

Privacy Protocol

Problematische (jeugd)groepen met hoog risico zorg-en veiligheidshuis Haaglanden

tussen ketenpartners zorg- en veiligheidshuis Haaglanden



Veiligheidshuis

Inhoudsopgave

Artikel 1: Definities	5 -
Artikel 2: Afzonderlijke en Gezamenlijke Verwerkingsverantwoordelijken	7 -
Artikel 3: Doel Verwerking Persoonsgegevens	7 -
Artikel 4: Categorieën Persoonsgegevens	8 -
Artikel 5: Verwerkingen en verstrekkingen van persoonsgegevens ten behoeve van het behandelen van een casus.....	8 -
5.1 Verwerking van persoonsgegevens door de Procesregisseur.....	8 -
5.2 Verstrekken van persoonsgegevens ten behoeve van het casusoverleg.....	9 -
5.3 Verstrekken van gegevens bij het uitvoering geven aan afspraken uit het casusoverleg	9 -
Artikel 6: Grondslag voor het verwerken en verstrekken van persoonsgegevens ten behoeve van het behandelen een casus en de van toepassing zijnde taken van partijen	9 -
Artikel 7: Doorverwerking geheimhoudingsbepalingen en toepassing toestemmingsvereiste	11 -
Artikel 8: Documentatie individuele verstrekkingen	12 -
Artikel 9: Dataminimalisatie	12 -
Artikel 10: Kwaliteit	12 -
Artikel 11: Bewaren en Vernietigen.....	12 -
Artikel 12: Beveiliging	13 -
Artikel 13: Geheimhouding.....	13 -
Artikel 14: Datalekken	14 -
Artikel 15: Privacy by Design	15 -
Artikel 16: Informatieverstrekking aan Betrokkenen	16 -
Artikel 17: Rechten van de Betrokkenen	17 -
Artikel 18: Recht op inzage	17 -
Artikel 19: Recht op correctie en verwijdering.....	18 -
Artikel 20: Recht op bezwaar.....	18 -
Artikel 21: Recht op overdraagbaarheid van Persoonsgegevens	19 -
Artikel 22: Verwerkers	19 -
Artikel 23: Verstrekking aan derden	19 -
Artikel 24: Verwerkingsregister en Functionaris Gegevensbescherming.....	19 -
Artikel 25: Aansprakelijkheid	20 -
Artikel 26: Toezicht en handhaving	20 -
Artikel 27: Wijzigingen	20 -
Artikel 28: Toetreding	21 -
Artikel 29: Duur, opzegging, beëindiging.....	21 -
Artikel 30: Opvolging	21 -
Artikel 31: Monitoring, toezicht, audit, wetenschappelijk onderzoek en evaluatie	21 -
Artikel 32: Toepasselijk recht	22 -

Bijlage 1: Toetredingsformulier nieuwe partner tot Protocol

Bijlage 2: Doeleinden Verwerking van Persoonsgegevens per processtap

Bijlage 3: Categorieën Persoonsgegevens en Betrokkenen

De ondergetekenden:

De colleges van burgemeester en wethouders en de burgemeesters, ieder voor zover het zijn bevoegdheid betreft, van de gemeenten:

- Den Haag;
- Delft;
- Leidschendam-Voorburg;
- Midden-Delfland;
- Pijnacker-Nootdorp;
- Rijswijk;
- Wassenaar;
- Westland;
- Zoetermeer;

verder *afzonderlijk* aangeduid als 'Partij' of 'Gemeente' en *gezamenlijk als 'Gemeenten'*,

en

- Politie regionale eenheid Den Haag;
- Openbaar Ministerie;
- Reclassering Nederland;
- Leger des Heils reclassering;
- Fivoor;
- Parnassia Groep;
- GGZ Delfland;
- GGZ Rivierduinen;
- Jeugdbescherming West;
- Raad voor de kinderbescherming;
- Veilig Thuis;
- GGD Haaglanden;
- Goodwillwerk Leger des Heils Regio Den Haag;
- Dienst Justitiële Inrichtingen Haaglanden;
- Middin;
- Teylingereind;
- Limor;
- Perspektief;
- JIT;
- Stichting Humanitas;
- William Schrikker Stichting;
- Kessler Stichting;
- Stichting Exodus;
- SHOP Den Haag;
- Stichting Barka;

hierna afzonderlijk te noemen 'Partij' en gezamenlijk, inclusief Gemeente[n], te noemen 'Partijen',

de volgende overwegingen in aanmerking nemende:

- Partijen in het kader van samenwerking op het gebied van integrale veiligheid en complexe casuïstiek zoals beschreven in het Landelijke Kader het zorg- en veiligheidshuis Haaglanden (hierna: 'het zorg- en veiligheidshuis') hebben opgezet;
- Partijen voor deze samenwerking afspraken hebben vastgelegd in het Convenant 'Samenwerking tussen ketenpartners in zorg- en veiligheidshuis Haaglanden, gesloten op nnb' (verder: het Convenant), waar dit Privacy Protocol deel van uitmaakt;
- voor de samenwerking in het zorg- en veiligheidshuis de uitwisseling van gegevens, waaronder Persoonsgegevens, tussen de Partijen noodzakelijk is;
- in het door Partijen opgezette zorg- en veiligheidshuis Persoonsgegevens worden verwerkt ten dienste en onder verantwoordelijkheid van Partijen;
- Partijen slechts die Persoonsgegevens binnen het zorg- en veiligheidshuis delen die noodzakelijk zijn voor het doel van de samenwerking;
- op de samenwerking wet- en regelgeving met betrekking tot de bescherming van Persoonsgegevens van toepassing is waarbij Partijen conform deze wet- en regelgeving willen samenwerken;
- dit Privacyprotocol (verder aangeduid als: 'het Protocol') de gedragsregels omschrijft bij het verstrekken en verder Verwerken van Persoonsgegevens door Partijen in het kader van de samenwerking op het gebied van integrale veiligheid en complexe multi-problematiek, alsook de verschillende verantwoordelijkheden met het oog op de rechten en plichten uit toepasselijke privacy wet- en regelgeving, belegd;
- met dit Protocol reeds invulling wordt gegeven aan de in Artikel 26 van de Europese Algemene Verordening Gegevensbescherming neergelegde verplichting voor Partijen om op een transparante wijze hun samenwerkingsafspraken en hun verantwoordelijkheden jegens elkaar en jegens Betrokkene vast te leggen;
- dit Protocol aansluit bij het bepaalde in het 'Landelijk Kader Veiligheidshuizen' van het Ministerie van Veiligheid en Justitie, vastgesteld in januari 2013 (verder aangeduid als: 'het Landelijk Kader') en het 'Handvat Gegevensuitwisseling in het zorg en veiligheidsdomein – een juridisch handvat voor zorg- en veiligheidshuizen', versie 1.1. van juli 2017, (verder aangeduid als: 'het Handvat'), alsmede bij de in het Handvat en het Landelijk Kader gebezigde terminologie;
- dit Protocol aansluit bij het bepaalde in het 7 stappen model (opgesteld vanuit het CCV) en landelijk opgestelde document 'Werkproces integrale aanpak problematische jeugdgroepen en groepsgedrag', versie 1.0 van 8 maart 2016;
- dit privacy protocol verder wordt aangehaald als 'het Protocol'.

verklaren te zijn overeengekomen:

Artikel 1: Definities

In dit Protocol en de daarbij behorende bijlage(n) wordt verstaan onder:

- 1.1. *Groepsaankpak*: De groepsaankpak omvat verschillende sporen; de groepsgerichte interventies, de gebiedsgerichte interventies, de gebiedsgerichte interventies inclusief ondermijning en persoonsgebonden aanpak. Voor problematische (jeugd)groepen met het label hoog risico vindt de persoonsgerichte aanpak op het Veiligheidshuis Haaglanden plaats.
- 1.2. *Persoonsgegevens*: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de Betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon (artikel 4 lid 1 AVG).
- 1.3. *Politiegegevens*: elk Persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (artikel 1, sub a, Wpg).
- 1.4. *Strafvorderlijke gegevens*: Persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafforderlijk onderzoek en die het openbaar ministerie in een straf dossier of langs geautomatiseerde weg verwerkt in een gegevensbestand (artikel 1 sub b Wjsg).
- 1.5. *Justitiële gegevens*: bij algemene maatregel van bestuur omschreven Persoonsgegevens of gegevens over een rechtspersoon inzake de toepassing van het strafrecht of de strafforderding, die in een bestand worden Verwerkt (artikel 1 sub a Wjsg, respectievelijk Bjsjg).
- 1.6. *Tenuitvoerleggingsgegevens*: persoonsgegevens of gegevens over een rechtspersoon inzake de tenuitvoerlegging van strafrechtelijke beslissingen, die in een dossier of een ander gegevensbestand zijn of worden verwerkt.
- 1.7. *Bijzondere Persoonsgegevens*: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van 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, zoals bedoeld in artikel 9 AVG).
- 1.8. *Strafrechtelijke persoonsgegevens*: Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (zoals bedoeld in artikel 10 AVG).
- 1.9. *Verwerken*: 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 (artikel 4 lid 2 AVG).
- 1.10. *Betrokkene*: de natuurlijke persoon op wie informatie, waaronder Persoonsgegevens, betrekking heeft (artikel 4 lid 1 AVG).
- 1.11. *Derde*: een natuurlijk persoon of rechtspersoon, niet zijnde de betrokkene, noch één der Partijen.
- 1.12. *Verwerkingsverantwoordelijke(n)*: een natuurlijk 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; wanneer de doelstellingen van en de middelen voor deze Verwerking in het Unierecht of het lidstatelijk recht is vastgesteld, kan daarin reeds zijn bepaald wie de

- Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen (artikel 4 lid 7 AVG).
- 1.13. *Afzonderlijke Verwerkingsverantwoordelijken*: Partijen zijn Afzonderlijke Verwerkingsverantwoordelijke voor zelfstandige Verwerkingen en wanneer verschillende Verwerkingen min of meer geïntegreerd zijn, maar geen sprake is van Gezamenlijke Verwerkingsverantwoordelijken.
 - 1.14. *Gezamenlijke Verwerkingsverantwoordelijken*: Van Gezamenlijke Verwerkingsverantwoordelijkheid is sprake wanneer Verwerkingen zijn geïntegreerd, en niet één Partij als Verwerkingsverantwoordelijke kan worden aangemerkt voor de geïntegreerde Verwerkingen. In dat geval zijn de Partijen Verwerkingsverantwoordelijken voor het geheel van de Verwerking.
 - 1.15. *Verwerker*: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt (artikel 4 lid 8 AVG).
 - 1.16. *Casusregie*: het uitvoeren van werkzaamheden gericht het bewaren van de onderlinge samenhang bij het uitvoeren van het plan van aanpak bij het behandelen van één specifieke Casus.
 - 1.17. *Procesregie*: het uitvoeren van werkzaamheden gericht op de totstandkoming van samenwerking tussen Partijen bij het behandelen van één specifieke Casus en de ondersteuning van de Casusregisseur bij de uitvoering van het plan van aanpak.
 - 1.18. *Casus*: een persoon of situatie die voldoet aan de criteria voor de problematische (jeugd)groep en die is Aangemeld door de gemeente bij het zorg- en veiligheidshuis voor bespreking in het Casusoverleg.
 - 1.19. *Aanmelding*: De gemeente meldt aan welke personen in de groepsaanpak op het veiligheidshuis worden besproken. Dit gebeurt door de Procesregisseur
 - 1.20. *Casusoverleg*: fase waarin overleg plaats vindt door Partijen gericht op de totstandkoming van een plan van aanpak, afstemming tijdens de uitvoering daarvan, en het beoordelen of Casus kan worden afgeschaald.
 - 1.21. *Afschaling*: fase die volgt op het besluit genomen door de Procesregisseur in afstemming met de casuscoördinator dat de betrokkenheid van het zorg- en veiligheidshuis niet langer nodig is, waarin het dossier dat in het systeem van het zorg- en veiligheidshuis is aangelegd ten behoeve van procesregie, geschoond wordt van alle niet langer noodzakelijke informatie, en uiteindelijk verdwijnt uit het systeem van het zorg- en veiligheidshuis; Dit gebeurt na instemming door de driehoek.
 - 1.22. *Procesregisseur*: de medewerker van de Gemeente die namens de burgemeester is belast met de werkzaamheden in artikel 12 van het Convenant.
 - 1.23. *Casuscoördinator*: de medewerker van een van de Partijen die is belast met de taken in artikel 13 van het Convenant.
 - 1.24. *Informatiecentrum*: de medewerkers van het zorg-en veiligheidshuis die belast zijn met de ondersteunende werkzaamheden met betrekking tot de werkprocessen.
 - 1.25. *Manager*: de persoon die is belast met de taken zoals geformuleerd in Artikel 9 van het Convenant.
 - 1.26. *Stuurgroep*: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 4 van het Convenant.
 - 1.27. *Partneroverleg*: het verband van afgevaardigden van Partijen zoals geformuleerd in Artikel 6 van het Convenant.
 - 1.28. *Privacyadviseur*: Ieder zorg- en veiligheidshuis heeft een medewerker die belast is met privacyadvisering of kan gebruik maken van een privacyadviseur van een gemeente. Deze persoon is ook belast met beleidsontwikkeling over gegevensverwerking en helpt mee met de voorbereiding van audits.

- 1.29. *Jaarplan*: het door de Stuurgroep op grond van Artikel 4.4 van het Convenant vastgestelde plan betreffende de operationele en inhoudelijke kaders en het financieel en inhoudelijk beleid van het zorg- en veiligheidshuis.
- 1.30. *Werkprocessen*: Het 7 stappenmodel (het CCV) en Werkproces integrale aanpak problematische jeugdgroepen en groepsgedrag (versie 1.0).
- 1.31. *AVG*: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
- 1.32. *Wjsg*: Wet justitiële en strafvorderlijke gegevens.
- 1.33. *Bjsg*: Besluit justitiële en strafvorderlijke gegevens.
- 1.34. *Wpg*: Wet politiegegevens.

Artikel 2: Afzonderlijke en Gezamenlijke Verwerkingsverantwoordelijken

- 2.1. Partijen in het zorg- en veiligheidshuis zijn Afzonderlijk Verwerkingsverantwoordelijke voor de Persoonsgegevens die zij verstrekken aan de Procesregisseur en aan Partijen in het kader van het Casusoverleg en Afschaling.
- 2.2. Partijen in het zorg- en veiligheidshuis zijn conform artikel 26 Algemene Verordening Gegevensbescherming Gezamenlijk Verwerkingsverantwoordelijken voor de Persoonsgegevens die zij, anders dan de verstrekking zoals bedoeld in artikel 2.1, Verwerken op locatie of in de informatiesystemen van het zorg- en veiligheidshuis in het kader van de samenwerking voor de doeleinden zoals omschreven in artikel 3.
- 2.3. Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis door personeel van het zorg- en veiligheidshuis geschiedt onder gezag van de Partij die de betreffende Persoonsgegevens heeft verstrekt. Deze Partij wordt voor die Verwerking aangeduid als Verwerkingsverantwoordelijke.

Artikel 3: Doel Verwerking Persoonsgegevens

- 3.1. Dit Protocol ziet op alle Verwerkingen van Persoonsgegevens door Partijen in het kader van de uitvoering van artikel 2.2 van het Convenant.
- 3.2. Het verwerken van Persoonsgegevens in het zorg- en veiligheidshuis vindt plaats met als doel het gezamenlijk door Partijen bijdragen aan de veiligheid als onderdeel van het integrale zorg- en veiligheidsbeleid van de Gemeente(n). De samenwerking is meer specifiek gericht op het voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit en maatschappelijke uitval bij complexe problemen, door een combinatie van repressie, bestuurlijke interventie én zorg, hetgeen gezien moet worden als een zwaarwegend algemeen belang. Meer specifiek draagt de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis bij aan:
 - a. het oplossen van complexe multi-problematiek, problematiek waarbij personen die het subject zijn in de casuïstiek te maken hebben met meerdere problemen die op meer dan één leefgebied spelen;
 - b. het voorkomen van (verder) crimineel en/of overlast-gevend gedrag of verder afglijden van die personen;
 - c. Verbeteren toekomstperspectief van personen die subject zijn in de casuïstiek;
 - d. Voorkomen van instroom naar de groepsaankpak vanuit het (gezins)systeem;
 - e. het oplossen van ernstige lokale of gebiedsgebonden veiligheidsproblematiek; en
 - f. het mogelijk maken van samenwerking met het oog op de hierboven geformuleerde doeleinden.
- 3.3. Om het onder artikel 3.2 geformuleerde doel te bereiken Verwerken Partijen gezamenlijk de nodige Persoonsgegevens in het kader van het Casusoverleg en Afschaling. Voor elk van deze fasen in het werkproces zijn specifieke doelen voor de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis van toepassing. Deze doelen zijn gespecificeerd in Bijlage 2.

- 3.4. Partijen Verwerken de Persoonsgegevens die zij in het kader van de samenwerking onder dit Protocol hebben verkregen niet voor andere doeleinden dan de doelen omschreven in artikel 3.2.
- 3.5. Bij het Verwerken van Persoonsgegevens in het zorg- en veiligheidshuis worden de volgende uitgangspunten in acht genomen:
- a. er is sprake van een strikte doelbinding per fase van de voor de te Verwerken Persoonsgegevens en alleen de voor het doel van die fase noodzakelijke persoonsgegevens worden verwerkt;
 - b. als het doel van de Verwerking van Persoonsgegevens wijzigt, of, de casus gaat door naar een volgende fase, wordt als eerste opnieuw beoordeeld of de eerder verwerkte gegevens ook daarvoor noodzakelijk zijn en vervolgens of de gegevens daarvoor ook (verder) gebruikt mogen worden;
 - c. een partner die in een bepaalde fase Persoonsgegevens verstrekt behoudt de zeggenschap over het verdere gebruik van die gegevens en of die voor een andere fase en/of andere doelen gebruikt mogen worden;
 - d. partners die bij de behandeling van een casus kennisnemen van Persoonsgegevens afkomstig van een andere partner mogen deze gegevens enkel verder gebruiken voor hun eigen taken in het kader van de casusbehandeling, als de partner die de gegevens heeft ingebracht, dit afzonderlijk accordeert.

Artikel 4: Categorieën Persoonsgegevens

- 4.1. In het kader van de samenwerking worden door Partijen van de in Bijlage 4 categorieën Betrokkenen de daarin genoemde categorieën Persoonsgegevens Verwerkt:
- 4.2. Partijen Verwerken Persoonsgegevens, inclusief Bijzondere en Strafrechtelijke Persoonsgegevens, binnen de wettelijke kaders van de voor iedere Partij toepasselijke wet- en regelgeving.
- 4.3. Partijen Verwerken Persoonsgegevens voor de onder artikel 3.2 geformuleerde doeleinden enkel in de informatiesystemen van het zorg- en veiligheidshuis, of in de door de Stuurgroep aangewezen informatiesystemen en conform het beveiligingsbeleid Veiligheidshuis Haaglanden.

Artikel 5: Verwerkingen en verstrekkingen van persoonsgegevens ten behoeve van het behandelen van een casus

5.1 Verwerking van persoonsgegevens door de Procesregisseur

- 5.1.1 De Procesregisseur verwerkt persoonsgegevens ten behoeve van de procesregie in het kader van de doelstellingen van de samenwerking zoals verwoord in artikel 3.2 slechts voor zover dit noodzakelijk is voor het bewerkstelligen van de in de desbetreffende fase aan de orde zijnde doelen voor gegevensverwerking als verwoord in artikel 3.3 en bijlage 2.
- 5.1.2 De Procesregisseur verwerkt de in het eerste lid bedoelde persoonsgegevens ten behoeve van een goede taakuitoefening van de aanmeldende partij, dan wel de goede taakuitoefening van de partij onder wiens verantwoordelijkheid de casusregisseur zoals verwoord in artikel 13 van het convenant valt.
- 5.1.3 Voor de verwerking van persoonsgegevens als bedoeld in artikel 5.1.1 zijn van toepassing de grondslag conform de AVG en/of andere wettelijke grondslag, en de wettelijke bepalingen op grond waarvan de aanmeldende partij, dan wel de partij onder wiens verantwoordelijkheid de casusregisseur valt, de casus heeft aangemeld respectievelijk de casusregie voert.
- 5.1.4 De verantwoordelijke voor de verwerking van persoonsgegevens zoals bedoeld in artikel 5.1.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.2 van dit protocol.

5.2 Verstrekken van persoonsgegevens ten behoeve van het casusoverleg

- 5.2.1 Partijen kunnen persoonsgegevens inbrengen in het kader van de doelstellingen van de samenwerking zoals verwoord in artikel 3.2 slechts voor zover dit noodzakelijk is voor het bewerkstelligen van de in de desbetreffende fasen aan de orde zijnde doelen voor gegevensverwerking als verwoord in artikel 3.3 en bijlage 2.
- 5.2.2 Persoonsgegevens als bedoeld in artikel 5.2.1 worden slechts ingebracht indien dit noodzakelijk is voor de goede vervulling van de eigen taak, en/of de goede uitvoering van de taak van de partij ten behoeve waarvan de werkzaamheden in het kader het casusoverleg worden uitgevoerd.
- 5.2.3 De grondslag conform de AVG voor het inbrengen van persoonsgegevens als bedoeld in artikel 5.2.1 wordt ontleend aan de eigen taak, en/of de taak van de partij ten behoeve waarvan de werkzaamheden in het kader van het casusoverleg worden uitgevoerd.
- 5.2.4 De verantwoordelijke voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.2.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.1 van dit protocol.

5.3 Verstrekken van gegevens bij het uitvoering geven aan afspraken uit het casusoverleg

- 5.3.1 Onverminderd het bepaalde in artikel 6 en 7, kunnen partijen persoonsgegevens verstrekken aan een andere partij in het kader van de doelstellingen van de samenwerking zoals verwoord in artikel 3.2 voor zover deze noodzakelijk zijn voor deze partij bij:
 - a. het uitvoering geven aan interventies en acties die in het casusoverleg zijn afgesproken;
 - b. het voeren van de casusregie op het plan van aanpak als dat in het casusoverleg is afgesproken;
 - c. het toebedelen van de casus aan een specifieke partij ten behoeve van verdere afhandeling, zoals het adviseren van de aanmelder of het aanbrengen van de casus bij een andere overlegtafel.
- 5.3.2 De grondslag conform de AVG voor het verstrekken van persoonsgegevens als verwoord in artikel 5.3.1 wordt ontleend aan de eigen taak en/of de taak van de partij die de activiteiten onder artikel 5.3.1 a t/m c uitvoert.
- 5.3.3 De verantwoordelijke voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.3.1 betreft de verantwoordelijke zoals bedoeld in artikel 2.3.

