoverleg / monitoring
 - Casusregie
 - Procesregie
4. Afschaling: periodieke herbeoordeling over samenwerking nog noodzakelijk is

Stap 2 is in feite de
beoordeling van de
basisbeginselen AVG

Vuistregels bij de samenwerking

1. Aanmelder is de leidende partij, die bepaalt de grondslag en regelt de bevoegdheidsverdeling
2. In triage wordt bepaald of er een casusregisseur nodig is, zo ja, dan wordt die de leidende partij
3. Strikte doelbinding ook bij verstrekking: gegevens alleen gebruiken waarvoor ze verstrekt zijn
4. Verstrekker van gegevens houdt zeggenschap over gebruik van gegevens
5. Géén verder gebruik van gegevens, gegevens worden niet 'mee naar huis' genomen
6. Toestemming is geen basis voor de samenwerking (behalve bij doorbreken medisch beroepsgeheim), wél transparantie naar betrokkene
7. Bij voorkeur verleent betrokkene instemming. Zo niet: hoe kan wel aan aarzeling van betrokkene tegemoet worden gekomen?
8. Als minder privacy-ingrijpende verwerking kán, dan móet dat (anoniem advies, minimalisatie, beperking bewaartermijn e.d.)



4. Nieuwe wettelijke ontwikkelingen

Wetgeving biedt eigenlijk onvoldoende grond

De Autoriteit Persoonsgegevens constateert dat gemeenten géén duidelijk beeld hebben van welke gegevens zij in het sociaal domein mogen verwerken, voor welke doelen zij dit mogen en op basis van welke grondslagen. Ook heeft geen van de 41 gemeenten duidelijk bepaald wat de rol van toestemming daarbij kan of moet zijn.

Grondslagen

De bepaling van de grondslagen voor de verwerking van persoonsgegevens bij de uitvoering van taken in het sociaal domein is complex. Dat komt omdat er verschillende domeinen en wetten zijn (de Jeugdwet, de Wmo 2015, de Participatiewet, de Wet gemeentelijke schuldhulpverlening en de Wet passend onderwijs) op grond waarvan gemeenten in het sociaal domein taken uitvoeren en persoonsgegevens verwerken.

Elke afzonderlijke wet bevat bepalingen over de verwerking van persoonsgegevens in dat specifieke domein. Gemeenten moeten de verschillende taken in het sociaal domein in samenhang met elkaar kunnen uitvoeren, maar deze wetten voorzien onvoldoende in een regeling voor deze integrale taakuitvoering. Ook is hiervoor geen overkoepelende wettelijke regeling aanwezig.

Toestemming

Gemeenten kunnen problemen bij het bepalen van de grondslagen voor de verwerking van persoonsgegevens in het sociaal domein niet vermijden door toestemming aan betrokkenen te vragen voor de verwerking van hun persoonsgegevens. Vooral niet als gemeenten die toestemming vragen in situaties waarin de betrokkenen afhankelijk zijn van de gemeente voor hulp, zoals de intake/toegangverlening. Betrokkenen kunnen daarbij niet in vrijheid toestemming geven.

Een 'onvrije' toestemming vormt geen grondslag. Gemeenten mogen dan alléén persoonsgegevens verwerken als zij zich kunnen baseren op een van de andere grondslagen uit artikel 8 van de Wet bescherming persoonsgegevens (Wbp).

- Rapport 'de rol van toestemming in het sociaal domein', AP, april 2016

Lopende wetgevingstrajecten en samenhang

Wetten in voorbereiding:

- Wetsvoorstel gegevensverwerking in samenwerkingsverbanden (WGS): gegevensuitwisseling tussen deelnemers vier wettelijke samenwerkingsverbanden: iCOV, RIEC, FeC en ZVH
- Wetsvoorstel Aanpak Meervoudige problematiek Sociaal Domein (WAMS): integrale aanpak sociaal en zorgdomein + verbinding strafrecht OOV – taken college b&w en gegevensuitwisseling partijen
- Wetsvoorstel Radicalisering: casusoverleg straf- en bestuursrechtpartners m.b.t. radicalisering
- Wetsvoorstel Straffen en beschermen: o.a. uitwisseling PI en college van b&w ten behoeve van reïntegratie ex-gedetineerden op 5 basisvoorwaarden
- Wetsvoorstel vroegsignalering schulden: uitwisseling instanties met college van b&w mbt betalingsachterstanden ten behoeve van voorkomen problematische schulden

Recent in werking getreden:

- Wvvgz, Wzd en Wfg (1-1-2020)
- Herziene verplichte meldcode huiselijk geweld en kindermishandeling (1-1-2019)



5. Bredere context

Bredere toepasbaarheid?