Artikel 6: Grondslag voor het verwerken en verstrekken van persoonsgegevens ten behoeve van het behandelen een casus en de van toepassing zijnde taken van partijen

- 6.1 De grondslag voor de verwerking van persoonsgegevens als bedoeld in artikel 5.1.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. Voor gegevens afkomstig van het Openbaar Ministerie, is de grondslag gelegen in de artikel 8a, 39f en 51c Wet justitiële en strafvorderlijke gegevens.
- 6.2 De grondslag voor het inbrengen van persoonsgegevens als bedoeld in artikel 5.2.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de aanmeldende partner, dan wel de partner onder wiens verantwoordelijkheid de casusregisseur valt, en/of de verstrekken partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens. De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
- 6.3 De grondslag voor de verstrekking van persoonsgegevens als bedoeld in artikel 5.3.1, is artikel 6 AVG lid 1 sub e, voor zover deze noodzakelijk zijn voor de uitvoering van taken van Algemeen belang door de ontvangende partij en/of de verstrekken partij. Voor de gegevens afkomstig van de politie is de grondslag gelegen in artikel 20 Wet politiegegevens.

- De grondslag voor het verstrekken van justitiële, strafvorderlijke en/of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg.
- 6.4 De onder 6.1, 6.2 en 6.3 bedoelde grondslag kan bij casussen slechts van toepassing zijn indien dit voortvloeit uit de goede uitvoering van de taken en werkzaamheden van partijen, en de verwerking plaats vindt namens of de verstrekking plaats vindt aan een van de onder a t/m l genoemde partijen en voorwaarden:
- a. het bestuursorgaan de burgemeester: de goede uitvoering van taken en de uitoefening van bevoegdheden van de burgemeester, waaronder in het bijzonder taken en bevoegdheden op het gebied van Openbare Orde en Veiligheid zoals neergelegd in de Gemeentewet artikel 172;
 - b. het bestuursorgaan het College van B&W: de goede uitvoering van taken van het College van B&W, waaronder in het bijzonder taken in het sociaal domein zoals bedoeld in de WMO artikel 2.3.1 t/m 2.3.5, de Jeugdwet artikel 2,3 en 2.4, de Participatiewet artikel 7.1, en de wet schuldhulpverlening artikel 3;
 - c. het Openbaar Ministerie: voor de strafrechtelijke handhaving van de rechtsorde alsmede andere bij de wet vastgestelde taken (artikel 124 Wet op de Rechterlijke organisatie). De grondslag voor het verstrekken van justitiële, strafvorderlijke of tenuitvoerleggingsgegevens is gelegen in de artikelen 8a, 39f en 51c van de Wjsg;
 - d. de Politie: vervulling van taken zoals bedoeld in de Politiewet artikel 3, te weten taken op het gebied van opsporing, handhaving van de rechtsorde en hulp aan hen die dat behoeven. De grondslag voor het verstrekken van persoonsgegevens inclusief politiegegevens is gelegen in artikel 20 Wpg. Deze verstrekkingen dienen nader te zijn vastgelegd in de onlosmakelijk bij dit Privacy-protocol behorende en ondertekende Artikel 20 Wpg Beslissing, waarin staat vermeld dat er alleen artikel 8 en 13 Politiegegevens worden verstrekt. De Artikel 20 Beslissing wordt ondertekend door de gemandateerde politiechef van de Eenheid, en het gezag te weten de Burgemeesters en de Officier van Justitie. In artikel 7 zijn nadere voorwaarden benoemd die van toepassing zijn op gegevens die in het kader van deze taken worden verstrekt;
 - e. de Raad voor de Kinderbescherming: de goede uitvoering van de taken van de Raad voor de Kinderbescherming, waaronder in het bijzonder taken zoals bedoeld in boek 1 afdeling 3 van het Burgerlijk Wetboek, waaronder de artt. 1:240 BW en de artt. 1:255 juncto 1:257 BW, de artt. 77o en 77hh van het Wetboek van Strafrecht, de artt. 126 nd en 491 van het Wetboek van Strafvordering alsmede art. 28 van het Besluit Tenuitvoerlegging Jeugdstrafrecht 1994, de Algemene Wet Bestuursrecht, de artt. 2.4, 3.1 en 3.2 van de Jeugdwet alsmede art. 7.3.11 lid 4 van de Jeugdwet en art. 4 onder c, lid 1 van de Wet Opnemings Buitenlandse Kinderen ter Adoptie(wobka). Met inachtneming van het Kwaliteitskader 2016 van de Raad voor de Kinderbescherming;
 - f. Veilig Thuis: de goede uitvoering van de taken van het AMHK, waaronder in het bijzonder taken zoals bedoeld in de Wmo artikel 4.1.1, met inachtneming van het handelingsprotocol Veilig Thuis.¹ Veilig Thuis verstrekt informatie en neemt deel aan het Casusoverleg voor zover dit noodzakelijk moet worden geacht voor het doen van onderzoek naar of het stoppen van huiselijk geweld in afhankelijkheidsrelaties of kindermishandeling;
 - g. een Reclasseringsinstelling: de goede uitvoering van taken van de reclasseringsinstelling, waaronder in het bijzonder taken zoals bedoeld in de Reclasseringsregeling 1995 artikel 8 lid 1;

¹ Veilig Thuis is nog geen zelfstandige rechtspersoon die formeel gezien een convenant en protocol kan tekenen. De rechtspersoonlijkheid van Veilig Thuis is ondergebracht bij de GGD GHOR Nederland.

- h. een Gecertificeerde Instelling zoals bedoeld in de Jeugdwet artikel 1.1: de goede uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering zoals bedoeld in de Jeugdwet artikel 1.1;
 - i. een instelling voor Geestelijke Gezondheidszorg: de uitvoering van de taken bij behandeling, verpleging, verzorging en begeleiding van personen met een psychische stoornis, inclusief verslaving met of zonder verblijf in het kader van de Wgbo of de Wet bopz;
 - j. een GGD: de uitvoering van de taken in het kader van de OGGZ op grond van artikel 1.2.1. sub a Wmo 2015;
 - k. de Dienst Justitiële Inrichtingen: de Dienst Justitiële Inrichtingen: voor de uitvoering van taken van de Minister van Justitie en Veiligheid, de selectiefunctionaris en de directeur van een justitiële inrichting op grond van de Beginselenwet justitiële jeugdinrichtingen, de Beginselenwet verpleging ter beschikking gestelden, de Penitentiaire beginselenwet en het Interimbesluit forensische zorg (per 1-1-2019 de wet Forensische zorg). De wettelijke grondslag voor de verwerking en verstrekking van persoonsgegevens is na inwerkingtreding van de wijziging van de Wet justitiële en strafvorderlijke gegevens (Wjsg) ter implementatie van de Europese richtlijn gegevensbescherming opsporing en vervolging gelegen in de Wjsg;
 - l. Een aanbieder zoals bedoeld in de Wmo artikel 1.1.1, zorgaanbieder zoals bedoeld in de Wlz artikel 1.1.1, dan wel een jeugdhulpaanbieder zoals bedoeld in de Jeugdwet artikel 1.1: voor de verlening van voorzieningen en/of de uitvoering van zorg- dan wel hulpverleningstaken en voor zover dit noodzakelijk is in het kader van de behandeling of hulpverlening.
- 6.5 Op de persoonsgegevens die worden verwerkt, ingebracht, en/of verstrekt zoals bedoeld in artikel 5 zijn uitdrukkelijk de uitgangspunten van artikel 3.5 van toepassing en het bepaalde in artikel 7.

Artikel 7: Doorverwerking geheimhoudingsbepalingen en toepassing toestemmingsvereiste

- 7.1 De geheimhoudingsbepaling van artikel 7 Wpg blijven rusten op de verstrekte gegevens. Dit geldt voor de ontvanger maar ook voor de tweede en derde ontvanger. Wanneer er over betrokkene in een eerder stadium op grond van artikel 16 lid 1b onder 2 Wpg politiegegevens zijn verstrekt aan de burgemeester óf op grond van artikel 15 Wpg politiegegevens ter beschikking zijn gesteld aan een Buitengewone Opsporingsambtenaar van een gemeente óf op grond van het Besluit politiegegevens (Bpg), voor een ander doel politiegegevens zijn verstrekt aan een van de convenantpartijen, dan worden deze gegevens door de desbetreffende ontvanger in principe niet als persoonsgegevens door verstrekt aan de Procesregisseur van het Zorg- en Veiligheidshuis. Bij voorkeur worden door de politie op grond van artikel 20 Wpg opnieuw actuele politiegegevens verstrekt aan de Procesregisseur van het Zorg- en Veiligheidshuis voor de doelen zoals genoemd in artikel 3.2, 3.3 en bijlage 2. De politie kan in uitzonderingsgevallen ook toestemming geven aan de ontvanger voor doorversterking aan de Procesregisseur van het zorg- en veiligheidshuis maar legt deze toestemming vast in haar systemen.
- 7.2 Indien voor het inbrengen en/of verstrekken van persoonsgegevens zoals bedoeld in de artikelen 5.2 en 5.3 toestemming noodzakelijk is voor doorbreken geheimhoudingsbepalingen zoals bijvoorbeeld verwoord in de Wgbo (artikel 7:457 BW) en artikel 88 wet big, de beroepscode van de Jeugdzorgwerker artikel J, beroepscode NIP artikel 71 t/m 87 (psycholoog), of beroepscode NVO artikel 8 (pedagoog), de Reclasseringsregeling 1995 artikel 37, dan:
- a. wordt deze gevraagd op het moment dat duidelijk is dat het inbrengen of verstrekken noodzakelijk is t.b.v. van de in de betreffende fase aan de orde zijnde doelen, of de uitvoering van de in 5.3.1 a t/m c genoemde activiteiten;

- b. worden deze persoonsgegevens uitsluitend verstrekt voor zover hiervoor de uitdrukkelijke toestemming is verkregen van de betrokkene of diens wettelijke vertegenwoordiger;
- c. legt de partij die de toestemming heeft verkregen deze schriftelijk vast en informeert Betrokkene dat hij zijn toestemming altijd weer kan intrekken;
- d. draagt de partij die toestemming heeft verkregen bij intrekking van die toestemming er zorg voor dat er geen verdere verstrekkingen meer plaats vinden;
- e. maakt de betrokken zorg- of hulpverlener een eigen afweging conform de voor hem geldende professionele standaarden, indien toestemming niet verkregen wordt en hij ervan overtuigd is dat zich hier een conflict van plichten voordoet, of goed hulpverlenerschap het verstrekken van persoonsgegevens verlangd.

Artikel 8: Documentatie individuele verstrekkingen

- 8.1. Indien Partijen daartoe verplicht zijn door voor hen geldende materiewetgeving, dan leggen zij de afzonderlijke verstrekkingen van Persoonsgegevens, inclusief onderbouwing van de noodzakelijkheid daarvan met het oog op de in artikel 5 en 6 vastgelegde grondslagen, vast. Dit geldt ten minste voor politie en OM. De politie documenteert iedere verstrekking conform de documentatieplicht van art 32 Wpg, het Openbaar Ministerie conform artikel 39j Wjsg.

Artikel 9: Dataminimalisatie

- 9.1 Partijen Verwerken niet meer Persoonsgegevens dan noodzakelijk met het oog op de in artikel 2.1 van dit Protocol geformuleerde doeleinden.
- 9.2 In het Casusoverleg Verwerken Partijen alleen die Persoonsgegevens die noodzakelijk zijn voor het opstellen en uitvoeren van een integraal plan van aanpak.
- 9.3 In het kader van Afschaling verwerken Partijen alleen die Persoonsgegevens die noodzakelijk zijn om te bepalen of het plan van aanpak in het Casusoverleg tot de gewenste resultaten heeft geleid. Indien wordt besloten dat behandeling van de Casus in het zorg- en veiligheidshuis niet of niet langer noodzakelijk is, worden de betreffende Persoonsgegevens niet langer in het zorg- en veiligheidshuis Verwerkt. De Procesregisseur ziet erop toe dat Persoonsgegevens conform artikel 11 worden geanonimiseerd of vernietigd.
- 9.4 Wanneer de Partij die Persoonsgegevens in het zorg- en veiligheidshuis heeft verstrekt, kennis verkrijgt over de onjuistheid van die Persoonsgegevens, informeert die Partij de Casusregisseur en Procesregisseur hierover. De Procesregisseur coördineert de eventuele correctie van Persoonsgegevens in het zorg- en veiligheidshuis.
- 9.5 Enkel de Procesregisseur, Casusregisseur, Manager, een medewerker van het Informatiecentrum en afgevaardigden van Partijen in het Casusoverleg hebben toegang tot de Persoonsgegevens die worden Verwerkt op locatie of in het informatiesysteem van het zorg- en veiligheidshuis en enkel voor zover noodzakelijk voor hun rol in een specifieke Casus.

Artikel 10: Kwaliteit

- 10.1 Partijen dragen er zorg voor dat de Persoonsgegevens die zij in het kader van de onder artikel 3.2 geformuleerde doeleinden verstrekken toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig zijn. De Partij die Persoonsgegevens in het zorg- en veiligheidshuis verstrekt blijft verantwoordelijk voor de juistheid, actualiteit en nauwkeurigheid van die Persoonsgegevens.

Artikel 11: Bewaren en Vernietigen

- 11.1 Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel of de doeleinden waarvoor ze worden Verwerkt zoals geformuleerd onder artikel 3 en met inachtneming van artikel 9.

- 11.2 Persoonsgegevens worden vernietigd zodra de Verwerking daarvan niet langer nodig is voor het doel waarvoor zij zijn Verwerkt, maar uiterlijk binnen 1 jaar na het besluit tot Afschaling.
- a. persoonsgegevens kunnen tot zes maanden na besluit tot Afschaling worden bewaard in een vorm waarmee enkel de Procesregisseur en informatiecentrum toegang hebben tot de gegevens;
 - b. na zes maanden na besluit tot Afschaling worden persoonsgegevens gearhiveerd en heeft enkel de Manager toegang tot die Persoonsgegevens;
 - c. na één jaar na besluit tot Afschaling worden de Persoonsgegevens vernietigd.
- 11.3 Na één jaar kunnen gegevens, niet zijnde Persoonsgegevens, enkel worden bewaard voor managementdoeleinden.

Artikel 12: Beveiliging

- 12.1 Partijen dragen zorg voor passende technische en organisatorische beveiligingsmaatregelen om Persoonsgegevens te beschermen tegen verlies of enige vorm van onrechtmatige Verwerking zoals omschreven in Bijlage 3. Die maatregelen betreffen onder meer, maar niet uitsluitend, maatregelen met betrekking tot de toegang tot Persoonsgegevens, alsook het gebruik van beveiligde verbindingen voor de verstrekking van Persoonsgegevens.
- 12.2 Wanneer Persoonsgegevens aan andere Partijen worden verstrekt, gebeurt dit uitsluitend op een adequaat beveiligde manier, conform de geldende beveiligingsnormen voor de betreffende gegevens.
- 12.3 De gemeente Den Haag draagt zorg voor de adequate beveiliging van Persoonsgegevens die worden Verwerkt op locatie en in de informatiesystemen van het zorg- en veiligheidshuis en rapporteert hierover indien nodig aan de Stuurgroep.
- 12.4 De Manager is verantwoordelijk voor het toezien op de naleving van de beschermingsmaatregelen zoals geformuleerd in het informatieveiligheidshuis Haaglanden voor de Verwerking van Persoonsgegevens op locatie en in de informatiesystemen van het zorg- en veiligheidshuis en rapporteert hierover aan de gemeente Den Haag en is bevoegd aanwijzingen te geven aan Partijen omtrent de juiste omgang met Persoonsgegevens in dat verband.

Artikel 13: Geheimhouding

- 13.1. Een ieder die op grond van dit Protocol kennis neemt van Persoonsgegevens is verplicht tot geheimhouding daarvan, tenzij de wet tot bekendmaking verplicht. De Manager, Procesregisseur en eventueel ander ondersteunend personeel van het zorg- en veiligheidshuis worden door middel van een geheimhoudingsverklaring tot geheimhouding gebonden.
- 13.2. Partijen dragen er zorg voor dat iedere medewerker die in de uitvoering van het Convenant of dit Protocol in aanraking komt met Persoonsgegevens geheimhouding van die gegevens waarborgt.
- 13.3. Alle medewerkers van het zorg- en veiligheidshuis, inclusief medewerkers op basis van een dienstverleningsovereenkomst, deelnemers aan Casusoverleggen en overige afgevaardigden van Partijen die toegang hebben tot Persoonsgegevens die onder dit Protocol worden Verwerkt, beschikken over een positieve Verklaring Omtrent Gedrag, danwel hebben een veiligheidsonderzoek op grond van de voor de eigen organisatie geldende wet- en regelgeving doorlopen.
- 13.4. Wettelijke geheimhoudingsplichten zijn onverminderd van toepassing op eenieder die Strafrechtelijke persoonsgegevens of andere Bijzondere Persoonsgegevens in het kader van de samenwerking in het zorg- en veiligheidshuis ontvangt.
- 13.5. De Partijen in het samenwerkingsverband mogen de Persoonsgegevens afkomstig van de politie en Openbaar Ministerie slechts verwerken voor het specifieke doel waarvoor deze zijn verstrekt ten behoeve van de Casus. Deze Persoonsgegevens mogen alleen verder worden Verwerkt door de ontvangende Partijen indien het doel van de verdere verwerking

verenigbaar is met dit doel waarvoor de Persoonsgegevens zijn verstrekt. Onverenigbaar gebruik van de gegevens, ook intern binnen de organisaties van de ontvangende Partijen, is niet toegestaan.

- 13.6. De Partijen in het samenwerkingsverband mogen de Persoonsgegevens afkomstig van andere Partijen die aan een geheimhoudingsplicht als onder meer bedoeld in de Wet Geneeskundige behandelovereenkomst (artikel 7:457 BW), Reclasseringsregeling 1995, Jeugdwet of Wet Maatschappelijke Ondersteuning zijn gebonden, slechts Verwerken voor het specifieke doel van de casus waarvoor deze zijn verstrekt. De Persoonsgegevens mogen alleen verder worden Verwerkt door de ontvangende Partijen met toestemming van de verstreckende Partij en indien het doel van de verdere verwerking verenigbaar is met dit doel waarvoor de Persoonsgegevens zijn verstrekt. Onverenigbaar gebruik van de Persoonsgegevens, ook intern binnen de organisaties van de ontvangende Partijen, is niet toegestaan.
- 13.7. Wanneer de grond voor het verstrekken van de Persoonsgegevens als bedoeld in lid 7 gebaseerd is op toestemming van Betrokkene als bedoeld artikel 6 lid 1 onder a AVG en/of artikel 9 lid 2 onder a AVG en Betrokkene trekt deze toestemming in, laat de verstreckende Partij dit aan de ontvangende Partij weten, waarbij ook de toestemming voor Verwerking en verdere Verwerking voor de ontvangende Partij vervalt.

Artikel 14: Datalekken

- 14.1. Partijen houden procedures in stand die er op gericht zijn om inbreuken in de beveiligingsmaatregelen zoals geformuleerd in Bijlage 3 met betrekking tot de bescherming van Persoonsgegevens redelijkerwijs te detecteren en daarop actie te ondernemen, daaronder begrepen maatregelen tot herstel.
- 14.2. De gemeente is verantwoordelijk voor het in stand houden van procedures zoals bedoeld in artikel 14.1 voor de Verwerking van Persoonsgegevens op locatie of in de informatiesystemen van het zorg- en veiligheidshuis. De Manager ziet toe op de naleving van deze procedures in het zorg- en veiligheidshuis.
- 14.3. Partijen stellen de Manager onverwijld maar uiterlijk binnen 24 uur na kennisneming op de hoogte van een inbreuk op persoonsgegevens in de zin van artikel 4, onder 12, AVG dan wel artikel 26g Wet justitiële en strafvorderlijke gegevens die een risico inhoudt voor de rechten en vrijheden van betrokkenen zoals bedoeld in artikel 33 AVG. Deze kennisgeving omvat in ieder geval:
- a. de aard en omvang van de inbreuk;
 - b. de contactgegevens van de persoon bij wie meer informatie over de inbreuk kan worden verkregen;
 - c. de maatregelen die kunnen worden genomen om de gevolgen van de inbreuk te voorkomen of beperken;
 - d. de mogelijke gevolgen en risico's van de inbreuk op de bescherming van Persoonsgegevens voor de Betrokkene;
 - e. de maatregelen die Partij zelf reeds heeft genomen of zal nemen om de bescherming van Persoonsgegevens te herstellen.
- 14.4. De Manager informeert Partijen middels het Partneroverleg schriftelijk over een inbreuk zoals bedoeld in artikel 14.3.
- 14.5. Partijen melden, indien wettelijk verplicht, een inbreuk zoals bedoeld in Artikel 14.3 bij de Autoriteit Persoonsgegevens. De Manager stuurt een afschrift van de melding aan de Autoriteit Persoonsgegevens aan het Partneroverleg en de Stuurgroep.
- 14.6. Wanneer een inbreuk als bedoeld in Artikel 14.3 waarschijnlijk een hoog risico voor de rechten en vrijheden van Betrokkene(n) zal inhouden als bedoeld in artikel 34 AVG, wordt deze over de inbreuk geïnformeerd. Partijen informeren de Betrokkene over de inbreuk. De beslissing tot melding aan de Betrokkene wordt in het Partneroverleg genomen. De inhoud

- van die melding wordt in het Partneroverleg afgestemd, danwel door het Partneroverleg aan één Partij gemandateerd.
- 14.7. Partijen verlenen elkaar de medewerking die redelijkerwijs van elkaar mag worden verwacht om aan de op Partijen rustende kennisgevingsverplichtingen te voldoen, mede met het oog op een eventueel onderzoek door de Autoriteit Persoonsgegevens.
- 14.8. Kennisgeving van de inbreuk aan de Autoriteit Persoonsgegevens door de Partijen gebeurt zonder onredelijke vertraging maar in ieder geval binnen 72 uur na ontdekking en geschiedt volgens de daartoe door de Autoriteit Persoonsgegevens ter beschikking gestelde procedure. De kennisgeving aan de Autoriteit Persoonsgegevens omvat minimaal:
- de aard van de inbreuk;
 - een omschrijving van de categorieën Betrokkenen van wie Persoonsgegevens zijn betrokken bij de inbreuk;
 - de categorieën Persoonsgegevens;
 - of de Persoonsgegevens zijn versleuteld, geanonimiseerd, of anderszins onbegrijpelijk zijn gemaakt;
 - de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
 - de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van de Persoonsgegevens en de maatregelen die Partij heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.
- 14.9. Kennisgeving van de inbreuk aan Betrokkene zoals bedoeld in Artikel 14.5 is niet vereist indien:
- passende technische en organisatorische maatregelen zijn genomen die de bescherming van Persoonsgegevens ook na de inbreuk garanderen;
 - achteraf genomen maatregelen de waarschijnlijkheid op een hoog privacy risico hebben weggenomen, of;
 - wanneer mededeling aan Betrokkene een onevenredig inspanning zou vragen.
- 14.10. Voorts kan de mededeling aan betrokkene worden uitgesteld, beperkt of achterwege gelaten worden, indien de inbreuk enkel ziet op gegevens afkomstig van het Openbaar Ministerie, en indien dit noodzakelijk en evenredig is:
- ter vermijding van belemmering van gerechtelijke onderzoeken of procedures;
 - ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
 - ter bescherming van de openbare veiligheid;
 - ter bescherming van de rechten en vrijheden van derden;
 - ter bescherming van de nationale veiligheid.
- 14.11. Partijen houden een overzicht bij van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van de Persoonsgegevens. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk, de gevolgen daarvan en de genomen corrigerende maatregelen, alsmede de tekst van de kennisgeving aan de Betrokkene. De Procesregisseur houdt een overzicht bij van gelijksoortige inbreuken die plaatsvinden op locatie of in de informatiesystemen van het zorg- en veiligheidshuis.

Artikel 15: Privacy by Design

- 15.1. Voorafgaand aan een (nieuwe) Verwerkingen onder dit Protocol, of de inzet van nieuwe technologieën voor de Verwerkingen onder dit Protocol, voeren Partijen middels het Partneroverleg een Gegevensbeschermingseffectbeoordeling uit conform artikel 35 AVG. De Manager coördineert dit proces.
- 15.2. Bij de uitvoering van de Gegevensbeschermingseffectbeoordeling wordt het model Gegevensbeschermingseffectbeoordeling Rijksdienst gevolgd.
- 15.3. Bij een voornemen omtrent de inzet van nieuwe technologieën kan dit voornemen ter advies worden voorgelegd aan het Landelijk Overleg Managers Veiligheidshuizen. Het Landelijk

Overleg Managers Veiligheidshuizen kan advies uitbrengen over de beoogde inzet van nieuwe technologieën.

- 15.4. De uitkomsten van de Gegevensbeschermingseffectbeoordeling worden ter besluitvorming voorgelegd aan de Stuurgroep. De Stuurgroep kan hiervoor advies vragen, aan het Partneroverleg over de voorgenomen nieuwe Verwerking zoals bedoeld in artikel 15.1. De Stuurgroep legt waar nodig op grond van artikel 36 AVG namens alle gezamenlijke Verwerkingsverantwoordelijken de beoogde Verwerking voor aan de Autoriteit Persoonsgegevens.

Artikel 16: Informatieverstreking aan Betrokkenen

- 16.1. Vóór het verstrekken van Persoonsgegevens in het kader van de samenwerking wordt Betrokkene door de aanmeldende partij geïnformeerd over het voornemen diens Persoonsgegevens verder te Verwerken in het kader van samenwerking in het zorg- en veiligheidshuis onder dit Protocol.
- 16.2. Deze informerende Partij maakt de het tijdstip waarop en de wijze van informeren kenbaar aan de overige bij een Casus betrokken Partijen.
- 16.3. De Manager draagt zorg voor het publiceren van een privacy statement op de website van het zorg- en veiligheidshuis.
- 16.4. Alle deelnemende partijen zorgen op hun eigen website voor vermelding van deelname aan het zorg- en veiligheidshuis en voor een verwijzing naar de website van het betreffende zorg- en veiligheidshuis/ de Veiligheidshuizen waaraan zij deelnemen, alsook voor verwijzing naar het zorg- en veiligheidshuis convenant(en) en het privacyprotocol(len).
- 16.5. De onder artikel 16.1 bedoelde informatieverstreking, alsook het onder artikel 16.3 genoemde privacy statement, bevatten ten minste de volgende informatie:
- a. de doeleinden voor de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis zoals beschreven in artikel 3.2;
 - b. de Partijen die deelnemen aan de samenwerking in het zorg- en veiligheidshuis;
 - c. de termijn waarvoor de Persoonsgegevens worden opgeslagen en bewaard zoals omschreven onder artikel 11, danwel de criteria voor het bepalen van die termijn;
 - d. dat Betrokkene verscheidene rechten heeft met betrekking tot de Verwerking van diens Persoonsgegevens zoals geformuleerd onder artikel 17 tot en met 21;
 - e. indien de Verwerking van Persoonsgegevens is gebaseerd op toestemming, dat Betrokkene het recht heeft deze te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de Verwerking van de Persoonsgegevens die heeft plaatsgevonden vóór intrekking van de toestemming;
 - f. dat Betrokkene het recht heeft een klacht in te dienen over de Verwerking van zijn of haar Persoonsgegevens onder dit Protocol bij het zorg- en veiligheidshuis en bij de Autoriteit Persoonsgegevens;
 - g. nadere uitleg indien de Persoonsgegevens moeten worden verstrekt of verder Verwerkt op grond van een wettelijke of contractuele verplichting;
 - h. nadere uitleg indien Betrokkene verplicht is de Persoonsgegevens te verstrekken;
 - i. indien sprake is van geautomatiseerde besluitvorming, met inbegrip van profilering, uitleg over de achterliggende logica, het belang van de verwerkingsactiviteiten en de verwachte gevolgen voor de Betrokkene;
 - j. de contactgegevens van de Procesregisseur bij wie de Betrokkene terecht kan voor meer informatie over de Verwerking van zijn Persoonsgegevens, dan wel waar hij zijn rechten geldend kan maken.
- 16.6. De informatieverplichting zoals bedoeld in artikel 16.1 is niet van toepassing indien het achterwege laten van informeren van Betrokkene noodzakelijk is in het belang van:
- a. de veiligheid van de staat;
 - b. de voorkoming, opsporing en vervolging van strafbare feiten;

- c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
 - d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c, of;
 - e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen.
- 16.7. Partijen leggen de motivatie voor het niet voldoen aan de informatieplicht op grond van Artikel 16.6 schriftelijk vast en leggen vast wanneer zij verwachten dat betrokkene wel geïnformeerd kan worden, alsook van welke omstandigheden dit afhankelijk is, hoe periodiek wordt getoetst of deze omstandigheden nog aanwezig zijn en hoe dan wel wanneer Betrokkene geïnformeerd zal worden.

Artikel 17: Rechten van de Betrokkenen

- 17.1. Betrokkenen kunnen bij Partijen een verzoek indienen om:
- a. inzage te krijgen in de Persoonsgegevens die door Partijen over hem of haar worden Verwerkt;
 - b. correctie of verwijdering van de hem betreffende Persoonsgegevens dan wel beperking van de Verwerking;
 - c. bezwaar te maken tegen de Verwerking;
 - d. zijn of haar Persoonsgegevens over te dragen.
- 17.2. Verzoeken door Betrokkene ten aanzien van Persoonsgegevens die worden Verwerkt op locatie of in het informatiesysteem van het zorg- en veiligheidshuis worden gecoördineerd door de Procesregisseur. De Procesregisseur wordt hierbij ondersteund door het informatiecentrum. De Procesregisseur legt het verzoek voor aan de betrokken partijen en stemt daarin met Partijen de beantwoording van het verzoek af.
- 17.3. Indien het verzoek als bedoeld in Artikel 17.1 direct is gericht aan een der Partijen wordt de Manager hierover zo spoedig mogelijk door die Partij in kennis gesteld, opdat deze de beantwoording van het verzoek conform artikel 17.2 kan coördineren. Beantwoording van het verzoek door de Partij wordt in het Partneroverleg afgestemd.
- 17.4. Het bepaalde in artikel 17.2 en artikel 17.3 ontslaat Partijen niet van diens verantwoordelijkheid als Verwerkingsverantwoordelijke ten aanzien van een verzoek van Betrokkene.
- 17.5. Artikel 17.1 t/m 17.4, alsmede de artikelen 18, 19 en 20 zijn niet van toepassing op gegevens die verstrekt zijn door het College van procureurs-generaal. Op deze gegevens is de Wet justitiële en strafvorderlijke gegevens van toepassing. Verstrekkingen van gegevens door het College van procureurs-generaal worden ingevolge artikel 8 van dit Protocol en artikel 39j Wjsg schriftelijk vastgelegd en bewaard voor de duur van 4 jaar. Inzage- en rectificatieverzoeken worden beoordeeld door de privacyfunctionaris van het verstreckende parket van het Openbaar Ministerie. Verzetschriften tegen verwerking van gegevens worden beoordeeld door de afdeling Bestuurlijke en juridische zaken van het Parket-Generaal.
- 17.6. Op gegevens die eerder verstrekt zijn door de politie is de geheimhoudingsplicht van de Wet politiegegevens van toepassing. Derhalve zijn artikel 18, 19 en 20 van dit Protocol niet van toepassing. Inzage- en correctieverzoeken worden beoordeeld door het Wpg loket van de verstreckende eenheid van de politie. Vezet- en bezwaarschriften tegen verwerking van gegevens worden beoordeeld door de privacyfunctionaris en/ of jurist van de verstreckende eenheid van de politie, conform art. 29 Wpg.

Artikel 18: Recht op inzage

- 18.1. In het geval het verzoek ziet op inzage in de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis door Partijen zoals bedoeld in artikel 17.1 onder a, dient de beantwoording van dat verzoek een volledig overzicht in begrijpelijke vorm met ten minste de volgende informatie te bevatten:
- a. de verwerkingsdoeleinden;

- b. de betrokken categorieën van Persoonsgegevens;
 - c. de ontvangers of categorieën van ontvangers aan wie de Persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
 - d. indien mogelijk, de periode gedurende welke de Persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
 - e. dat de Betrokkene het recht heeft de Verwerkingsverantwoordelijke(n) te verzoeken dat Persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
 - f. dat de Betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
 - g. wanneer de Persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
 - h. het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4 AVG bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de Betrokkene.
- 18.2. Het verzoek wordt binnen vier weken door de Manager beantwoord. Een verzoek tot inzage wordt enkel geweigerd, indien en voor zover dit noodzakelijk is met het oog op in de wet gespecificeerde weigeringsgronden.
- 18.3. Een eventuele (gedeeltelijke) afwijzing is schriftelijk en gemotiveerd.
- 18.4. Alvorens aan een verzoek als bedoeld in artikel 17.1 wordt voldaan, verifiëren Partijen de identiteit van de Betrokkene die het verzoek indient. Betrokkene dient hiervoor persoonlijk te identificeren bij het zorg- en veiligheidshuis.
- 18.5. Bij voldoen aan een verzoek als bedoeld in artikel 17.1, verstrekt de Manager namens de Verwerkingsverantwoordelijke aan de Betrokkene een kopie van de Persoonsgegevens die worden verwerkt.

Artikel 19: Recht op correctie en verwijdering

- 19.1. Indien de Betrokkene op grond van zijn verzoek om inzage een verzoek tot correctie of verwijdering van bepaalde hem of haar betreffende Persoonsgegevens zoals bedoeld in artikel 17.1 onder b doet bij het zorg- en veiligheidshuis, legt de Procesregisseur dit verzoek voor aan de deelnemers van het Casusoverleg met het oog op de beoordeling van het verzoek.
- 19.2. Onjuiste Persoonsgegevens betreffende de Betrokkene worden op diens verzoek onverwijld gecorrigeerd.
- 19.3. Persoonsgegevens betreffende de Betrokkene worden zonder onredelijke vertraging op diens verzoek verwijderd wanneer deze:
- a. voor het doel van de Verwerking onvolledig of niet ter zake dienend zijn; of
 - b. anderszins in strijd met een wettelijk voorschrift worden Verwerkt.
- 19.4. De gemeente informeert de Betrokkene over de beslissing omtrent zijn verzoek tot correctie of verwijdering van hem of haar betreffende Persoonsgegevens schriftelijk en gemotiveerd zo spoedig mogelijk, maar uiterlijk binnen 4 weken na ontvangst van het verzoek.

Artikel 20: Recht op bezwaar

- 20.1. Indien de Verwerking van Persoonsgegevens door Partijen is gebaseerd op de grondslagen van artikel 6 Algemene Verordening Gegevensbescherming, kan de Betrokkene daartegen te allen tijde bezwaar aantekenen in verband met zijn bijzondere persoonlijke omstandigheden.
- 20.2. Indien een verzoek tot bezwaar door Betrokkene bij één der Partijen wordt ingediend, informeert die Partij onverwijld de Manager over het ingediende verzoek.

- 20.3. De Manager legt het door Betrokkene ingeroepen recht tot bezwaar voor aan de betrokkenen bij het Casusoverleg om te beoordelen of het verzoek gerechtvaardigd is en coördineert de afhandeling daarvan.
- 20.4. De Manager informeert de Betrokkene over de beslissing zoals bedoeld in artikel 17.3 binnen 4 weken en draagt er zorg voor dat de beslissing binnen deze 4 weken wordt uitgevoerd. Een beslissing om niet, of niet geheel, te voldoen wordt altijd gemotiveerd en kan met het oog op artikel 21 AVG enkel worden gebaseerd op dwingende gerechtvaardigde gronden.

Artikel 21: Recht op overdraagbaarheid van Persoonsgegevens

- 21.1. Het recht op overdraagbaarheid van Persoonsgegevens is niet van toepassing op Partijen in het zorg- en veiligheidshuis.

Artikel 22: Verwerkers

- 22.1. Partijen besteden de Verwerking van Persoonsgegevens onder dit Protocol niet uit zonder dat de partijen tevoren schriftelijk toestemming heeft gegeven over de beoogde verandering inzake de inzet van Verwerkers die ten behoeve van het zorg- en veiligheidshuis Persoonsgegevens Verwerken.
- 22.2. Een overeenkomst van opdracht tussen Partijen en een door partijen goedgekeurde Verwerker inzake Verwerking van Persoonsgegevens dient ten minste hetzelfde beschermingsniveau te bieden aan de belangen van Betrokkene als het onderhavige Protocol. Meer in het bijzonder moet de Verwerker voor de Verwerkingen van Persoonsgegevens in het kader van dit Protocol een vergelijkbaar niveau van beveiliging garanderen als in Bijlage 3 van dit Protocol.
- 22.3. Partijen leggen de afspraken tussen hen en Verwerkers(s) omtrent de omgang met Persoonsgegevens die Verwerker ten behoeve van Partijen Verwerkt, in een schriftelijke overeenkomst vast. De Manager is bevoegd deze overeenkomst namens Partijen aan te gaan.
- 22.4. De Manager houdt een lijst bij van de overeenkomsten die met schriftelijke toestemming van de partijen zijn overeengekomen, welke lijst minimaal eenmaal per jaar wordt bijgewerkt. Deze lijst zal beschikbaar worden gehouden ten behoeve van Partijen en de toezichthouder.

Artikel 23: Verstrekking aan derden

- 23.1. Persoonsgegevens die in het kader van dit Protocol worden Verwerkt, worden niet verstrekt aan anderen dan deelnemers aan het Casusoverleg, behoudens het bepaalde in Artikel 19 en tenzij Partijen hiertoe wettelijk verplicht zijn. Deze verstrekking wordt schriftelijk vastgelegd door de Procesregisseur.
- 23.2. Indien een verstrekking van Persoonsgegevens aan derden plaatsvindt, is dat een individuele afweging van elke Partij op grond van zijn eigen wet- en regelgeving.

Artikel 24: Verwerkingsregister en Functionaris Gegevensbescherming

- 24.1. Partijen registreren hun Verwerkingen van Persoonsgegevens onder dit Protocol in een eigen register van verwerkingsactiviteiten.
- 24.2. Aanvullend neemt de Manager de Verwerkingen van Persoonsgegevens op locatie en in de informatiesystemen van het zorg- en veiligheidshuis op in een gezamenlijk register van verwerkingsactiviteiten onder dit Protocol ten behoeve van Partijen.
- 24.3. Het register van verwerkingsactiviteiten bevat minimaal de volgende informatie:
 - a. de naam en contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken (of diens vertegenwoordiger);
 - b. de verwerkingsdoeleinden;
 - c. een beschrijving van de categorieën Persoonsgegevens die worden Verwerkt;
 - d. een beschrijven van de categorieën Betrokkenen;

- e. de categorieën van ontvangers aan wie de Persoonsgegevens worden (of zullen worden) verstrekt;
 - f. indien van toepassing, doorgifte van Persoonsgegevens aan derde landen of internationale organisaties.
- 24.4. De Functionarissen Gegevensbescherming van de afzonderlijke Partijen hebben, zonder aankondiging van bezoek vooraf, recht op toegang tot de gebouwen en overleg ruimtes van het zorg- en veiligheidshuis en tot de Verwerkingen en register van Verwerkingen, alsook toegang tot enige andere informatie, voor zover dit noodzakelijk is voor diens toezichthoudende werkzaamheden.
- 24.5. De Privacy Adviseur van het zorg- en veiligheidshuis dient als eerste aanspreekpunt voor de betrokken Functionarissen Gegevensbescherming.
- 24.6. De Functionarissen Gegevensbescherming van de Verwerkingsverantwoordelijken houden toezicht op de naleving van de verplichtingen in dit Protocol en zijn bevoegd aanwijzingen te geven aan de Manager en Procesregisseur.

Artikel 25: Aansprakelijkheid

- 25.1. Partijen zetten zich in voor een goede uitvoering van het bepaalde in dit Protocol en zullen zich houden aan de dienaangaande in dit Protocol gemaakte afspraken.
- 25.2. Partijen zijn ieder voor zich aansprakelijk voor aanspraken van Betrokkenen, of Derden op schadevergoeding op grond van directe of indirecte schade, administratieve boetes of andere aanspraken van derden in geval van toerekenbare tekortkoming door de aangesproken Partij in de nakoming van het bepaalde in dit Protocol en de bijbehorende Bijlagen.
- 25.3. Wanneer meerdere Verwerkingsverantwoordelijken of Verwerkers bij dezelfde Verwerking betrokken zijn, en verantwoordelijk zijn voor schade die door die Verwerking is veroorzaakt, wordt elke Verwerkingsverantwoordelijke of Verwerker voor de gehele schade aansprakelijk gehouden teneinde te garanderen dat de betrokkene daadwerkelijk wordt vergoed.
- 25.4. Een Verwerker is slechts aansprakelijk voor de schade die door Verwerking is veroorzaakt wanneer bij de Verwerking niet is voldaan aan de specifiek tot Verwerkers gerichte verplichtingen van de Algemene Verordening Gegevensbescherming of buiten dan wel in strijd met de rechtmatige instructies van de Verwerkingsverantwoordelijke is gehandeld.
- 25.5. Onverminderd het gestelde in lid 4 kan iedere Verwerkingsverantwoordelijke of Verwerker die de volledige vergoeding heeft betaald vervolgens bij de andere Verwerkingsverantwoordelijken of Verwerkers die bij dezelfde Verwerking betrokken zijn, het deel van de schadevergoeding verhalen dat overeenkomt met hun deel van de aansprakelijkheid voor de schade. Een Verwerkingsverantwoordelijke of Verwerker kan door andere Verwerkingsverantwoordelijken of Verwerkers worden vrijgesteld van onderlinge betaling van schadevergoeding indien hij bewijst dat hij op geen enkele wijze verantwoordelijk is voor het schadeveroorzakende feit.

Artikel 26: Toezicht en handhaving

- 26.1. Onverminderd de verantwoordelijkheden van de Functionarissen Gegevensbescherming van de verwerkingsverantwoordelijken houden de Manager en de Procesregisseur toezicht op de naleving van de verplichtingen in dit Protocol en zijn bevoegd aanwijzingen te geven aan medewerkers in het zorg- en veiligheidshuis omtrent de uitvoering van het bepaalde in dit Protocol.

Artikel 27: Wijzigingen

- 27.1. De bepalingen in dit Protocol kunnen door de Partijen in gezamenlijk overleg worden gewijzigd. Wijzigingen in dit Protocol worden door de Stuurgroep besloten. Mondelinge mededelingen, toezeggingen of afspraken welke betrekking hebben op de inhoud van dit

Protocol, hebben geen rechtskracht, tenzij deze uitdrukkelijk schriftelijk zijn bevestigd door de Stuurgroep.

- 27.2. Wijziging van het Protocol vergt het opnieuw ondertekenen door Partijen van het gewijzigde Protocol.
- 27.3. In geval van wijzigingen, waaronder inbegrepen toetreding van een nieuwe organisatie tot dit Protocol, die door een Partij onaanvaardbaar worden ervaren, kan deze Partij deelname aan het zorg- en veiligheidshuis schriftelijk opzeggen met ingang van het tijdstip waarop het gewijzigde Protocol van kracht wordt. Na opzegging van deelname aan het Convenant en dit Protocol verkrijgt die Partij niet langer toegang tot de Persoonsgegevens die op locatie of in de informatiesystemen van het zorg- en veiligheidshuis worden verwerkt onder dit Protocol.

Artikel 28: Toetreding

- 28.1. Toetreding door andere organisaties tot dit Protocol kan enkel wanneer die Partij is toegetreden tot het Convenant conform Artikel 20 van dat Convenant.
- 28.2. Partijen worden vooraf door de secretaris van de Stuurgroep op de hoogte gebracht van de voorgenomen toetreding. Indien de toetredende partij niet staat benoemd in het Handvat dient voorafgaand aan de uitwisseling van Persoonsgegevens met de toetredende partij een juridische analyse te worden opgesteld conform hoofdstuk 5 van het Handvat. De toetredende Partij voert waar nodig de aanbeveling uit die analyse uit, alvorens uitwisseling van Persoonsgegevens in het zorg- en veiligheidshuis met die partij plaatsvindt.
- 28.3. In geval van toetreding tot het Convenant, vindt toetreding tot het Protocol plaats door middel van ondertekening van Bijlage 1 bij dit Protocol door die andere organisatie en de Manager veiligheidshuis Haaglanden.

Artikel 29: Duur, opzegging, beëindiging

- 29.1. Dit Protocol treedt in werking op de dag van ondertekening door Partijen en wordt voor dezelfde duur als het Convenant. In geval van verlenging van het Convenant wordt dit Protocol met een gelijklopende termijn verlengd.
- 29.2. De stuurgroep kan, zonder rechterlijke tussenkomst en met meerderheid van stemmen, na ingebrekestelling, een Partij met onmiddellijke ingang uitsluiten van de samenwerking in het zorg- en veiligheidshuis, indien de afspraken zoals neergelegd in dit Protocol niet door de desbetreffende Partij worden nagekomen.
- 29.3. Verplichtingen die naar hun aard zijn bestemd om ook na beëindiging of uitsluiting van het project voort te duren, blijven na beëindigingen van dit Protocol bestaan. Tot deze verplichtingen behoren onder meer die ter zake van geheimhouding en de beveiliging van Persoonsgegevens.