- Kenmerken van bovenstaande redenering voor zorg & veiligheidshuizen:
 - Ondersteuning van kwetsbare mensen
 - Samenwerkende partijen
 - Bij multiproblematiek
 - Waar samenwerking noodzakelijk is om het probleem op te lossen
 - Op grensvlak zorg & veiligheid, inclusief de soms 'botsende' paradigma's van die domeinen
 - Gebruik van medische gegevens
 - Gebruik van strafrechtelijke en justitiële gegevens
 - Nav privacywetgeving eisen aan werkwijze en zorgvuldigheid



Onderwerpen in onderzoek bij de VNG en IBD

- Veiligheidsdomein:
 - Mensenhandel
 - Ondernijning
 - Radicalisering
- Zorgdomein:
 - Meldpunten niet-acute zorg
 - Gegevensdeling mbt bemoeizorg
 - Verkennend onderzoek in de Wvvgz
- Sociaal domein:
 - Sociale wijkteams (Wmo, Jeugdwet)
 - Jongeren 18-26, aansluiting onderwijs, werk en zorg
 - Werk & Inkomen en GGZ



Voorbeelden van wat we hiervoor (willen) ontwikkelen

(in willekeurige volgorde)

- Handreikingen privacy & gegevensdeling
- Model convenanten, model privacyprotocol
- Training aan
 - uitvoerende professionals
 - beleidsmakers, privacy-officers
- E-Learning modules
- Voorlichtingsbijeenkomsten, sessies op conferenties
- Bundeling van goede voorbeelden
- (referentie) DPIA, c.q. algemene effectbeoordeling (art. 35.10 AVG)

In het algemeen samen met de ketenpartners en de betrokken ministeries!

Ondersteuning vanuit IBD

Handreikingen en stappenplannen over privacy / AVG!!



HOME

ACTUEEL

OVER DE IBD

DIENSTEN VAN DE IBD

PRIVACY

PRODUCTEN

Producten Informatiebeveiliging & Privacy

Hieronder is een overzicht gemaakt van kennisproducten op het gebied van Informatiebeveiliging en Privacy.

Producten
Informatiebeveiliging

Producten
Privacy





6. Discussie, vragen, spreekuur!

Ingediende vragen

1. Wat gaan de handreikingen UPP en de Wams voor gemeenten opleveren?
2. Hoe kan de persoonlijke levenssfeer van betrokkenen goed beschermd blijven als de mogelijkheden voor domeinoverstijgende gegevensuitwisseling vergroot worden? Hoe zorg je voor een juiste belangenafweging tussen betrokkenen en organisatie? Hoe maak je een zorgvuldige omgang met persoonsgegevens aantoonbaar?
3. De relatie wie is waarvan? Hoe is de relatie verantwoordelijke/verwerker.
4. Ik zou naast aanpak Ondernijning ook graag aandacht willen voor aanpak Persoonsgerichte aanpak.
5. In Hoorn is een document in voorbereiding over samenwerking tussen gemeente (wijkcoördinator, openbare orde en toezicht), politie, jongerenwerk (Stichting Netwerk) en woningbouwcorporatie. De samenwerking bestaat al lang (Rondje Overlast). Tijdens overleg worden overlastsituaties besproken. Besproken wordt wat elke partij kan doen om de overlast aan te pakken. Lukt het niet om de overlast te beëindigen dan wordt er opgeschaald bijv. door een persoonsgerichte aanpak. **Vraag**: wat is er minimaal nodig is om de samenwerking goed te laten functioneren in het Rondje Overlast? Tevens is er discussie of voor het bespreken van overlastsituaties een DPIA nodig is.

Ingediende vragen (vervolg)

6. Uniforme en gedragen richting. Zit nog wel eens verschil tussen ALV VNG richting en landelijke gemeentelijke "domeinspecifieke" gremia. Praktijk: "Landelijk hebben wij met meerdere 100.000 plus gemeenten besloten om dit en dit te doen en het risico te nemen" of "De G5 doet /mag dit wel dus wij ook".
7. Hoe betrek je de verantwoordelijke medewerkers erbij en hoe houdt je ze betrokken?
8. Welke handvatten worden meegegeven aan collega's die binnen een wijkteam samenwerken met o.a. politie en zorginstellingen?
9. In een samenwerking met politie valt gemeente onder de AVG en politie onder Wpg. Is het noodzakelijk om 'convenant-partner' (art. 20 Wpg) te zijn van politie om goed samen te kunnen werken? Hebben andere gemeenten ervaring met het afsluiten van zulke convenanten? Is het ook mogelijk om een convenant gebaseerd op de AVG af te sluiten met politie, of moet een convenant voldoen aan Wpg-eisen voordat uitwisselen van informatie mogelijk is?



Aanvullende vragen?



Evaluatie bespreekuur

Adviezen en tips voor verbetering?

Suggesties voor vervolgonderwerpen?

- **Niet behandelde vragen worden nagestuurd.**
- Contact: privacy@vng.nl



Vervolg

- Woensdag 27 mei om 10:30: Thema Big Data & Open Data

- Contact: privacy@vng.nl