Artikel 30: Opvolging

- 30.1. Dit Protocol vervangt alle eerdere door Partijen gesloten Protocollen met betrekking tot de Verwerking van Persoonsgegevens in het zorg- en veiligheidshuis voor de doelen zoals beschreven in Artikel 3.1 van dit Protocol.

Artikel 31: Monitoring, toezicht, audit, wetenschappelijk onderzoek en evaluatie

31.1

- a. In het kader van een opdracht tot uitvoering van een wetenschappelijk onderzoek zijn Partijen gezamenlijk opdrachtgever en worden de specifieke bepalingen uit wet- en regelgeving alsmede de interne voor Partijen geldende voorschriften voor wetenschappelijk onderzoek van Partijen in acht genomen.
- b. Partijen zullen dit Protocol twee jaar na inwerking treden landelijk en regionaal evalueren, waarbij bij voorkeur een audit zal plaatsvinden door een externe onafhankelijke partij.

Artikel 32: Toepasselijk recht

32.1. Op dit Protocol is Nederlands recht van toepassing.

Aldus overeengekomen:

Gemeente Den Haag	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Mw. P.C. Krikke; Burgemeester	
Datum:	
5.1.2.e	

Gemeente Delft	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Mw. J.M. van Bijsterveldt, Burgemeester	
Datum:	
5.1.2.e	

Gemeente Leidschendam-Voorburg	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Dhr. K. Tigelaar, Burgemeester	
Datum:	
5.1.2.e	

Gemeente Midden-Delfland	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Dhr. A.J. Rodenburg, Burgemeester	
Datum:	
5.1.2.e	

Gemeente Pijnacker-Nootdorp	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Mw. F. Ravestein, Burgemeester	
Datum:	
5.1.2.e	

Gemeente Rijswijk	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Dhr. M.J. Bezuijen, Burgemeester	
Datum:	5.1.2.e
5.1.2.e	

Gemeente Wassenaar	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Dhr. J.F. Koen, (wnd) Burgemeester	
Datum:	5.1.2.e

Gemeente Westland	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Mw. A.M.A. van Ardenne, (wnd) Burgemeester	
Datum:	

Gemeente Zoetermeer	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Dhr. C.B. Aptroot, Burgemeester	
Datum:	5-12-2018
5.1.2.e	

Openbaar Ministerie, het College van procureurs-generaal	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Dhr. A.J.A.M. Nieuwenhuizen, Hoofdofficier van Justitie n.d. M. Zwinkels, plv HO	
Datum:	5-12-18
5.1.2.e	

Politie, Korpschef Politie	
<i>in dezen rechtsgeldig vertegenwoordigd door:</i>	
Dhr. P.J.A. Entken, Hoofd Operatiën/ plv. Politiechef	
Datum:	5.1.2.e
5.1.2.e	

Bijlage 1: Toetredingsformulier nieuwe partner tot Protocol

[naam organisatie], statutair gevestigd te [...] en kantoorhoudend aan [...], hierbij rechtsgeldig vertegenwoordigd door [naam, functie],

overwegende dat:

- deelname aan het Protocol gelet op de publieke en/of maatschappelijke taak die zichzelf in het kader van integrale veiligheid en complexe casuïstiek toedicht en gelet op de verantwoordelijkheid en/of bevoegdheid van ondergetekende een bijdrage levert aan de doelstelling zoals geformuleerd in artikel 2 van het Convenant en artikel 3.2 van het Protocol;
- de Stuurgroep positief heeft besloten op toetreding van ondergetekende aan het Convenant en dit Protocol;

verklaart daartoe het volgende:

- ondergetekende onderschrijft de in het Protocol geformuleerde doelstellingen, verplicht zich de bepalingen in het Protocol te zullen naleven en verklaart zich in dit kader gerechtigd tot het uitwisselen van Persoonsgegevens met Partijen.

Aldus ondertekend te [...], op datum [...]

Naam organisatie:

Naam bevoegde functionaris:

.....

Namens zorg- en veiligheidshuis Haaglanden:

Naam:

.....

Bijlage 2: Doeleinden Verwerking van Persoonsgegevens per processtap

Partijen Verwerken in het kader van het zorg- en veiligheidshuis voor ieder van onderstaande fasen enkel de Persoonsgegevens die voor die afzonderlijke fase noodzakelijk zijn voor de uitvoering van ieder van de daarbij geformuleerde toepasselijke processtappen: Hier verwijzen naar het vertaaldocument waarin alle processtappen zijn beschreven.

Casusoverleg

- opstellen gezamenlijk toestandsbeeld door bij het Casusoverleg betrokken Partijen;
- opstellen beeld onderlinge verbanden (jeugd)groep door bij het Casusoverleg betrokken partijen;
- opstellen integraal plan van aanpak, rekening houdend met rol en plek in (jeugd)groep;
- monitoren van de uitvoering en resultaten van het plan van aanpak;
- bepalen of verdere verstrekking van Persoonsgegevens aan andere samenwerkingsverbanden noodzakelijk en mogelijk is;
- besluiten tot afbouwen betrokkenheid zorg- en veiligheidshuis;
- besluiten tot Opschaling van de Casus;

Afschaling

- bepalen van noodzakelijke te verstrekken Persoonsgegevens in het kader van Afschaling en de verstrekking daarvan aan bijvoorbeeld de Casusregisseur.

Bijlage 3: Categorieën Persoonsgegevens en Betrokkenen

Partijen Verwerken ten behoeve van de doelstellingen en onder voorwaarden zoals beschreven in dit Protocol enkel de volgende categorieën Persoonsgegevens van de volgende categorieën Betrokkenen:

Categorie 1:

Categorie Betrokkenen:

Van Personen, op wie het onder dit Protocol beschreven plan van aanpak en bijbehorende interventies zijn gericht, worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:.

Persoonsgegevens:

- volledige personalia (naam, geboorteplaats, geboortedatum);
- adresgegevens (straat, huisnummer, postcode, woonplaats);
- contactgegevens (telefoonnummer, e-mailadres);
- gegevens omtrent woonsituatie;
- financiële gegevens;
- gegevens betreffende relaties met overige gezinsleden/ directe sociale contacten;
- toezicht- en handavingsgegevens, gegevens omtrent bestuursrechtelijke maatregelen of voornemens daartoe

Strafrechtelijke Persoonsgegeven, te weten:

- politiegegevens (artikel 8 en 13 Politiegegevens);
- strafvorderlijke gegevens en relevante justitiële gegevens;
- tenuitvoerleggingsgegevens

Bijzondere Persoonsgegevens:

- indien van toepassing en noodzakelijk voor de aanpak:
 - gezondheid;
 - seksueel leven;
 - levensovertuiging;
 - politieke opvattingen.

Categorie 2:

Categorie Betrokkenen:

Van directe relaties van Categorie1 Betrokkenen, waaronder gezinsleden en directe sociale contacten, worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:

Persoonsgegevens:

- volledige personalia (naam, geboortedatum, geboorteplaats);
- adresgegevens (straat, huisnummer, postcode, woonplaats);
- contactgegevens (telefoonnummer, e-mailadres);
- toezicht- en handavingsgegevens of omtrent bestuurlijke maatregelen of voornemens daartoe voor zo ver in directe relatie met Betrokkene van Categorie 1;
- gegevens omtrent inzage verzoeken, verzoeken om rectificatie, bezwaar en klachten.

Strafrechtelijke Persoonsgegeven, te weten:

- politiegegevens (artikel 8 en 13 Politiegegevens);
- strafvorderlijke gegevens.

Bijzondere Persoonsgegevens en gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten zoals bedoeld in artikel 9 en 10 AVG

Categorie 3:

Categorie Betrokkenen:

Van medewerkers van instanties of instellingen die betrokken zijn bij de begeleiding, zorg- en hulpverlening van betrokkene (ook interventies voorafgaande aan de Aanmelding), worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:

Persoonsgegevens:

- naam;
- naam organisatie organisatieaanduiding (typering bijv. instelling voor GGZ);
- contactgegevens (zakelijk telefoonnummer, e-mailadres);
- datum start betrokkenheid en einde betrokkenheid.

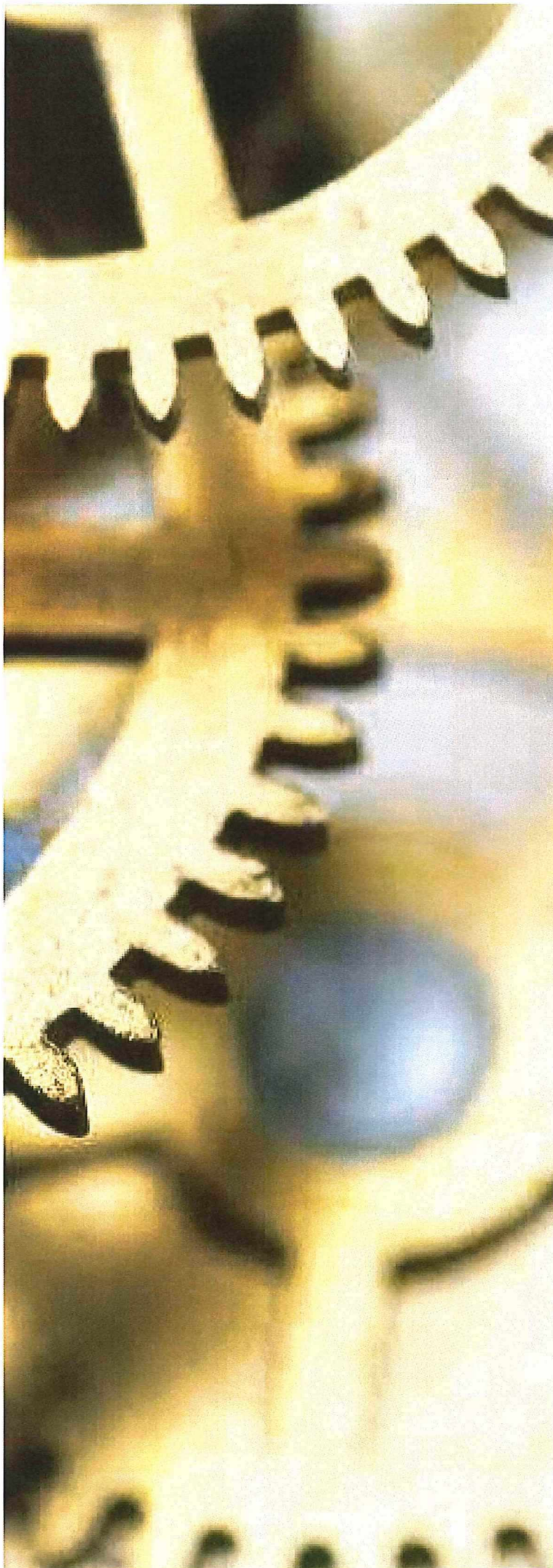
Categorie 4:

Categorie Betrokkenen:

Van Medewerkers van derden die betrokken zijn bij de uitvoering van interventies (ook interventies voorafgaande aan de Aanmelding), worden geen andere dan de volgende categorieën Persoonsgegevens verwerkt:

Persoonsgegevens:

- naam;
- naam organisatie organisatieaanduiding (typering bijv. instelling voor GGZ);
- functie binnen het zorg- en veiligheidshuis;
- contactgegevens (zakelijk telefoonnummer, e-mailadres);
- datum start betrokkenheid en einde betrokkenheid



Convenant

Persoonsgerichte aanpak voorkoming radicalisering en extremisme

CONVENANT PERSOONSGERICHTE AANPAK VOORKOMING RADICALISERING EN EXTREMISME

Inleiding

Dreiging

Het (mondiale) jihadisme vormt een substantiële en langdurige bedreiging voor de internationale veiligheid en stabiliteit en voor de veiligheid van Nederland. Het ontstaan van de Islamitische Staat in Irak en Syrië (ISIS) en het uitroepen van “het kalifaat” vormt een destabiliserende factor, zowel op lokaal, nationaal als mondiaal niveau. Deze internationale ontwikkelingen hebben hun weerslag op Nederland. Enerzijds doordat uit Nederland afkomstige jihadisten aansluiting zoeken bij internationale terroristische organisaties, anderzijds doordat aanhangers van het jihadisme zich ook in ons land openlijk manifesteren. In Nederland is de jihadistische beweging een kleine, maar gevaarlijke groepering die geweld legitimeert en propageert als middel om haar doelen te realiseren. Recente aanslagen, waaronder die in België, Turkije, Frankrijk en Duitsland, tonen het gebruik van geweld door extremisten op westers grondgebied.

De als gevolg van de oorlog in Syrië ontstane grootschalige asielstroom richting West-Europa wakkert ook in Nederland een heftig maatschappelijk debat aan over de opvang van vluchtelingen, (gebrek aan) invloed op de besluitvorming en gevoelens van onveiligheid en van tweedeling in de maatschappij. Deze polarisatie kan een voedingsbodem zijn voor radicalisering en kan de weerbaarheid van individuele personen sterk beïnvloeden. Ook kunnen links- en rechts-extremistische groeperingen in reactie hierop extra in beweging komen.

Deze ontwikkelingen leiden tot een dreiging tegen de democratische rechtsorde die verschillende vormen aanneemt. Reeds enige tijd is de kans dat in Nederland een aanslag wordt gepleegd substantieel¹. De druk op de open en vrije samenleving neemt toe door de groeiende invloed van personen en organisaties die aanzetten tot afzondering, onverdraagzaamheid en soms zelfs tot haat en daarmee de vrijheid en ontwikkeling van anderen proberen in te perken. De burger staat hierbij in meerdere opzichten centraal, want uiteindelijk zijn het burgers die zich bedreigd voelen of een bedreiging vormen, polariseren of samenbrengen, kwetsbaar of weerbaar blijken en dader of slachtoffer kunnen zijn.

Taken en verantwoordelijkheden

De overheid, in de breedste zin des woords, staat vanuit verschillende taken en verantwoordelijkheden voor de uitdaging om deze dreiging te beperken en te keren. Zo heeft de overheid een taak in het maatschappelijk debat en de inrichting van de samenleving, heeft zij mede een belangrijke taak in de participatie en de ondersteuning van hulpbehoeftigen in de samenleving en heeft zij mede een taak ten aanzien van de psychosociale zorg en de ontwikkeling van personen. Ook is zij verantwoordelijk voor de integriteit van overheidsinstituties, de handhaving van de rechtsorde en de veiligheid.

¹ Zie het Dreigingsbeeld Terrorisme Nederland (DTN) 32 t/m 42.

De overheid bestaat uit verschillende organen en instanties, met eigen taken en verantwoordelijkheden:

- Het bestuur en de volksvertegenwoordiging geven, met journalisten, wetenschappers en opiniemakers, richting aan het maatschappelijk debat door de gemeenschappelijke normen en waarden actief uit te dragen, door de grenzen aan te geven waarbinnen dat debat kan plaatsvinden, door het debat te faciliteren en erop toe te zien dat iedereen in vrijheid daaraan kan deelnemen.
- De gemeente (het college van burgemeester en wethouders) heeft als kerntaken onder meer burgerzaken, milieu, zorg en welzijn, veiligheid en openbare orde, werk en inkomen, jeugd en onderwijs en infrastructuur. De gemeente speelt een belangrijke rol bij de participatie van zorgbehoeftigen, onder andere gehandicapten, ouderen, werklozen, jeugdigen en asielzoekers of vreemdelingen met een verblijfvergunning. Zij speelt onder meer een rol bij de basisbehoeften en faciliteren een basisniveau op het gebied van wonen, inkomen, onderwijs, cultuur en sport. Op deze manier kunnen mensen zich ontwikkelen en meedoen in de samenleving.
- De burgemeester, de politie en het Openbaar Ministerie hebben de taak om te zorgen voor een zo veilig mogelijke leefomgeving. Van personen van wie aanleiding is te veronderstellen dat zij een gevaar vormen voor de veiligheid, wordt een inschatting gemaakt van de aard en omvang van die dreiging. Daders van strafbare feiten worden waar mogelijke en opportuun opgespoord en vervolgd en de openbare orde wordt gehandhaafd.
- De Raad voor de Kinderbescherming heeft tot taak om te komen tot een onbedreigd ontwikkelingsperspectief voor het kind. Hoewel ouders het recht én de plicht hebben om hun kinderen op te voeden, komt de ontwikkeling van een kind soms ernstig in gevaar doordat ouders hun verantwoordelijkheid niet kunnen nemen of doordat vrijwillige hulp stagneert of onmogelijk is. In dat geval moet de overheid ingrijpen. Het belang van het kind staat immers voorop.
- De Reclasseringsinstellingen hebben tot taak bij te dragen aan de veiligheid van de samenleving door het beheersen van risico's en veroordeelden of verdachten te stimuleren zijn of haar gedrag te veranderen. Op die manier werken zij aan het voorkomen van criminaliteit en het terugdringen van recidive. De reclasseringsinstellingen begeleiden de uitvoering van straffen en maatregelen en ander beslissingen van justitiële instanties.

De overheid staat bij het realiseren van deze taken niet alleen. Aan het daadwerkelijk omarmen van het gewelddadige gedachtengoed gaat een proces van radicalisering vooraf, dat niet altijd op eenduidige wijze verloopt. Van personen die zich vanuit hun diepste overtuiging afkeren van onze democratische rechtsorde kan slechts tot een optimale aanpak worden gekomen als de overheid, dat wil zeggen al die verschillende organen en instanties, vanuit hun eigen taak en verantwoordelijkheid, als één geheel werkt aan de oplossing van de bredere problematiek en samenwerkt met andere maatschappelijke instellingen die hierbij een rol kunnen spelen. In deze gevallen is het geheel meer dan de som der delen. Het kan hierbij gaan om instellingen van maatschappelijk werk, instellingen voor de geestelijke gezondheidszorg, stichtingen voor reclassering, (jeugd)zorgaanbieders en gecertificeerde (jeugd)hulpinstellingen. Zo kunnen

instellingen voor de geestelijke gezondheidszorg personen met een psychiatrische aandoening helpen zoveel mogelijk de regie over hun eigen leven te houden, hen helpen om hun rol in de samenleving weer op te pakken en met hen werken aan ontwikkeling of herstel van de zelfstandigheid.

Deze verschillende taken en verantwoordelijkheden vormen, samen met onze fundamentele normen en waarden, een belangrijk deel van de fundering van de democratische rechtsorde waarop onze samenleving is gebaseerd. Dat het fundament van onze open en vrije samenleving door extremistische en / of terroristische groeperingen wordt bedreigd brengt mee dat een gemeenschappelijke en integrale aanpak op persoonsniveau noodzakelijk is.

Verdediging en versterking rechtsorde

In de Nationale Contraterrorismestrategie is de inzet van het kabinet en de lokale partners voor de komende jaren weergegeven. Onderdeel van de nationale aanpak van terrorisme en extremisme is een multidisciplinair casusoverleg in alle betrokken gemeenten, dat is gericht op het voorkomen van radicalisering en op deradicalisering van diegenen die er reeds extremistische denkbeelden op nahouden. Deze multidisciplinaire aanpak is een gezamenlijke verantwoordelijkheid van de lokale veiligheids- en zorginstanties. Waar dit voor de casuïstiek noodzakelijk is, werken de betrokken landelijke en lokale partijen intensief samen in een casusoverleg. Vanuit hun eigen rol en gelet op hun eigen taak en verantwoordelijkheid, dragen deze organisaties bij aan de verdediging en versterking van de democratische rechtsorde. Doel van dit samenwerkingsverband is daarmee de risico's voor de samenleving die uitgaan van radicalisering, extremisme, uitreizen of terugkeer te reduceren en zorg te bieden aan subjecten, waaronder minderjarigen. De deelnemende partijen wisselen waar nodig en mogelijk informatie uit, schatten het risico in dat van een persoon uitgaat en stellen aan de hand daarvan een persoonsgericht pakket met effectieve maatregelen samen. Het betreft hier maatregelen en/of interventies die door het bestuur, de strafrechtelijke instanties of door maatschappelijke instellingen kunnen worden getroffen.

Er is geen standaard aanpak mogelijk gebleken ten aanzien van personen die gevoelig zijn voor extremistisch gedachtengoed. Uit wetenschappelijk onderzoek naar radicalisering en uit de ervaringspraktijk blijkt dat er geen eenduidig profiel van "de jihadist" of "de terrorist" bestaat. Telkens spelen diverse (sociale, economische, culturele) factoren op meerdere niveaus een rol in processen van radicalisering. Een eenduidige verklaring bestaat dan ook niet. Ook is bekend dat risicogedrag niet alleen verband houdt met ideologische overtuiging. Dat betekent dat telkens, in elke casus, zorgvuldig gekeken moet worden naar de achterliggende oorzaken van risicogedrag. Vanuit dat inzicht in achterliggende oorzaken zal vervolgens, in iedere casus, bezien moeten worden welke aanpak en interventies nodig zijn. Dat vergt een persoonsgerichte aanpak en vereist nauwe samenwerking tussen en inzet van verschillende instanties en disciplines: van veiligheid tot specialistische zorg. Op basis van de specifieke omstandigheden van het geval wordt per casus op grond van een referentiekader met objectieve criteria beoordeeld of een persoonsgerichte, integrale benadering van het subject noodzakelijk is. Indien dit het geval is, wordt voor elke casus beoordeeld welke organen of instanties een taak hebben en betrokken dienen te worden bij de aanpak, en door welk organen of instanties derhalve relevante gegevens, waaronder ook persoonsgegevens, verwerkt moeten worden. Het is van belang dat deze gegevensverwerking rechtmatig en zorgvuldig

geschiedt en dat geheimhouding van de persoonsgegevens die de partners aan elkaar verstrekken wordt gegarandeerd. Dit wordt met de navolgende afspraken beoogd.

Partijen:

Kernpartijen

- a. De gemeente Den Haag;
- b. het Openbaar Ministerie, het College van procureurs-generaal, te dezen vertegenwoordigd door de Hoofdofficier van Justitie van het arrondissementsparket Den Haag;
- c. de politie, de korpschef van politie, te dezen vertegenwoordigd door de politiefchef van Den Haag;

Casuspartijen

- d. De Raad voor de Kinderbescherming, te dezen vertegenwoordigd door de gebiedsmanager Haaglanden;
- e. De Reclassering Nederland, te dezen vertegenwoordigd door de (wnd) regiodirecteur Zuid-West.

Overwegende dat:

- partijen, gelet op hun verantwoordelijkheid ten aanzien van het reduceren van risico's verbonden aan radicalisering, extremisme, uitreizen, of terugkeer en het bieden van zorg aan subjecten hebben besloten tot de instelling van een samenwerkingsverband, daarbij gebruik makend van hun wettelijke taken en bevoegdheden;
- in het samenwerkingsverband de bij de casuïstiek betrokken partijen in gezamenlijkheid komen tot de vaststelling van een integraal plan van aanpak ten aanzien van extremisten, geradicaliseerde personen of personen die dreigen te radicaliseren (zoals uitreizigers of potentiële uitreizigers en terugkeerders) onverlet reeds bestaande zorgkaders en / of andere samenwerkingsvormen die naast het casusoverleg bestaan;
- partijen het noodzakelijk achten dat de werkzaamheden van de betrokken partijen voor de uitvoering van het integraal plan van aanpak op doelmatige en effectieve wijze op elkaar aansluiten;
- voor de totstandkoming en uitvoering van het integraal plan van aanpak het noodzakelijk en onvermijdelijk is dat partijen relevante gegevens, waaronder ook persoonsgegevens, verwerken;
- partijen zich ervan bewust zijn dat zij bij het uitwisselen van persoonsgegevens gehouden zijn aan de op hen van toepassing zijnde wet- en regelgeving en dat bij de uitwisseling van persoonsgegevens de persoonlijke levenssfeer van het subject dient te worden gewaarborgd;

- de Wet bescherming persoonsgegevens (Wbp) op dit convenant van toepassing is. De Wbp wordt als het van toepassing zijnde voorschrift vervangen door de Algemene Verordening Gegevensbescherming (EU 2016/679) bij inwerkingtreding van deze verordening.

Spreken het volgende af:

Artikel 1 definities

In aanvulling op de definities gegeven in de Wbp wordt in dit convenant verstaan onder:

- achterblijver:** persoon met wie een uitreiziger in gezinsverband leefde;
- casusoverleg:** het casusoverleg ter voorkoming van radicalisering en extremisme bestaande uit de vertegenwoordiger(s) van de betrokken partijen, en vertegenwoordigers van externe casuspartners betrokken bij het opstellen, uitvoeren of monitoren van het integraal plan van aanpak;
- externe casuspartner:** een derde die noodzakelijk is bij het opstellen, uitvoeren of monitoren van het integraal plan van aanpak en die is opgenomen in bijlage 1 bij dit convenant;
- extremisme:** de benaming van het fenomeen waarbij personen of groepen, op buitenparlementaire wijze over de grenzen van de wet gaan en met (gewelddadige) acties politieke besluitvorming proberen te beïnvloeden;
- integraal plan van aanpak:** het document waarin het doel van de persoonsgerichte, integrale benadering van het subject en de hiertoe door partijen en eventueel betrokken externe casuspartners te treffen maatregelen zijn vastgelegd;
- radicalisering:** Een proces van toenemende bereidheid om de uiterste consequentie uit een denkwijze te aanvaarden en die in daden om te zetten. Deze toenemende bereidheid kan leiden tot gedrag dat andere mensen diep kwetst of in hun vrijheid raakt, kan aanleiding zijn voor individuen of groepen om zich af te keren van de samenleving en kan leiden tot het gebruik van geweld;
- referentiekader:** Het objectieve kader waarin criteria worden gegeven om te bepalen of een persoonsgerichte, integrale benadering van het subject noodzakelijk is;
- signaal:** een feitelijke gedraging die ingevolge het referentiekader mogelijkwerijds duidt op radicalisering, extremisme, uitreizen, of terugkeer van een natuurlijk persoon;
- subject:** de betrokkene die voorwerp van bespreking is in de weegploeg of het casusoverleg;
- terugkeerder:** een uitreiziger die na verblijf bij een jihadistische groepering of in een jihadistisch strijdgebied terugkeert naar het land dat hij of zij voor de uitreis verlaten heeft of een ander land dat niet is aan te merken als jihadistisch strijdgebied;
- uitreiziger:** een persoon die zijn eigen land verlaat om zich aan te sluiten bij een jihadistische groepering in een jihadistisch strijdgebied;

- l. **uitvoerder:** de functionaris die onder verantwoordelijkheid en in naam van de verantwoordelijke als bedoeld in de Wbp, zorg draagt voor een zorgvuldig beheer van de gegevens;
- m. **Weegploeg:** overleg, bestaande uit de vertegenwoordiger(s) van de kernpartijen, belast met het verzamelen van de verschillende eigen signalen en signalen van derden en de selectie van de aangebrachte casuïstiek op basis van het referentiekader, teneinde te bepalen of voor het subject een persoonsgerichte, integrale benadering noodzakelijk is, en welke partijen en externe casuspartners hierbij betrokken dienen te worden.

Artikel 2 de taken en bevoegdheden van de partijen

De wettelijke taken en bevoegdheden van de partijen zijn:

- a. voor de gemeente: de handhaving van de openbare orde op grond van artikel 172 Gemeentewet en zijn wettelijke taken op het terrein van het toegankelijk maken en aanbieden van voorzieningen op het terrein van jeugdzorg, werk en inkomen, scholing, uitkeringen en schuldsaneringen;
- b. voor de politie: de daadwerkelijke handhaving van de rechtsorde en de verlening van hulp aan hen die deze behoeven op grond van artikel 3 van de Politiewet;
- c. voor het Openbaar Ministerie: de strafrechtelijke handhaving van de rechtsorde op grond van artikel 124 Wet op de rechterlijke organisatie;
- d. voor de Raad van de Kinderbescherming: de taken en bevoegdheden volgend uit artikel 238, tweede lid, van het Burgerlijk Wetboek Boek 1, in het bijzonder het beschermen van minderjarigen tegen ernstige bedreigingen in hun ontwikkeling en gezondheid, het optreden ten behoeve van minderjarigen en het op verzoek of uit eigen beweging autoriteiten en instellingen van advies voorzien;
- e. voor Reclasseringsinstellingen: het op basis van de Reclasseringsregeling 1995 bijdragen aan de veiligheid van de samenleving door het beheersen van risico's, en veroordeelden of verdachten te stimuleren zijn of haar gedrag te veranderen. Op die manier werken zij aan het voorkomen van criminaliteit en het terugdringen van recidive. De reclasseringsinstellingen voeren taakstraffen uit en houden toezicht op maatregelen en andere beslissingen van justitiële instanties. Haar taken bij geradicaliseerde personen worden verricht door een specialistisch landelijk georganiseerd team. Dit team is toegerust om de specifieke signalen van radicalisering te herkennen en daarop te acteren.

Artikel 3 Doel van het samenwerkingsverband

Doel van dit samenwerkingsverband is:

- het reduceren van de risico's voor de samenleving die uitgaan van radicalisering, extremisme, uitreizen, of terugkeer en het bieden van zorg aan subjecten en / of
- het reduceren van risico's voor de ontwikkeling van minderjarigen door radicalisering, extremisme, uitreizen of terugkeer.

Daarvoor is het noodzakelijk dat de partijen, ieder vanuit de eigen expertise, komen tot een gemeenschappelijke aanpak, die in onderling overleg en samenhang wordt vastgesteld.

Om dit doel te kunnen bereiken wisselen de partijen signalen en / of andere noodzakelijke (persoons-)gegevens uit, waardoor partijen in gezamenlijkheid een effectief en doelmatig integraal plan van aanpak kunnen vaststellen ten aanzien van in Nederland verblijvende geradicaliseerde personen of personen die dreigen te radicaliseren, gericht op:

- a. het bevorderen van deradicalisering;
- b. het stimuleren van gedragsverandering;
- c. het beperken van veiligheidsrisico's;
- d. het voorkomen van uitreizen naar een strijdgebied;
- e. het bieden van zorg aan subjecten;
- f. het bieden van hulp aan achterblijvers, indien gewenst.

De werkwijze van dit casusoverleg is beschreven in artikel 8 van het Convenant en verder uitgewerkt in de als bijlage 2 gevoegde procesbeschrijving.

Artikel 4 Verantwoordelijkheid

De kernpartijen zijn gezamenlijk de verantwoordelijke in de zin van de Wbp voor de gegevensverwerking in het kader van dit samenwerkingsverband. De verwerking van persoonsgegevens in het kader van de uitvoering van dit Convenant is door de kernpartijen bij de Autoriteit Persoonsgegevens gemeld.

Artikel 5 Uitvoerder

Voor de (dagelijkse) uitvoering van werkzaamheden hebben de kernpartijen een uitvoerder aangesteld. De uitvoerder heeft onder meer tot taak alle voorbereidende werkzaamheden ten behoeve van de weegploeg en het casusoverleg te verrichten, het informatiesysteem bij te houden en overige op verzoek van de kernpartijen te verrichten werkzaamheden.

Artikel 6 Grondslag verstrekking persoonsgegevens

De grondslag met betrekking tot de gegevensverwerking is:

- a. *Voor het OM:* op grond van het bepaalde in artikel 39f, eerste lid, Wet justitiële en strafvorderlijke gegevens kan het College van procureurs-generaal, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, aan personen en instanties voor bepaalde doeleinden strafvorderlijke gegevens verstrekken;
- b. *Voor de politie:* op grond van artikel 20 Wet politiegegevens mag de politie met het oog op een zwaarwegend algemeen belang, ten behoeve van een samenwerkingsverband van de politie met personen of instanties, politiegegevens voor bepaalde doeleinden aan die personen en instanties verstrekken en op grond van artikel 18, tweede lid, Wet politiegegevens mag de politie structureel, specifiek omschreven politiegegevens

verstrekken voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang.

- c. *Voor de gemeente*: op grond van artikel 8, aanhef en onder e van de Wbp mag de gemeente persoonsgegevens verwerken indien de verwerking noodzakelijk is voor de goede vervulling van zijn publiekrechtelijke taak dan wel van het bestuursorgaan waaraan hij de gegevens verstrekt.
- d. *Voor de Raad voor de Kinderbescherming*: op grond van artikel 8, aanhef en onder e van de Wbp mogen persoonsgegevens door de Raad van de Kinderbescherming worden verstrekt indien de gegevensverwerking noodzakelijk is voor de goede vervulling van zijn publiekrechtelijke taak dan wel van het bestuursorgaan waaraan de gegevens worden verstrekt;
- e. *Voor de Reclassering Nederland*: op grond van artikel 8 Reclasseringsregeling 1995 juncto artikel 8, aanhef en onder c van de Wbp mogen persoonsgegevens door de Reclassering worden verstrekt indien de verstrekking noodzakelijk is voor de uitvoering van reclasseringswerkzaamheden:
 - I. het houden van toezicht op en het begeleiden van personen die worden verdacht van of die zijn veroordeeld wegens een strafbaar feit;
 - II. het geven van voorlichting en advies aan justitiële instanties;
 - III. het voorbereiden en begeleiden van de uitvoering van de taakstraffen.

Artikel 7 Werkwijze Weegploeg

1. Signalen worden door de weegploeg verkregen door tussenkomst van een van de kernpartijen.
2. Signalen worden aan de weegploeg verstrekt:
 - a. *Door de politie*: via een vertegenwoordiger van de politie die deelneemt aan de weegploeg;
 - b. *Door het OM*: via een vertegenwoordiger van het OM die deelneemt aan de weegploeg;
 - c. *Door de gemeente*: via een vertegenwoordiger van de gemeente die deelneemt aan de weegploeg.
3. De weegploeg analyseert signalen, met toepassing van het als bijlage 3 gevoegde referentiekader, en beoordeelt of voor een subject een persoonsgerichte, integrale benadering noodzakelijk is, en welke partijen en externe casuspartners hierbij betrokken dienen te worden.
4. Na de analyse van de weegploeg zijn er twee mogelijkheden:
 - 1) de analyse van de signalen leidt, eventueel na het inwinnen van additionele informatie, tot een beslissing van de weegploeg om het subject te agenderen in een casusoverleg of
 - 2) uit analyse van de signalen blijkt dat deze onvoldoende substantieel zijn om het subject te agenderen in het casusoverleg.

Artikel 8 Gegevensverwerking weegploeg

1. Ten behoeve van de weegploeg legt de uitvoerder gegevens vast in een digitaal bestand, separaat van het digitaal bestand ten behoeve van het casusoverleg als bedoeld in artikel 10.
2. In het digitaal bestand worden vastgelegd:
 - a. de NAW-gegevens van het subject;
 - b. een omschrijving van de signalen;
 - c. de naam en de contactgegevens van de melder die de signalen heeft ingebracht;
 - d. de analyse van de signalen op basis van het referentiekader;
 - e. de beslissing om het subject al dan niet te agenderen in het casusoverleg;
 - f. de beslissing dat het integraal plan van aanpak is afgesloten.
3. De gegevens in het digitaal bestand worden periodiek gecontroleerd op juistheid en volledigheid en worden zo nodig aangepast.
4. Onverlet het vijfde lid, zijn gegevens uit het digitaal bestand uitsluitend toegankelijk voor kernpartijen en slechts voor zover dit noodzakelijk is voor het doel van de weegploeg.
5. Indien agendering van het subject in een casusoverleg plaatsvindt wordt een kopie van de relevante gegevens uit het bestand van de weegploeg overgedragen aan het bestand van het casusoverleg.

Artikel 9 Werkwijze van het casusoverleg

1. Aan het casusoverleg nemen die partijen en externe casuspartners deel die betrokken dienen te zijn bij het integraal plan van aanpak.
2. De deelnemers verstrekken elkaar in het casusoverleg, met inachtneming van de toepasselijke wettelijke kaders, de bij hen berustende signalen of andere relevante gegevens inzake het subject dat door de weegploeg in het casusoverleg is geagendeerd, waaronder ook begrepen persoonsgegevens voor zover die relevant en noodzakelijk zijn voor het opstellen, uitvoeren of monitoren van het integraal plan van aanpak.
3. het casusoverleg stelt een integraal plan van aanpak op inzake het subject.
4. Het casusoverleg monitort de voortgang van het integraal plan van aanpak en adviseert de kernpartijen tot afsluiting daarvan indien de voortgang van het integraal plan van aanpak hiertoe aanleiding geeft.
5. Indien noodzakelijk, kan advies worden gevraagd aan de Nationaal Coördinator Terrorismedebestrijding en Veiligheid (NCTV) of aan andere deskundigen met expertise op het gebied van voorkomen en tegengaan van radicalisering en extremisme.

Artikel 10 Gegevensverwerking casusoverleg

1. Ten behoeve van het casusoverleg legt de uitvoerder gegevens vast in een digitaal bestand, separaat van het digitaal bestand ten behoeve van de weegploeg als bedoeld in artikel 8.
2. In het digitaal bestand worden vastgelegd:
 - a. de NAW-gegevens van het subject;
 - b. een omschrijving van de signalen;
 - c. de naam en de contactgegevens van de partij die de signalen heeft ingebracht;

- d. de analyse van de signalen op basis van het referentiekader;
 - e. de acties die partijen ondernemen naar aanleiding van de analyse van de signalen;
 - f. de NAW-gegevens en andere relevante gegevens van achterblijvers voor zover dit noodzakelijk is voor de uitvoering van het integraal plan van aanpak;
 - g. de NAW-gegevens en andere relevante gegevens van personen uit het sociale netwerk van het subject, voor zover deze betrokken zijn of anderszins een rol spelen bij de uitvoering van het integraal plan van aanpak;
 - h. de beslissing dat het integraal plan van aanpak is afgesloten.
3. De gegevens in het digitaal bestand worden periodiek door de uitvoerder gecontroleerd op juistheid en volledigheid en worden zo nodig aangepast.
 4. Partijen hebben toegang tot de gegevens uit het digitale bestand, voor zover dit noodzakelijk is voor het doel van het casusoverleg.
 5. Externe casuspartners hebben toegang tot het integraal plan van aanpak. Andere informatie uit het digitaal bestand, voor zover deze informatie persoonsgegevens betreft, wordt uitsluitend aan externe casuspartners verstrekt voor zover dat noodzakelijk is ten behoeve van de bijdrage en expertise die door de desbetreffende partij moet worden geleverd voor het opstellen en uitvoeren dan wel monitoren van het plan van aanpak en voor de doorverstrekking daarvan toestemming is gegeven door de convenantspartijen. Deze doorverstrekking wordt vastgelegd in het bestand van het casusoverleg. Daarbij wordt vermeld de noodzaak van de verstrekking alsmede de soort gegevens die zijn verstrekt.

Artikel 11 Informatieplicht

1. In het belang van de transparantie over de geïntegreerde en persoonsgerichte aanpak voorkoming radicalisering en extremisme wordt het convenant en de bijlagen gepubliceerd in de Staatscourant.
2. Onverlet het gestelde in het derde lid worden de verplichtingen ten aanzien van de betrokkene die voortvloeien uit de informatieplicht zoals omschreven in artikel 34 van de Wbp nagekomen op het moment dat de weegploeg is gekomen tot één van de twee mogelijkheden genoemd in artikel 7, vierde lid.
3. Voordat de verantwoordelijke de verplichtingen ten aanzien van de betrokkene die voortvloeien uit artikel 34 van de Wbp nakomt, voeren de kernpartijen onderling overleg. Mede op basis van dit overleg beoordeelt de verantwoordelijke of aan de informatieplicht kan worden voldaan of dat dit nog niet mogelijk is gelet op een van de belangen zoals omschreven in artikel 43 van de Wbp, te weten:
 - a. de veiligheid van de Staat;
 - b. de voorkoming, opsporing en vervolging van strafbare feiten;
 - c. gewichtige economische en financiële belangen van de Staat en van andere openbare lichamen;
 - d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen genoemd onder b en c;
 - e. de bescherming van de betrokkene of van rechten en vrijheden van anderen.

4. Indien de verantwoordelijke oordeelt dat niet, of nog niet aan de informatieplicht zoals omschreven in het eerste lid, kan worden voldaan, wordt daarvan een aantekening gemaakt in het bestand.
5. Zodra er geen beletselen meer zijn, als bedoeld in het derde lid, zal de betrokkene worden geïnformeerd, ook in de gevallen waar is besloten af te zien van verdere maatregelen en/of interventies.

Artikel 12 rechten van betrokkenen

1. De betrokkene of zijn wettelijke vertegenwoordiger indien het een jongere betreft die de leeftijd van zestien nog niet heeft bereikt of indien de betrokkene onder curatele is gesteld dan wel voor de jongere een mentorschap is ingesteld, richt zijn of haar verzoek om inzage en / of correctie aan de uitvoerder. De verantwoordelijke kan ook andere functionarissen aanwijzen die onder coördinatie van de uitvoerder met de dagelijkse uitvoering van inzage-, correctie- en verzetsverzoeken zijn belast.
2. De betrokkene of zijn wettelijk vertegenwoordiger, kan aan de verantwoordelijke om inzage in zijn persoonsgegevens verzoeken.
3. Nadat de identiteit van de betrokkene is vastgesteld wordt het verzoek zo spoedig mogelijk, maar uiterlijk binnen 4 weken na ontvangst, beantwoord. De betrokkene ontvangt een overzicht (in een begrijpelijke vorm) van de gegevens die worden verwerkt, de doelen of de doeleinden waarvoor deze gegevens worden verwerkt, de (mogelijke) ontvangers van deze gegevens en de informatie over de herkomst van die gegevens.
4. Het verzoek om inzage kan worden geweigerd indien een van de uitzonderingsgronden als bedoeld in artikel 43 van de Wbp zich voordoet. De betrokkene ontvangt in dat geval een gemotiveerde afwijzing.
5. De betrokkene of zijn wettelijke vertegenwoordiger geeft in het verzoek aan welke correcties hij of zij uitgevoerd wil zien en om welke reden. De verantwoordelijke voldoet zo spoedig mogelijk, maar uiterlijk binnen 4 weken na ontvangst van het verzoek, aan het verzoek indien en voor zover de persoonsgegevens:
 - a. feitelijk onjuist zijn;
 - b. Voor het doel van de verwerking onvolledig of niet ter zake dienend zijn;
 - c. Anderszins in strijd met een wettelijk voorschrift worden verwerkt.
6. De verantwoordelijke draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering en/of afscherming in ieder geval uiterlijk binnen vier weken na deze beslissing wordt uitgevoerd. Zij doet hiervan een kennisgeving aan partijen.

Artikel 13 Bewaartermijn

1. Onverlet het gestelde in het derde en vierde lid worden de persoonsgegevens na de laatste verwerking gedurende een termijn van 5 jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens vernietigd.

2. Uiterlijk 1 jaar na de laatste verwerking worden de persoonsgegevens gearhiveerd in een niet-actieve digitale omgeving en zijn de gegevens slechts nog raadpleegbaar door de kernpartijen.
3. Persoonsgegevens in het bestand van de weegploeg die betrekking hebben op personen waarvan is beslist om deze niet te agenderen in het casusoverleg worden niet langer bewaard dan noodzakelijk is voor de doeleinden van het bestand, met een maximumtermijn van 6 maanden, en vervolgens vernietigd.
4. Voor zover dit noodzakelijk is voor een doel als bedoeld in dit convenant kunnen persoonsgegevens die overeenkomstig het tweede lid worden bewaard, in opdracht van de verantwoordelijke, ter beschikking worden gesteld aan de weegploeg voor hernieuwde verwerking.

Artikel 14 Geheimhouding

1. De partijen zijn verplicht tot geheimhouding van persoonsgegevens waarvan zij kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.
2. Aan derden die inzage hebben of, in overeenstemming met het bepaalde in dit convenant, op andere wijze persoonsgegevens verkrijgen, leggen de partijen een plicht tot geheimhouding op. Deze plicht strekt tot geheimhouding van de persoonsgegevens waarvan derden kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Artikel 15 Beveiligingsmaatregelen

1. De verantwoordelijke beveiligt de persoonsgegevens van de betrokkenen tegen verlies of enige vorm van onrechtmatige verwerking. Men treft daartoe de nodige passende technische en organisatorische maatregelen.
2. De verantwoordelijke draagt zorg voor de beveiliging van de persoonsgegevens tegen verlies, diefstal of enige andere vorm van onrechtmatig gebruik. Daartoe wordt door de verantwoordelijke een beveiligingsplan vastgesteld dat vervolgens ook wordt geïmplementeerd. In dit beveiligingsplan is in ieder geval aandacht voor:
 - a. Fysieke maatregelen voor toegangsbeveiliging, inclusief de organisatorische controle;
 - b. De lees- en schrijfbevoegdheden van de partijen;
 - c. Wijze van toekennen, wijzigen en intrekken van autorisaties;
 - d. Logische toegangscontroles;
 - e. Automatische *logging* van toegang tot gegevens, inclusief een periodieke controleprocedure;
 - f. Controle op toegekende bevoegdheden;
 - g. Een incidentenregistratie: beveiligingsincidenten, inclusief datalekken, worden gemeld, geregistreerd en afgehandeld (ingevolge artikel 34a Wbp meldplicht datalekken).

3. De verantwoordelijke draagt zorg voor de implementatie van deze beveiligingsmaatregelen door de uitvoerder en controleert ook periodiek de naleving daarvan. Het beveiligingsbeleid wordt jaarlijks geëvalueerd en desgewenst herzien.
4. De partijen zijn verplicht te handelen in overeenstemming met de beveiligings- en toegangsrichtlijnen zoals opgesteld door de verantwoordelijke.

Artikel 16 Afdwingbaarheid

Dit convenant is niet in rechte afdwingbaar.

Artikel 17 Geschillen

Alle geschillen tussen partijen in verband met dit convenant worden in goed onderling overleg tussen de partijen beslecht.

Artikel 18 Inwerkingtreding, opzegging ,wijziging en evaluatie

1. Dit convenant treedt in werking per 1 maart 2018 en wordt voor onbepaalde tijd aangegaan.
2. Elke partij kan zijn deelname aan dit convenant opzeggen met inachtneming van een opzegtermijn van 3 maanden. Artikel 14 blijft ook na opzegging voor partijen van kracht.
3. Wanneer een partij het convenant opzegt, blijft het convenant voor de overige partijen in stand voor zover de inhoud en strekking ervan zich daartegen niet verzetten.
4. Dit convenant wordt 2 jaar na inwerkingtreding geëvalueerd.

Naam organisatie: Gemeente Den Haag	Datum:
Naam wettelijk functionaris: Pauline Krikke	Handtekening: 5.1.2.e
Functie: Burgemeester	5.1.2.e

Naam organisatie: Het Openbaar Ministerie, het College van procureurs-generaal,	Datum: 22-1-18
Namens deze:	Handtekening: 5.1.2.e
Naam wettelijk functionaris: Dhr. A.J.A.M. Nieuwenhuizen	
Functie: Hoofdofficier van Justitie	

Naam organisatie: De politie, de korpschef van politie,	Datum: 18/1/18
Namens deze:	Handtekening: 5.1.2.e
Naam wettelijk functionaris: Dhr. P. van Musscher	
Functie: Politiechef van Den Haag	

Naam organisatie: Raad voor de Kinderbescherming	Datum: 22-01-2018
Naam wettelijk functionaris: Dhr. A. de Raad	Handtekening: 5.1.2.e
Functie: Gebiedsmanager Haaglanden	5.1.2.e

Naam organisatie: Reclassering Nederland	Datum: 5.1.2.e
Naam wettelijk functionaris: Dhr.A. Cardol	Handtekening: 5.1.2.e
Functie: (wnd) Regiodirecteur Zuid-West	5.1.2.e



**Zorg- en
Veiligheidshuis**
Haaglanden

GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Versie : 1.0
Datum : 10-11-2021

Documentinformatie

Versiegeschiedenis

Versie	Versie datum	Samenvatting van de aanpassing	Opmerkingen
0.1	26-5-2021	Eerst invulling van het document door 5.1.2.e	
0.2	02-06-2021	Aanvullingen door 5.1.2.e	
0.3	11-06-2021	Aanvullingen door 5.1.2.e	
0.4	15-06-2021	Aanvullingen door 5.1.2.e	
1.0	10-11-2021	Aanvullingen maatregelen n.a.v. afronding BIO baseline toets en Risico analyse door 5.1.2.e	Versie naar MT van 22-11-2021

Inhoudsopgave

Managementsamenvatting	4
Inleiding	4
Doelstelling	4
Aanpak	4
Bevindingen	5
Vervolgproces	5
 Inleiding	6
Wat is een GEB?	6
Verwerkingenregister	6
Wanneer is een GEB verplicht?	6
Uitkomsten GEB	6
Toezenden aan de Gegevensautoriteit (GA) en de Functionaris Gegevensbescherming (FG)	7
 A. Beschrijving kenmerken gegevensverwerking	8
1. Voorstel van de verwerking	8
2. Persoonsgegevens	8
3. Verwerkingsdoeleinden	9
4. Gegevensverwerking	9
5. Betrokken partijen en/of organisaties	13
6. Verwerkingslocatie(s)	14
7. Juridisch en beleidsmatig kader	14
8. (Semi-)Geautomatiseerde besluitvorming, profilering of big data-verwerkingen	14
 B. Beoordeling rechtmatigheid gegevensverwerkingen	15
9. Grondslag verwerking	15
10. Bijzondere persoonsgegevens	16
11. Doelbinding verdere verwerking	17
12. Noodzaak en evenredigheid	17
13. Rechten van de betrokkene	18
 C. Beschrijving en beoordeling risico's voor de betrokkenen	19
14. Risico's	19
 D. Beschrijving voorgenomen maatregelen	19
15. Maatregelen	19
 Bijlage 1 Begrippenkader	20

Basisinformatie met betrekking tot deze verwerking van persoonsgegevens

Datum:	26-05-2021
Naam van de verwerking	Persoonsgerichte aanpak Zorg- en Veiligheidshuis Haaglanden
Ingangsdatum van de verwerking	01-07-2021
Organisatie/Afdeling waar de verwerking plaatsvindt:	Zorg- en Veiligheidshuis Haaglanden
Contactpersoon m.b.t. deze verwerking:	5.1.2.e
Privacyfunctionaris	5.1.2.e
Betrokken bij deze GEB:	5.1.2.e (5.1.2.e)

Functionaris gegevensbescherming

Datum:	
Reactie:	

Gezien door verwerkingsverantwoordelijke

Naam:	
Functie:	
Datum:	
Opmerkingen:	

Managementsamenvatting

Inleiding

Voor u ligt een *gegevensbeschermingseffectbeoordeling* (hierna: GEB), oftewel een DPIA¹ (*data protection impact assessment*) voor de processen rond de persoonsgerichte aanpak bij het Zorg- en Veiligheidshuis Haaglanden. Deze beoordeling is uitgevoerd op grond van de Algemene Verordening Gegevensbescherming (hierna: AVG). Een GEB wordt uitgevoerd in het geval dat een gegevensverwerking waarschijnlijk een wettelijk hoog privacy-risico oplevert voor de personen van wie een organisatie gegevens verwerkt.

Doelstelling

Het doel van deze GEB is om op een heldere en structurele manier inzicht te verkrijgen in de risico's die gepaard gaan met de verwerking van persoonsgegevens.

Volgens art. 4 lid 2 AVG wordt onder het verwerken van persoonsgegevens verstaan: 'elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, 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.'

Vervolgens worden er in deze GEB aanbevelingen gedaan om de geconstateerde risico's te kunnen reduceren tot een acceptabel niveau.

Aanpak

Deze GEB AVG is gebaseerd op het Rijksmodel.² Deze GEB is ingevuld door 5.1.2.e in samenspraak met betrokken medewerkers van het Zorg- en Veiligheidshuis Haaglanden. In onderdelen A en B zijn kenmerken van de gegevensverwerking en de rechtmatigheid onderzocht. Hieruit zijn vervolgens privacy risico's geformuleerd. Voor de privacy risicoanalyse is een apart formulier opgesteld. Deze geeft invulling aan de onderdelen C en D van het GEB formulier.

¹ Bij de gemeente Den Haag spreekt men van DPIA, maar we hanteren in dit document GEB omdat het document gebaseerd is op een template van de Politie.

² Model gegevensbeschermingseffectbeoordeling Rijksdienst (DPIA), 29 september 2017

Bevindingen

Er is opdracht gegeven aan de *information security officer* voor de volgende activiteiten:

- Uitvoeren van een BIO (baseline informatiebeveiliging overheid) baselinetoets om de impact op het proces te bepalen.
- Uitvoeren van een uitgebreide risicoanalyse.
- Beoordeling risicoanalyse leverancier met als doel om te toetsen of de leverancier voldoet aan de gestelde eisen.
- Beoordeling van uit te voeren/uitgevoerde pentest.
- Gevraagd en ongevraagd advies te geven tijdens het traject op het gebied van informatiebeveiliging, inclusief het bijwonen van (relevante) overleggen.

Uit de BIO baseline toets blijkt dat PGAX dient te voldoen aan de Basis Beveiligingsniveau (afgekort BBN) 2.

De leverancier is ISO27001 gecertificeerd. Doormiddel van de leverancierstoets is beoordeeld dat leverancier voldoet aan de eisen van ISO27001 en zich hier onafhankelijk voor laat toetsen. Daarnaast voldoet de leverancier aan alle eisen die worden gesteld in de leverancierstoets. Uit de leverancierstoets zijn daarom geen negatieve bevindingen gedaan, waarbij verbeteracties benodigd zijn.

In de ondertekende contracten is informatieveiligheid voldoende geborgd, conform de eisen horend bij de BBN2 score.

Er is een aanvullende risicoanalyse uitgevoerd, waarin twee *kleine* risico's gevonden. Namelijk:

Risico 1: Mede door de vele accounts van ketenpartners is er een kans dat er accounts actief zijn van mensen die niet meer zijn betrokken bij het proces en/of uit dienst zijn. Hierdoor is de kans aanwezig een persoon toegang heeft tot gegevens binnen PGAX die hier niet meer voor bevoegd is, waarmee het risico bestaat dat gegevens gelekt worden.

Risico 2: In het verleden zijn persoonsgegevens gelekt door het versturen van brieven naar verkeerde adressen. Dit risico bestaat nog steeds. Hierbij worden er NAW-gegevens van betrokkenen onbewust gelekt naar niet bevoegde.

Er zijn drie scenario's voorgesteld met mitigerende maatregelen voor deze risico's. In overleg met en akkoord van de information security officer is gekozen voor *scenario 2*:

Gedeeltelijk opvolgen BIO eisen, maatregelen op basis van dataclassificatie en mitigerende risico maatregelen.

Vervolgproces

De proceseigenaar heeft opdracht gegeven om te voldoen aan BIO eisen en accepteert risico's op de genoemde onderwerpen.

Concreet zijn de volgende mitigerende acties uit te voeren:

- We gaan de betrokken netwerkpartners dringend vragen z.s.m. melding te doen van uitdienststreding van medewerkers en actie te ondernemen om toegang tot PGAx voor deze mensen te ontfeggen.
Voor medewerkers bij het ZVHH en de gemeente Den Haag geldt het *single sign on principe* en is toegang tot PGAx gekoppeld aan het gemeentelijk account.
- We gaan het procesdeel waarin 'brieven per post' worden gestuurd melden dat men extra voorzichtig moet zijn bij de adressering ten einde onjuiste adressering te voorkomen.

Inleiding

Wat is een GEB?

Een GEB is een instrument om de verwerking van persoonsgegevens inzichtelijk te maken en te motiveren.

Vervolgens dient het om (vooraf) de privacyrisico's van een gegevensverwerking in kaart te brengen en de beslissers te ondersteunen bij het nemen van maatregelen om de risico's te beperken. Een GEB staat gelijk aan 'Data protection impact assessment' (DPIA).

Dit GEB -document is gebaseerd op het Rijksmodel. Artikel 35 AVG schrijft de verplichte onderdelen van een GEB voor: de beschrijving en onderbouwing van de verwerking en de risico analyse met passende maatregelen.

Verwerkingenregister

Iedere verwerking wordt ingevolge artikel 24 van het privacyprotocol verwerkt in het verwerkingenregister van de partner. Zodra de partner een verwerking start neemt de manager van het Zorg- en Veiligheidshuis de verwerkingen van persoonsgegevens op in een gezamenlijk register van verwerkingsactiviteiten onder het privacyprotocol.

De functionarissen gegevensbescherming van de partners hebben recht op toegang tot de informatie en daarmee ook tot het gebouw waarin het zorg- en veiligheidshuis is gevestigd.

Wanneer is een GEB verplicht?

In de AVG is op hoofdlijnen beschreven wanneer een GEB verplicht is. Dat is het geval als een gegevensverwerking waarschijnlijk een hoog privacy-risico oplevert voor de personen van wie een organisatie gegevens verwerkt. Dit bepaalt de verwerkingsverantwoordelijke zelf. In ieder geval is een GEB verplicht als deze voorkomt op de lijst van de Autoriteit Persoonsgegevens. Tot slot heeft de Europese toezichthouder (European Data Protection Supervisor) een lijst met criteria opgesteld waarvan twee of meer criteria een GEB vereisen. Als er geen GEB is opgesteld, mag de verwerking niet plaatsvinden.³

Uitkomsten GEB

De meerwaarde van een GEB bestaat uit:

1. inzicht in de verwerking van persoonsgegevens;
2. motiveren van het verwerken van persoonsgegevens: de rechtmatigheidstoets;
3. inzicht in de mate waarin de rechten betrokkenen worden uitgevoerd: positie betrokkene versterken;
4. motiveren waarom de verwerking proportioneel is en voldoende doelgebonden is;
5. het brengt de risico's in kaart en de passende maatregelen.

Wanneer de verwerkingsverantwoordelijke geen maatregelen treft om de risico's te beperken, is deze verplicht de toezichthouder, de Autoriteit Persoonsgegevens, hierover te raadplegen (artikel 36 AVG). De toezichthouder zal een termijn stellen om de maatregelen alsnog te treffen. De toezichthouder kan al zijn bevoegdheden in dit geval toepassen zoals een tijdelijke verwerkingsbeperking of verbod opleggen (artikel 58 AVG).

³ Meer uitleg over de richtlijnen en criteria van de Autoriteit Persoonsgegevens en de Europese Toezichthouder (EDPS) zijn te vinden op: <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-guidelines>

A. Beschrijving kenmerken gegevensverwerking

Onder A wordt de eerste stap beschreven van de GEB: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling. Beschrijf hier op gestructureerde wijze de voorgenomen gegevensverwerking en de verwerkingsdoeleinden.

1. Voorstel van de verwerking

Beschrijf waar de GEB op ziet, waarom er is gekozen om een GEB uit te voeren en de context waarbinnen deze plaatsvindt op hoofdlijnen.

Antwoord:

Het zorg- en veiligheidshuis is een samenwerkingsverband waarin zorg- en strafpartners en gemeenten, onder eenduidige regie, werken aan complexe zorg- en veiligheidsproblemen. De doelstelling van de samenwerking is bijdragen aan de algemene veiligheid, het verbeteren van de persoonlijke situatie, het voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit en/of maatschappelijke uitval. Dit gebeurt door een combinatie van repressie, bestuurlijke interventies en zorg, hetgeen moet worden gezien als een zwaarwegend algemeen belang. Om de persoonsgegevens die voor dit doel worden verwerkt in goede banen te leiden is het systeem PGAX geselecteerd

2. Persoonsgegevens

2a: Geef per categorie van betrokkene aan welke persoonsgegevens van de betrokkene verwerkt worden. Vul de tabel in.

Persoonsgegevens ¹⁾	Type Persoonsgegevens ²⁾	Categorie van betrokkenen ³⁾
Voornaam	normaal	<i>Client, medewerker, ketenpartner</i>
Achternaam	normaal	<i>Client, medewerker, ketenpartner</i>
Geboorte datum	normaal	<i>Client</i>
BSN-nummer	Wettelijk ID nummer	<i>Client</i>
Geboorte plaats	normaal	<i>Client</i>
Geslacht	normaal	<i>Client</i>
Emailadres	normaal	<i>Client, medewerker, ketenpartner</i>
Functie	normaal	<i>Medewerker, ketenpartner</i>
Telefoonnummer	normaal	<i>Client, medewerker, ketenpartner</i>
Organisatie	normaal	<i>Medewerker, ketenpartner</i>
Financiële gegevens (inkomen)	gevoelig	<i>Client</i>
Houding, gedrag en vaardigheden	bijzonder	<i>Client</i>
Werk, opleiding en tijdsbesteding	normaal	<i>Client</i>
Huisvesting	normaal	<i>Client</i>

(Huiselijke) relaties ook eventueel omtrent seksualiteit	bijzonder	<i>Client</i>
Geestelijke geschondenheid (geen diagnostiek)	bijzonder	<i>Client</i>
Lichamelijke gezondheid (geen diagnostiek)	bijzonder	<i>Client</i>
Middelengebruik en verslavingen	bijzonder	<i>Client</i>
Justitie en politie gegevens	bijzonder	<i>Client</i>
Ideologie en religie	bijzonder	<i>Client</i>
Interventies op alle levensgebieden zoals behandelingen, vormen van huisvesting of strafrechtelijke onderzoeken	bijzonder	<i>Client</i>

Toelichting

1) Bijvoorbeeld: Naam, geboortedatum, rekeningnummer en BSN.	2) Type persoonsgegevens kunnen zijn: • Normaal • Gevoelig • Bijzonder • Strafrechtelijk • Wet. ID-nr	3) Betrokkenen: meerdere categorieën op 1 persoonsgegeven mogelijk. Bijvoorbeeld: medewerkers, leveranciers, bezoekers en sollicitanten.
---	--	---

2b: Welke bewaartermijn(-en) is/zijn er? En hoe wordt hier uitvoering aan gegeven?

Antwoord:

Persoonsgegevens worden vernietigd zodra de Verwerking daarvan niet langer nodig is voor het doel waarvoor zij zijn verwerkt, maar uiterlijk binnen 1 jaar na het besluit tot Afschaling.

- a. persoonsgegevens kunnen tot zes maanden na besluit tot Afschaling worden bewaard in een vorm waarmee enkel de Procesregisseur en informatiecentrum toegang hebben tot de gegevens;
- b. na zes maanden na besluit tot Afschaling worden persoonsgegevens gearhiveerd en heeft enkel de Manager toegang tot die Persoonsgegevens;
- c. na één jaar na besluit tot Afschaling worden de Persoonsgegevens vernietigd.

3. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerking zo specifiek mogelijk.

Het verdient de voorkeur de verwerkingsdoeleinden zoveel mogelijk te baseren op het niveau van werk- en organisatieprocessen.

Antwoord:

Partijen verwerken ieder afzonderlijk en gezamenlijk in het systeem van het Zorg- en Veiligheidshuis persoonsgegevens van betrokkenen. De verwerking is gereguleerd in artikel 24 van het privacyprotocol. Partijen verwerken in het kader van het zorg- en veiligheidshuis voor ieder van onderstaande fasen enkel de Persoonsgegevens die voor die afzonderlijke fase noodzakelijk zijn voor de uitvoering van ieder van de daarbij geformuleerde toepasselijke processtappen: Hier verwijzen naar het vertaaldocument waarin alle processtappen zijn beschreven.

Intake / Aanmelding

☐ beoordelen of een Casus die door een Partij wordt aangedragen voldoet aan de criteria voor behandeling in het zorg- en veiligheidshuis. Deze criteria volgen uit het Landelijk Kader.

Triage

- ☐ bepalen eerste beeld en verrijken van informatie uit Intake;
- ☐ op basis van informatie van partners komen tot een nadere afweging ten aanzien van de routing van de casus, tot een bepaling van doel en thema's van een eventueel Casusoverleg, en tot een afweging welke partners relevant zijn om te betrekken bij een Casusoverleg;
- ☐ voorbereiding Casusoverleg.

Casusoverleg

- ☐ opstellen gezamenlijk toestandbeeld door bij het Casusoverleg betrokken Partijen;
- ☐ opstellen integraal plan van aanpak;
- ☐ monitoren van de uitvoering en resultaten van het plan van aanpak;
- ☐ bepalen of verdere verstrekking van Persoonsgegevens aan andere samenwerkingsverbanden noodzakelijk en mogelijk is;
- ☐ besluiten tot afbouwen betrokkenheid zorg- en veiligheidshuis;
- ☐ besluiten tot Opschaling van de Casus.

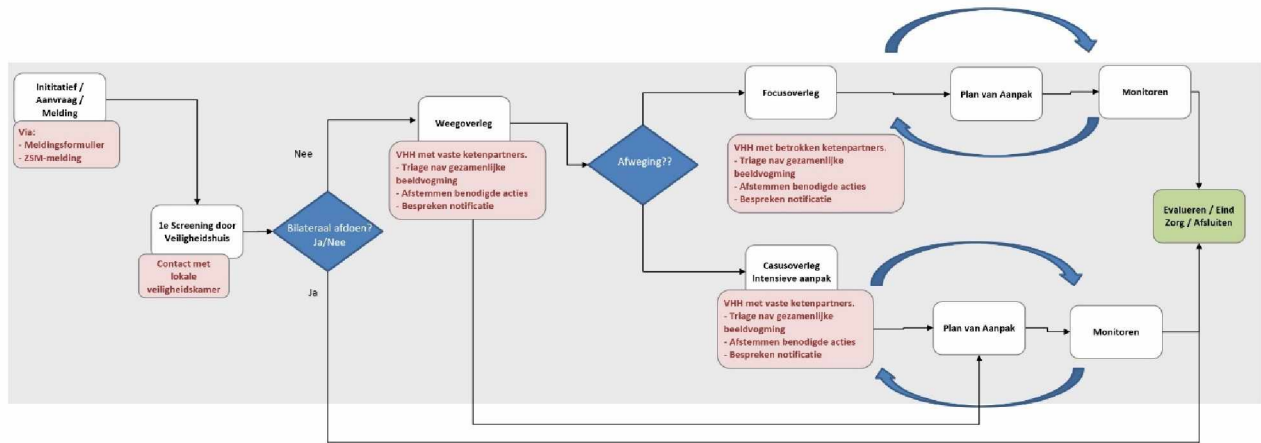
Afschaling

- ☐ bepalen van noodzakelijke te verstrekken Persoonsgegevens in het kader van Afschaling en de verstrekking daarvan aan bijvoorbeeld de Casusregisseur

4. Gegevensverwerking

Geef een beschrijving van de gegevensstroom.

Indien beschikbaar kan je een reeds bestaande 'dataflow' of procesbeschrijving toevoegen. Zo niet vul de tabel in volgens het voorbeeld in de figuur. Maak de gegevensverwerking inzichtelijk met behulp van onderstaande gegevensstroom. Van welke bronnen zijn de persoonsgegevens afkomstig, in welke vorm worden de persoonsgegevens aangeleverd, hoe ziet de verwerking eruit, in welke vorm wordt de verwerking opgeleverd en naar wie gaan de opgeleverde gegevens?



Hieronder volgt een beschrijving per processtap en activiteiten, welke gegevens worden verwerkt (in de zin van de AVG) met het bijbehorend(e) systeem/systemen.

Proces stap	Actie	Gegevens	Systeem
Intake	melding	• datum • doel van de melding • meldende organisatie • naam medewerker • functie medewerker • email • telefoonnummer • naam client • tussenvoegsels • voorletters • voornamen • geboortedatum • omschrijving problematiek	PGAx- portaal MS Outlook Haal Centraal / BRP
Triage	Informatie uitvraag, agendering, bespreking, besluit	• Gegevens intake • Financiële gegevens • Beschikt over ID bewijs / paspoort • Houding, gedrag en vaardigheden • Werk, opleiding en tijdsbesteding • Huisvesting • (Huiselijke) relaties • Geestelijke gezondheid (geen diagnostiek) • Lichamelijk gezondheid (geen diagnostiek) • Middelengebruik en verslavingen • Sociaal netwerk • Justitie en politie informatie • Ideologie • Datum, tijdstip overleg	MS Outlook PGAx Middenvelder
Casusoverleg	Beelvorming, oordeelsvorming en besluitvorming	• Gegevens intake & triage • Globaal doel aanpak • Oordeel ketenpartner • Interventies op client gekoppeld aan levensgebieden • ZSM advies • Casuscoördinator	MS Outlook PGAx
Plan van Aanpak	Interventies en informatie updates	• Gegevens intake, triage, casusoverleg en PvA • Stand van zaken levensgebieden intake • Stand van zaken interventies	MS Outlook PGAx

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen (brief, applicatie, mail, cloud) de persoonsgegevens worden verwerkt.

Benoem of sprake is van een handmatig of geautomatiseerd proces, (semi-)geautomatiseerde besluitvorming, profilering of big dataverwerkingen.

Bron	Gegevens van partners en derden, Gegevens uit eerdere onderzoeken, BRP
Input	Door inbrengen persoonsgegevens in PGAx (al dan niet met tussenkomst medewerkers ZVHH)
Verwerking	(Persoons-)gegevens worden verrijkt; gefaciliteerd door ZVHH (Procesregie)
Output	Plan van Aanpak, Interventies en zsm-advies
Ontvangers	Partners en derden (al dan niet ten gevolge van inbreng persoonsgegevens) en medewerkers ZVHH

5. Betrokken partijen en/of organisaties

Welke externe organisatie(s) is/zijn betrokken bij deze verwerking?			
Welke	Rol van deze organisatie ¹⁾	Doel toegang tot gegevens	Toelichting
Gemeenten: Den Haag; Delft; Leidschendam-Voorburg; Midden-Delfland; Pijnacker-Nootdorp; Rijswijk; Wassenaar; Westland; Zoetermeer; Partijen: Politie regionale eenheid Den Haag; Openbaar Ministerie; Reclassering Nederland; Leger des Heils reclassering; Fivoor; Parnassia Groep; GGZ Delfland; GGZ Rivierduinen; Jeugdbescherming West; Raad voor de kindbescherming; Veilig Thuis; GGD Haaglanden; Goodwillwerk Leger des Heils Regio Den Haag; Dienst Justitiële Inrichtingen Haaglanden; Middin; Teylingereind; Limor; Perspektief; JIT; Stichting Humanitas; William Schrikker Stichting; Kessler Stichting; Stichting Exodus; SHOP Den Haag; Stichting Barka;	Gezamenlijke verwerkings-verantwoordelijken	Leveren en opvragen van persoonsgegevens teneinde de eigen casus op te lossen	
Ranshuijsen BV	Verwerker		Ranshuijsen B.V.

			Adres: Westblaak 167, 3012 KJ Rotterdam Postadres: Postbus 52109,3007 LC Rotterdam Telefoon: 010 452 11 75 E-mail: info@renvl.nl Website: https://www.renvl.nl/
JustID	Ontvanger		Meldingen bij ZVHH worden gecontroleerd op bekendheid van deze persoon bij andere ZVHen. Dit proces vindt plaats dmv een zgn Middenvelder (Geautomatiseerd proces zonder opslag persoonsgegevens)

¹⁾ Een 'rol' kan zijn:

- Verwerkingsverantwoordelijk
- Verwerker
- Ontvanger
- Gezamenlijke verwerkingsverantwoordelijke

Afspraken over gegevensverwerking met externe partijen	Ja	Nee	Toelichting
Is er sprake van een schriftelijke overeenkomst?	x		
Bij een overeenkomst: contractnummer / contractreferentie, systeem/waar het contract wordt beheerd	x		20.461.BSD
Maken de volgende onderwerpen (IB-eisen, delen van gegevens, geheimhouding, vernietiging/teruggave gegevens bij einde contract, informeren over datalek) deel uit van deze overeenkomst?	x		
Indien van toepassing, is er een separate verwerkersovereenkomst gesloten?	x		
Wordt gewerkt met achterliggende partijen / subverwerkers? <i>NB: als onze contractspartij géén verwerker is, dan ligt de verantwoordelijkheid dat deze achterliggende partijen aan de AVG voldoen bij onze contractspartij.</i>		x	
Zijn er afspraken met samenwerkingspartners? <i>Dit kan zijn op basis van een convenant.</i>			

Toelichting (optioneel):

Het Zorg- en Veiligheidshuis Haaglanden is een 'netwerkorganisatie'. Dat houdt in dat het samenwerkt met een groot, en variërend aantal instanties bij de behandeling van verschillend gevallen. De partners in het ZVH zijn gezamenlijke verwerkingsverantwoordelijke.

6. Verwerkingslocatie(s)

Geef aan waar de gegevensverwerking plaatsvindt.

- ☒ Nederland
- ☐ EU
- ☐ EER
- ☐ VS
- ☐ Anders, t.w.....

Is er bij de overdracht van persoonsgegevens aan externe partijen buiten de EER sprake van contracten, clauses adequaatheidsbesluit?

Antwoord:

Er is géén sprake van overdracht of uitwisseling van gegevens met externe partijen buiten de EER. Er is gekozen voor een SaaS-oplossing met uitdrukkelijk afspraak om applicatie en opslag in Nederland op te slaan.

7. Juridisch en beleidsmatig kader

Noem de wet- en regelgeving en het beleid met betrekking tot de taken die uitgevoerd worden. Het gaat om de taken waarvoor de persoonsgegevens verwerkt worden.

Denk aan: Verzuimregelgeving, BW, Belastingregelgeving, Archiefwet, Arbeidsrecht, Telecomwet, Boetebeleid etc.

Antwoord:

Gemeentewet, Wet maatschappelijke ondersteuning, jeugdwet, participatiewet, wet gemeentelijke schuldhulpverlening, Wjsg, Wpg, Wetboek van Strafrecht, Wetboek van Strafvordering en aanvullende wetgeving, Burgerlijk wetboek en aanvullende wetgeving, Reclasseringsregeling Wgbo, Wbopz en Beginselwet justitiële inrichtingen.

8. (Semi-)Geautomatiseerde besluitvorming, profilering of big data-verwerkingen

Benoem of sprake is van (semi)geautomatiseerde besluitvorming, profilering of big dataverwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Antwoord:

Er is géén sprake van (semi) geautomatiseerde besluitvorming, profilering of big dataverwerking.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel aan de hand van de feiten zoals vastgesteld in onderdeel A of de voorgenomen gegevensverwerkingen rechtmatig zijn. Het gaat hier om de beoordeling van de juridische rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen. Beoordeel tevens de wijze waarop invulling wordt gegeven aan de rechten van de betrokkenen. Voor dit onderdeel van de GEB is in het bijzonder juridische expertise nodig.

9. Grondslag verwerking

Bepaal op welke grondslagen de gegevensverwerkingen worden gebaseerd.

- de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
- 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;
- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
- ◆ 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;
- 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.

Geef een toelichting op de gekozen grondslag:

Toelichting:

Zie antwoord bij vraag 7

Indien gekozen is voor het gerechtvaardigd belang als rechtsgrond dan moeten de volgende factoren betrokken worden in de belangenafweging:

Gevolgen voor betrokkenen, let op kind:

nvt

Aanvullende waarborgen om ongewenste gevolgen voor betrokkenen te beperken:

nvt

De ernst van de inmenging voor de betrokkene:

nvt

Kon betrokkene deze verwerking verwachten, is betrokkene geïnformeerd?

Ja, middels notificatiebrief

10. Bijzondere persoonsgegevens

10a: Beoordeel per bijzonder persoonsgegeven of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Neem de bijzondere gegevens over die zijn ingevuld bij vraag 2.

Kruis aan welke bijzondere gegevens u verwerkt. Het zijn persoonsgegevens waaruit valt af te leiden:

- X Ras of etnische afkomst
- X Politieke opvattingen
- X Religieuze of levensbeschouwelijke overtuigingen
- ☒ Lidmaatschap vakbond
- ☒ Een verwerking van genetische gegevens
- ☒ Een verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon
- X Een verwerking van gegevens over gezondheid
- X Een verwerking van gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid

Is het mogelijk om af te zien van het verwerken van deze bijzondere persoonsgegevens?

Antwoord:

Nee, de betrokkene dient juist geïdentificeerd te worden aan de hand van deze kenmerken

Geef per bijzonder gegeven aan welke uitzondering op het verwerkingsverbod van toepassing is. Zie de toelichting. Het kan gaan om:

- Een algemeen geformuleerde uitzondering op basis van de AVG art 9 lid 2.
- In de UAVG zijn deze algemeen geformuleerde uitzonderingen nader uitgewerkt. Daarnaast zijn uitzonderingen per bijzonder persoonsgegeven opgenomen. Zie de artikelen 22 t/m 30 UAVG.

Uitzonderingsgronden inzake bijzondere persoonsgegevens	Op welk persoonsgegeven is dit van toepassing?
Artikel 9 AVG jo Artikel 25 onder a UAVG	Ras en Etniciteit
Artikel 9 AVG jo Artikel 22 lid 2 onder d UAVG	Politieke opvattingen, religieuze of levensbeschouwelijke opvattingen en seksuele geaardheid
Artikel 9 AVG jo Artikel 30 lid 3 onder a UAVG	Gezondheid
	De hiervoor genoemde bepalingen hebben steeds ten doel en rechtvaardiging om bijzondere persoonsgegevens te verwerken ten einde betrokkene middels een gezamenlijke aanpak passend in de doelstellingen van het ZVH te begeleiden.

10b. Beoordeel of de verwerking van persoonsgegevens van strafrechtelijke aard is toegestaan op basis van de artikelen 32 en 33 UAVG.

Welke persoonsgegevens van strafrechtelijke aard worden door u verwerkt?

Antwoord:

Alle benodigde gegevens tbv de voorliggende casus

Is het mogelijk om af te zien van het verwerken van deze persoonsgegevens van strafrechtelijke aard?

Antwoord:

Nee

Geef aan welke uitzondering op het verwerkingsverbod van toepassing is.

Uitzonderingsgronden inzake gegevens van strafrechtelijke aard	Op welk persoonsgegeven is dit van toepassing?
Artikel 33 lid 1 onder b UAVG	Strafrechtelijke gegevens die zijn ingebracht

10c. Beoordeel of de verwerking van een wettelijk identificatienummer op basis van specifieke regelgeving is toegestaan.

Is een wettelijk identificatienummer toegestaan	JA	Nee	Zo ja, welke of hoe?
Wordt een wettelijk identificatienummer gebruikt zoals BSN.	X		BSN
Is er een wettelijke grondslag? Wet algemene bepalingen burgerservicenummer (Wabb)	X		Artikel 10 Wabb
Is het mogelijk om af te zien van het verwerken van wettelijke ID-nummers?		X	

10d. Beoordeel of er sprake is van de verwerking van andere gevoelige gegevens.

Verwerking gevoelige gegevens	JA	Nee	Zo ja, welke of hoe?
Is er sprake van gevoelige persoonsgegevens afhankelijk van de context zoals financiële gegevens, beoordelingen, loonbeslag, locatie?	X		Financiële gegevens
Zijn er extra beveiligingsmaatregelen genomen?			

11. Doelbinding verdere verwerking

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, **beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld (zoals beschreven bij vraag 3).**

Antwoord:

Gegevens kunnen ingezet worden voor wetenschappelijk of statistisch onderzoek. Deze verwerking zal altijd geanonimiseerd plaatsvinden.

12. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden (zoals beschreven bij vraag 3). Ga hierbij in ieder geval in op:

- a. *Proportionaliteit*: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
- b. *Subsidiariteit*: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt?

Noodzaak en evenredigheid	JA	Nee
Zijn alle persoonsgegevens die gebruikt worden noodzakelijk voor het doel waarvoor de gegevens verzameld zijn?	X	
Kan het doel bereikt worden met geanonimiseerde of gepseudonimiseerde data?		X
Is het mogelijk om op andere wijze aan het doel te voldoen (zonder de belastende persoonsgegevens te gebruiken)?		X

Nadere toelichting:

Om een compleet beeld te hebben van de betrokkene teneinde deze optimaal te kunnen ondersteunen worden er veel persoonsgegevens van hem verwerkt. Het is niet steeds op voorhand te zeggen welke persoonsgegevens wel en welke niet uiteindelijk van belang zijn voor het plan van aanpak. Desondanks handelen partners met de grootst mogelijke zorgvuldigheid zoals vastgelegd in het privacyprotocol.

13. Rechten van de betrokkene

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzonderingen of dat is toegestaan. Informeert u de betrokkene? Op welke wijze?

Nadere toelichting:

Op de website van de Partners en van ZVH wordt verwezen naar de mogelijkheid om de rechten als bedoeld in artikel 15 ev van de AVG in te roepen. Teneinde een dergelijk verzoek in goede banen te leiden zijn er voor ZVH privacyprotocollen opgesteld. ZVH vervult in dergelijke verzoeken een coördinerende rol met uitzondering van de politiegegevens en de justitiële en strafvorderlijke gegevens.

C. Beschrijving en beoordeling risico's voor de betrokkenen

14. Risico's

Er is een aanvullende risicoanalyse uitgevoerd, waarin twee *kleine* risico's gevonden. Namelijk:

Risico 1: Mede door de vele accounts van ketenpartners is er een kans dat er accounts actief zijn van mensen die niet meer zijn betrokken bij het proces en/of uit dienst zijn. Hierdoor is de kans aanwezig een persoon toegang heeft tot gegevens binnen PGAx die hier niet meer voor bevoegd is, waarmee het risico bestaat dat gegevens gelekt worden.

Risico 2: In het verleden zijn persoonsgegevens gelekt door het versturen van brieven naar verkeerde adressen. Dit risico bestaat nog steeds. Hierbij worden er NAW-gegevens van betrokkenen onbewust gelekt naar niet bevoegde.

D. Beschrijving voorgenomen maatregelen

15. Maatregelen

De proceseigenaar heeft opdracht gegeven om te voldoen aan BIO eisen en accepteert risico's op de genoemde onderwerpen.

Concreet zijn de volgende mitigerende acties voorgenomen om uitgevoerd te worden:

- We gaan de betrokken netwerkpartners dringend vragen z.s.m. melding te doen van uit diens treding van medewerkers en actie te ondernemen om toegang tot PGAx voor deze mensen te ontfeggen.
Voor medewerkers bij het ZVHH en de gemeente Den Haag geldt het *single sign on principe* en is toegang tot PGAx gekoppeld aan het gemeentelijk account: bij uitdienst treding en opheffing van het gemeentelijk account vervalt automatisch de toegang tot PGAx.
- We gaan het procesdeel waarin 'brieven per post' worden gestuurd melden dat men extra voorzichtig moet zijn bij de adressering ten einde onjuiste adressering te voorkomen.

Bijlage 1 Begrippenkader

Hieronder volgen de belangrijkste begrippen die in dit document worden gebruikt.

Begrip	Toelichting
AVG/ GDPR	Algemene Verordening Gegevensbescherming / General Data Protection Regulation. Europese regelgeving gericht op de bescherming van persoonsgegevens en het vrije verkeer van die gegevens. In werking sinds 25 mei 2018.
GEB / DPIA	Gegevensbeschermingseffectbeoordeling of data protection impact assessment.
Normale Persoonsgegevens	Elk kenmerk dat direct of indirect herleidbaar is tot een natuurlijke persoon. Bijvoorbeeld naam, identificatienummer, locatie, IP-adres, fysieke en sociale kenmerken. De verwerking van deze gegevens moet voldoen aan een aantal beginselen.
Bijzondere persoonsgegevens	Persoonsgegevens die betrekking hebben op gevoelige informatie zoals etniciteit, seksuele gerichtheid, politieke, religieuze of levensbeschouwelijke overtuigingen en gegevens over gezondheid. Verwerking van deze gegevens is verboden tenzij aan specifieke voorwaarden wordt voldaan.
Gevoelige persoonsgegevens	Naast de bijzondere persoonsgegevens zijn er nog andere gevoelige gegevens. Persoonsgegevens die een hogere impact op de privacy hebben dan gewone persoonsgegevens zijn bijv. beoordelingen, gegevens over kwetsbare personen als minder valide personen, bewoners van zorginstellingen, financiële gegevens zoals salaris en bankrekeninggegevens.
Bijzondere categorie	Een bijzondere categorie van persoonsgegevens is gegevens van strafrechtelijke aard, hiervoor gelden strenge voorwaarden. Ook wettelijke persoonsidentificerende nummers zijn persoonsgegevens van een bijzondere categorie omdat deze alleen met een wettelijke grondslag verwerkt mogen worden.
Rechten betrokkene	Een persoon over wie persoonsgegevens verwerkt worden, heeft recht op inzage, vergetelheid, rectificatie en aanvulling, dataportabiliteit, beperking, met betrekking tot profilering en besluitvorming, en het recht op duidelijke informatie over wat er met de persoonsgegevens gebeurt.
Anonimiseren	Het zodanig verwerken van persoonsgegevens dat deze nooit meer herleidbaar zijn tot een persoon. Alleen wanneer de verwerking vanaf het allereerste begin anoniem plaatsvindt, is de AVG / GDPR niet van toepassing.
Pseudonimiseren	Het zodanig verwerken van persoonsgegevens dat deze alleen nog herleidbaar zijn tot een persoon met behulp van aanvullende gegevens, waarbij deze aanvullende gegevens apart worden bewaard en beveiligd met technische en organisatorische maatregelen.
Verwerking	Een verwerking is een al dan niet geautomatiseerd proces waarbij persoonsgegevens betrokken zijn, denk aan het verzamelen, vastleggen, raadplegen en vernietigen van persoonsgegevens.
Grondslag verwerking	Verwerking van persoonsgegevens is toegestaan wanneer één van de volgende grondslagen van toepassing is (art. 6 AVG): • Toestemming van betrokkene (vastgelegd); • noodzakelijk voor de uitvoering van een overeenkomst; • wettelijke verplichting; • bescherming van vitale belangen; • vervulling van een taak van algemeen belang / openbaar gezag; • behartiging van gerechtvaardigd belang van verantwoordelijke of een derde.

	Voor de verwerking van bijzondere gegevens, gegevens van strafrechtelijke aard of wettelijke persoonsidentificerende nummers is een aparte grondslag nodig.
Verwerkings-verantwoordelijke art. 4 AVG	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; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.
Verwerker art. 4 AVG	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Ontvanger art. 4 AVG	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk 4.5.2016 NL Publicatieblad van de Europese Unie L 119/33 persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijke recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn.
Derde art. 4 AVG	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.

VERTROUWELIJK

RIEC Den Haag

t.a.v. 5.1.2.e

Postbus 16471

2500 BL Den Haag

Per mail: 5.1.2.e

Datum : 11 mei 2022
Ons kenmerk : 9820
Adviseur : 5.1.2.e
Betreft : advies gegevensdeling met HEIT

Geachte 5.1.2.e

Op 17 maart 2022 is afgesproken dat wij een advies opstellen over het delen van informatie tussen het RIEC Den Haag en het HEIT. Op 25 april 2022 zond ik u een eerste versie van dit advies. Vandaag bespreken wij deze eerste versie van het advies, naar aanleiding waarvan ik hierbij de definitieve versie toestuur.

Inleiding

Het Regionaal Informatie- en Expertise Centrum (RIEC) Den Haag ondersteunt haar ketenpartners bij de aanpak van georganiseerde criminaliteit. Met deze ketenpartners is een samenwerkingsconvenant afgesproken. Het Haags Economisch Interventie Team (HEIT) is een onderdeel van de directie Veiligheid van de gemeente Den Haag en valt onder direct gezag van de burgemeester van Den Haag. Binnen het HEIT werken de gemeente, de Belastingdienst, de Douane, de Inspectie SZW, de Nederlandse Voedsel- en Warenautoriteit (NVWA), het UWW en drie omgevingsdiensten samen om ondermijnende en criminele bedrijfsactiviteiten aan te pakken. Om dit doel te bereiken, voert het HEIT bestuurlijke integrale controles (interventies) uit bij (mogelijk) malafide ondernemingen op basis van meldingen of signalen. Iedere ketenpartner voert hierbij de eigen publiekrechtelijke controlebevoegdheden uit.

Binnen het kader van de HEIT samenwerking worden persoonsgegevens tussen ketenpartners uitgewisseld om te komen tot een controle. De mogelijkheid tot het delen van persoonsgegevens is opgenomen in het samenwerkingsconvenant. Hiervoor is een werkproces opgesteld dat een afgeleide vormt van het RIEC werkproces van signaal tot interventie.

Naar aanleiding van het actualiseren van de werkprocessen bij het RIEC Den Haag, ontstaat de vraag of de HEIT samenwerking nog altijd past binnen de kaders van het RIEC convenant. Daarnaast wordt naar verwachting in 2022 of 2023 het RIEC als samenwerkingsverband in de Wet Gegevensverwerking door Samenwerkingsverbanden (WGS) opgenomen, waardoor een wettelijke grondslag ontstaat voor de gegevensverwerking binnen het RIEC-samenwerkingsverband. Het is onduidelijk of het HEIT dan voor de informatiedeling nog kan functioneren onder de RIEC-kaders in de WGS.

Het RIEC samenwerkingsconvenant

De samenwerking tussen de partners in het HEIT vindt momenteel plaats volgens de afspraken in het RIEC-LIEC convenant en bijbehorend Privacyprotocol RIEC'S-LIEC (laatste versie september 2021). In deze documenten staat nauwkeurig beschreven op welke wijze convenantpartners in het samenwerkingsverband persoonsgegevens delen. Daarnaast worden de verwerkingsverantwoordelijken verplicht op transparante wijze hun verantwoordelijkheden voor de nakoming van de AVG vast te stellen, zoals de uitoefening van de rechten van betrokkenen. Er is tevens een meldplicht datalekken opgenomen waarin duidelijk staat beschreven op welke wijze de verwerkingsverantwoordelijken dienen om te gaan met een (mogelijk) datalek.

Artikel 26 van de Algemene verordening gegevensbescherming (AVG) biedt de mogelijkheid aan verschillende instanties, bedrijven en organisaties om voor een gezamenlijk doel persoonsgegevens te verwerken. Deze deelnemers aan een samenwerkingsverband in de zin van artikel 26 AVG zijn dan gezamenlijk aan te merken als verwerkingsverantwoordelijken. Artikel 26 AVG bepaalt dat de gezamenlijke verwerkingsverantwoordelijken een onderlinge regeling dienen te treffen, waarin de nakoming van de verplichtingen uit hoofde van de AVG worden vastgelegd. Uit de regeling moet duidelijk blijken welke rol de gezamenlijke verwerkingsverantwoordelijken vervullen en wat hun verhouding met de betrokkenen is, met name met betrekking tot de uitoefening van de rechten van de betrokkenen.

In artikel 5.1 van het Privacyprotocol RIEC'S-LIEC is vastgelegd dat het doel van de samenwerking een bestuurlijke en geïntegreerde aanpak van de georganiseerde criminaliteit betreft, door naast het strafrechtelijk laten vervolgen van individuele betrokkenen en het ontmantelen van criminele samenwerkingsverbanden ook bestuursrechtelijke interventies en fiscale handhaving aan te wenden om de georganiseerde criminaliteit te bestrijden. In artikel 6 van het Privacyprotocol RIEC'S-LIEC is vastgelegd dat op de gegevensverwerkingen binnen het RIEC de AVG en de Uitvoeringswet AVG (UAVG) van toepassing zijn.

De grondslag voor de verwerking van gegevens door het samenwerkingsverband wordt gevonden in artikel 6, eerste lid, onder e, van de AVG. De verwerkingsgrondslagen voor de verstrekking van persoonsgegevens door de partners aan het samenwerkingsverband RIEC zijn terug te vinden in wettelijke bepalingen die op de convenantpartners van toepassing zijn. Voor een aantal convenantpartners gelden artikelen uit de AVG en de UAVG als wettelijke grondslag. Voor een aantal andere convenantpartners gelden (daarnaast) sectorale wetten waarin bepalingen die betrekking hebben op de verstrekking van persoonsgegevens zijn opgenomen, zoals de Gemeentewet, de Wet politiegegevens, de Wet justitiële en strafvorderlijke gegevens en de Algemene wet inzake rijksbelastingen (AWR).

De onderwerpen die conform artikel 26 AVG in een onderlinge regeling dienen te zijn opgenomen, zijn in het Privacyprotocol RIEC'S-LIEC neergelegd. Gelet op de doelstelling van het HEIT en het beschreven werkproces, voldoet naar de huidige maatstaven de samenwerking binnen het HEIT aan de bepalingen van de AVG en past dit binnen de kaders van het RIEC convenant. Door het RIEC-LIEC convenant en bijbehorend Privacyprotocol RIEC'S-LIEC van toepassing te verklaren op de samenwerking binnen het HEIT, wordt voldaan aan de eisen van artikel 26 AVG. Bij iedere nieuwe verwerking van persoonsgegevens door en binnen het HEIT, dient wel te worden nagegaan of die verwerking binnen het HEIT samenwerkingsverband overeenkomst met de doelstellingen van het RIEC-LIEC convenant en artikel 5.1 van het Privacyprotocol RIEC'S-LIEC.

Het wetsvoorstel Gegevensverwerking door samenwerkingsverbanden

Momenteel ligt het wetsvoorstel Gegevensverwerking door samenwerkingsverbanden (WGS) ter beoordeling bij de Eerste Kamer der Staten-Generaal. Volgens de toelichting op het wetsvoorstel doet zich bij de huidige samenwerkingsverbanden een aantal knelpunten voor. Zo bevatten sectorale wetten op basis waarvan gegevens worden uitgewisseld geen goede grondslag voor de verwerking van (persoons)gegevens aan en door samenwerkingsverbanden. Veel van dit soort samenwerkingsverbanden werken momenteel samen op basis van een door hen zelf opgesteld convenant. Ook is het juridisch niet toegestaan dat private partijen toegang krijgen tot de gegevens uit een samenwerkingsverband of deze gegevens met elkaar delen. Het doel van de WGS is om een wettelijke grondslag voor samenwerkingsverbanden te gaan bieden. De WGS omschrijft een samenwerkingsverband als

“Een verband van deelnemers die gezamenlijk gegevens verwerken voor een bij of krachtens deze wet vastgestelde doelstelling van zwaarwegend algemeen belang.”

In de WGS worden vier samenwerkingsverbanden aangewezen als samenwerkingsverbanden in de zin van die wet. Het betreft het Financieel Expertisecentrum (FEC), de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV), de Regionale Informatie- en Expertisecentra (RIEC's) en de Zorg- en Veiligheidshuizen.

Het wetsvoorstel bevat in hoofdstuk 3 een delegatiegrondslag op basis waarvan andere samenwerkingsverbanden en deelnemers bij Algemene Maatregel van Bestuur (AMvB) kunnen worden aangewezen. Deze samenwerkingsverbanden mogen slechts in het leven worden geroepen voor drie doelstellingen, namelijk het voorkomen en bestrijden van criminaliteit, onrechtmatig gebruik van overheidsmiddelen en ontduiking van wettelijke verplichtingen.

Tijdens de parlementaire behandeling is door de Tweede Kamer een amendement aangenomen dat regelt dat een voorhangprocedure wordt gevolgd voor de toevoeging van nieuwe deelnemers aan een samenwerkingsverband bij AMvB, gekoppeld aan een voorafgaande goedkeuring door het parlement. Zo is het dus uiteindelijk aan het parlement om te bepalen of er een zwaarwegend algemeen belang bestaat dat het aanwijzen van een samenwerkingsverband rechtvaardigt. De wetgever wil dat de WGS een expliciete juridische basis gaat bieden voor de gegevensverwerking door samenwerkingsverbanden die het doel hebben fraude, criminaliteit en/of ondermijning tegen te gaan.

Een eigen protocol?

Het RIEC-LIEC convenant is in het wetsvoorstel WGS gecodificeerd in paragraaf 2.3. Na de inwerkingtreding van de WGS zijn de bepalingen van deze paragraaf van toepassing op de samenwerking binnen het RIEC en zullen deze bepalingen in de plaats treden van het convenant. Omdat het HEIT in de WGS niet wordt genoemd en niet bij AMvB is aangewezen, kan na inwerkingtreding van de WGS niet meer worden verwezen naar de bepalingen uit het RIEC-convenant. De vraag komt dan aan de orde of het HEIT de huidige samenwerking kan voortzetten door de deelnemers een eigen convenant te laten overeenkomen. In artikel 1.2, lid 2 WGS is bepaald dat deze wet onverlet laat dat deelnemers van een samenwerkingsverband onderling gegevens kunnen blijven verwerken bij of krachtens een andere dan deze wet. Voor de samenwerking binnen het HEIT is geen andere specifieke wet beschikbaar waarop de samenwerking kan worden gebaseerd en de juridische basis voor het delen van persoonsgegevens binnen het HEIT dient om die reden te worden gebaseerd op de algemene bepaling van artikel 26 AVG.

De AVG verzet zich niet tegen het delen van persoonsgegevens binnen een samenwerkingsverband, als de deelnemers daaraan zijn te beschouwen als gezamenlijke verwerkingsverantwoordelijken en een onderlinge regeling treffen. Als de deelnemers aan het HEIT hun gezamenlijke verantwoordelijkheid ten aanzien van het doel waarvoor en de middelen waarmee persoonsgegevens worden verwerkt, transparant omschrijven in een onderlinge regeling die voldoet aan artikel 26 AVG, dan is het delen van persoonsgegevens niet in strijd met de privacywetgeving. Deze onderlinge regeling, het eigen protocol dus, kan worden opgesteld met als basis daarvoor het huidige RIEC-LIEC convenant en bijbehorend Privacyprotocol RIEC'S-LIEC.

Hoewel het op grond van de AVG en overige privacywetgeving, zoals de Wet politiegegevens, niet verboden is om met een eigen protocol de samenwerking binnen het HEIT voort te zetten, wordt daarmee naar onze overtuiging wel voorbij gegaan aan de bedoeling van de wetgever om samenwerkingsverbanden die als doel hebben gezamenlijk gegevens te laten verwerken om fraude, criminaliteit en/of ondermijning tegen te gaan, te voorzien van een expliciete juridische basis. Hiervoor is de WGS nu juist bedoeld. De doelstellingen van het HEIT zijn weliswaar verenigbaar met de doelen die in het RIEC-LIEC convenant en bijbehorend Privacyprotocol RIEC'S-LIEC worden genoemd, de expliciete juridische basis die de wetgever daarvoor wenselijk acht, ontbreekt.

Aansluiten bij de WGS?

Om aan de bedoeling van de wetgever te voldoen, dus om de verwerking van persoonsgegevens via de samenwerking binnen het HEIT te baseren op een expliciete juridische grondslag, is de meest aangewezen weg daarvoor het HEIT via een AMvB door de Minister te laten aanwijzen als samenwerkingsverband in de zin van de WGS. Artikel 3.1 WGS geeft aan dat dit mogelijk is voor een doelstelling van zwaarwegend algemene belang inzake het voorkomen en bestrijden van criminaliteit, onrechtmatig gebruik van overheidsmiddelen en ontduiking van wettelijke verplichtingen. De doelstellingen van het HEIT lijken aan te sluiten bij deze doelstellingen. Hiervoor dient een voordracht te worden gedaan bij de Minister van Justitie en Veiligheid en/of de Minister voor Rechtsbescherming en het parlement dient daar mee in te stemmen.

Bovenstaande procedure zal de nodige tijd in beslag nemen en niet kan worden gegarandeerd dat het HEIT ook daadwerkelijk bij AMvB wordt aangewezen als samenwerkingsverband in de zin van de WGS. Als het HEIT na inwerkingtreding van de WGS daartoe (nog) niet is aangewezen maar de samenwerking wil voortzetten, zal zij (in ieder geval tijdelijk) een eigen protocol dienen te hanteren.

Conclusie en aanbevelingen

Op grond van de bovenstaande bevindingen komen wij tot de volgende conclusie en aanbevelingen.

1. Het wetsvoorstel WGS ligt op dit moment ter beoordeling bij de Eerste Kamer der Staten-Generaal. Op dit moment is niet duidelijk of en zo ja wanneer de WGS in werking zal treden. Mede door de Autoriteit Persoonsgegevens is de nodige kritiek geleverd op het wetsvoorstel. Het is de vraag of de Eerste Kamer zich de kritiek van de Autoriteit Persoonsgegevens zal aantrekken en of het wetsvoorstel al of niet of in sterk gewijzigde vorm wordt aangenomen. Wij adviseren om, zolang de WGS niet in werking is getreden, het RIEC-LIEC convenant en bijbehorend Privacyprotocol RIEC'S-LIEC te blijven hanteren als juridische grondslag voor de samenwerking binnen het HEIT.

Daarbij wijzen wij er wel op dat als binnen het HEIT persoonsgegevens worden verwerkt om een reden die niet past bij de doelstellingen die in het RIEC-LIEC convenant zijn neergelegd, het HEIT dit dient te ondervangen. Dat is mogelijk door de reden voor de betreffende verwerking nog eens kritisch te beschouwen en eventueel te herformuleren, door af te zien van de verwerking of door binnen het HEIT aanvullende afspraken te maken en vast te leggen, als aanvulling op het RIEC-LIEC convenant en het Privacyprotocol RIEC'S-LIEC.

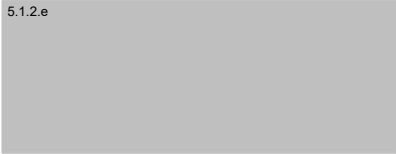
2. Ter voorbereiding op de inwerkingtreding van de WGS adviseren wij om een document op te stellen waarin het HEIT bij de Minister wordt voorgedragen om te worden aangewezen als samenwerkingsverband dat bij AMvB onder de werking van de WGS valt. Daarin dient duidelijk te worden gemaakt dat de doelstellingen van het HEIT overeenkomen met de in artikel 3.1 WGS geformuleerde doelstellingen en dat het een zwaarwegend belang betreft aangezien het HEIT zich richt op het bestrijden van economische ondermijning, dus op het bestrijden van georganiseerde criminaliteit die gebruikmaakt van legale structuren in de stad.
3. Voorts adviseren wij om een eigen protocol overeen te komen met de deelnemers aan het HEIT, waarbij het RIEC-LIEC convenant en bijbehorend Privacyprotocol RIEC'S-LIEC als uitgangspunt kan worden genomen. Daarbij kan eventueel ook worden onderzocht of bepalingen van convenanten van andere samenwerkingsverbanden, zoals het convenant van de Landelijke Stuurgroep Interventieteams (LSI), passend zijn voor het HEIT samenwerkingsverband. Dit eigen protocol van het HEIT kan dan dienen als tijdelijke basis voor de verwerking van gegevens binnen het HEIT zolang het HEIT nog niet bij AMvB is aangewezen als samenwerkingsverband dat onder de WGS valt of als blijvende basis als een dergelijk verzoek tot aanwijzing niet wordt gedaan of door de Minister wordt afgewezen.
4. Als instanties die momenteel aan het HEIT deelnemen, na inwerkingtreding van de WGS niet op basis van een eigen protocol willen blijven deelnemen, waaronder mogelijk de Belastingdienst, dan is de uitwisseling van persoonsgegevens voor een gezamenlijk doel met deze instanties niet meer mogelijk. Daarvoor bestaat dan immers geen rechtsgrond meer. Persoonsgegevens zijn gegevens waarmee een natuurlijk, nog levend persoon kan worden geïdentificeerd. Bedrijfsgegevens (met uitzondering van de eenmanszaak) zijn geen persoonsgegevens. Het blijft dus wel mogelijk om bedrijfsgegevens, zoals de naam van het bedrijf en de statutaire vestigingsplaats, uit te wisselen met (bijvoorbeeld) de Belastingdienst om tot een gezamenlijke aanpak te komen.

5. Tot slot blijft het mogelijk dat een deelnemer aan het HEIT (bijvoorbeeld de gemeente of de Belastingdienst) binnen het RIEC samenwerkingsverband een individuele casus inbrengt als deze casus zich daar volgens de bepalingen van de WGS voor leent.

Wij vertrouwen er op u met onderhavig advies voldoende te hebben geïnformeerd. Mochten er vragen of onduidelijkheden zijn, neemt u dan vooral contact met ons op.

Hoogachtend,

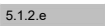
5.1.2.e



5.1.2.e



5.1.2.e



Uit de DPIA:	Reactie vanuit gemeente Den Haag:	Reactie vanuit VKA:
Algemeen:	We merken dat ^{5.1.2.e} constatering doet, maar we missen hierin de nuance. Het doel van deze DPIA is dat het document ondersteunend is aan het traject om te komen tot een nieuw convenant en privacy protocol, ondertekend door alle HEIT partners. Het is niet wenselijk dat een DPIA vragen gaat oproepen bij partners.	Zie toelichting op hieronder genoemde punten. De DPIA betreft een onafhankelijk rapport dat is opgesteld door ^{5.1.2.e} . Op basis van de feiten, zoals opgehaald tijdens de workshops, hebben we (privacy) risico's geconstateerd en maatregelen voorgesteld.
Pagina 13. Eerste alinea Het wetsvoorstel: WGS versterkt de juridische basis...tm deze worden opgesteld en waren ten tijde van de plenaire bijeenkomst nog niet afgerond"	Deze tekst zou genuanceerd kunnen worden. De doelstellingen van het HEIT en het RIEC zijn verenigbaar, maar dit betekent niet dat het HEIT opgaat in het RIEC en daarom kan het niet onder de WGS gaan vallen. Dit is juridisch al uitgelopen.	Wij zien vanuit privacy oogpunt een risico ten aanzien van de wettelijke grondslag op het moment dat het HEIT wordt losgekoppeld van het RIEC. Wij kunnen dit risico niet onbenoemd laten, omdat dit risico valt binnen de scope en reikwijdte van deze DPIA. Een definitieve beoordeling vanuit ^{5.1.2.e} op dit moment was niet mogelijk, omdat inzage in het advies van het LIEC niet mogelijk was. Ik heb de tekst op pagina 13 gedeeltelijk genuanceerd door jouw opmerking hierin te verwerken.
Pagina 16. Tweede alinea De WGS is op 17 december jl goedgekeurd....tm omdat het huidige wetsvoorstel nog aan amendering onderhevig is'	Afgelopen jaar is met de juristen van het LIEC hierover gesproken en het HEIT kan niet gaan vallen onder de WGS. Er is geadviseerd om deze route te gaan volgen. Zoals aangegeven in de vorige versie: de tekst over de WGS kan uit de DPIA gehaald worden omdat geen relevantie heeft voor het HEIT. Dat er voor andere landelijk opererende samenwerkingsverbanden	Ik heb deze aanvulling verwerkt in de tekst van de rapportage. Daarnaast een kleine nuance toegevoegd. De verwijzing naar de Wgs is noodzakelijk om te vermelden in deze DPIA, omdat het de onderbouwing is voor de wettelijke grondslag. Dit is tevens relevant in het kader van de verantwoordingsplicht en is onderdeel



	wel een juridische grondslag is ontwikkeld, heeft geen meerwaarde voor het HEIT.	van de eisen die de AP stelt voor een aanvaardbare EDPD.
Pagina 16. Vijfde alinea Risico: er is geen wettelijke grondslag voor gegevensuitwisseling binnen het HEIT Er is geen juridische basis voor gegevensverwerking binnen het HEIT doordat het HEIT geen juridische status heeft en ondanks het zwaarwegende algemeen belang waarvoor de gegevensverwerking plaatsvindt.	Dit zinsnede wordt als risico beoordeeld terwijl dit m.i. geen risico is. Het HEIT opereert al sinds 2004 zo. De RIECs al sinds 2011 en het Veiligheidshuis Den Haag al sinds 2009. Als het risico zo groot zou zijn, dan zou, als we deze redenatie zouden moeten volgen, deze samenwerkingsverbanden ook risico moeten lopen. Maar benoemd dat dan ook zo. Er is op dit moment geen wettelijke grondslag, maar dat is op dit moment voor geen enkele samenwerkingsorganisatie in Nederland. Beter zou zijn om te schrijven: risico: dek het risico voor het gemis van een wettelijke grondslag voor gegevensuitwisseling zo goed mogelijk af. Geen enkel samenwerkingsverband in Nederland heeft deze juridische basis. Het HEIT gaat dit risico goed afdekken door een eigen covenant en Privacy protocol op te stellen (eind dit jaar afgerond). Op dit moment werkt het HEIT onder het covenant & privacy covenant van het RIEC. (kortom, het risico is op dit moment hetzelfde als voor het RIEC of een veiligheidshuis)	Hoewel er nu vanuit juridisch optiek een wettelijke grondslag ontbreekt, wordt dit hiaat in de wetgeving opgelost met de komst van de Wgs. Dit geldt echter niet, zoals hiervoor aangegeven, in het bijzonder voor de situatie waarin het HEIT onafhankelijk van het RIEC gaat opereren. Ondanks de oplossing met de Wgs, is dit vanuit juridisch oogpunt een risico wat binnen de scope van de DPIA valt en wij daarom moeten adresseren. Dit risico geldt tevens voor andere samenwerkingsverbanden. Dat hebben we ook benoemd in de rapportage. Ik heb de maatregel aangevuld overeenkomstig jouw opmerking. De gegevensverwerking blijft echter onrechtmatig binnen het HEIT.
De WGS beoogt een algemene juridische grondslag te geven voor gegevensverwerking door overheidsorganisaties voor het bestrijden van , onder andere, ernstige vormen van criminaliteit en ondermijning. Het HEIT wordt in de WGS niet aangewezen als samenwerkingsverband in deze context	Zie eerdere opmerking. In samenspraak met het LIEC is ervoor gekozen om weer onder het oude HEIT covenant te gaan vallen. Deze zinsnede is daarom niet relevant en overbodig.	Zie eerdere opmerking.
Maatregel (pagina 17) Rond het HEIT covenant en bijbehorende privacy protocol af.	Dit is de omgekeerde wereld. De DPIA is gestart als voorwaarde voor het covenant en het PP, en niet andersom.	Een DPIA brengt de risico's voor een specifieke verwerking in beeld. Een van de belangrijke voorwaarden rondom het verwerken van gegevens is

		duidelijkheid tussen partijen over onderlinge gegevensdeling en de daarover gemaakte afspraken. Deze worden doorgaans vastgelegd in een convenant, privacy protocol of andere documentatie. Nu deze nog niet definitief zijn, vormt dit een privacyrisico welke we moeten benoemen in de DPIA.
Zoek uit of de doelstellingen van het HEIT en het RIEC verenigbaar zijn.	Dit is al uitgelopen en dit is verenigbaar.	Zie eerdere opmerking.
Het HEIT kan als dienst vanuit de gemeente Den Haag worden aangeboden en vanuit deze rol signalen oppakken en interventies coördineren	Dit lijkt me niet relevant voor bovenstaand stuk. Dit doet het HEIT al 7 jaar, het gaat niet om deze casussen.	
Indien het noodzakelijk is om gegevens uit te wisselen met ketenpartners zou dit kunnen geschieden onder het RIEC convenant (zie als voorbeeld hoe de ondermijningsbrigade van de gemeente Amsterdam is ingericht)	De gemeente Amsterdam heeft een Ondermijningsbrigade die twee maanden geleden opgericht en gestart is. Zij delen bij hun casussen nauwelijks informatie, alleen het adres van de te bezoeken onderneming. Ze hebben de intentie om ook een kopie van de Kvk inschrijving en het Kadaster (open bronnen) te delen. Ze hebben geen convenant of privacy protocol. Uiteraard hebben ze de mogelijkheid om als gemeente deel te nemen aan RIEC casussen en kunnen ze in dat kader ook controles uitvoeren waarbij wel de informatie gedeeld is, zo gaat het in Den Haag ook al 7 jaar. Echter het verschil is dat het HEIT voor het RIEC rond de 10 a 15 controles per jaar uitvoert en zelfstandig tussen de 350 a 500 controles. De Ondermijningsbrigade is een pilot en is de afgelopen jaren diverse malen bij het HEIT langs geweest om te leren hoe het HEIT werkt aangezien het HEIT al 17 jaar lang bestaat.	Met de verwijzing naar de ondermijningsbrigade willen we alleen een voorstel doen voor de inrichting. We zullen deze voorgestelde maatregel verwijderen .
4.4. Data minimalisatie Pagina 19 paragraaf 8	Hier is op de vorige versie van de DPIA al aangegeven: het HEIT is al zeer terughoudend met het delen van (persoons) informatie.	Daar sluit ik mij bij aan. Dit is echter niet relevant voor alle partijen. Het debriefingsdocument, zoals begrepen uit de workshop, wordt wel met alle partijen gedeeld.



Risico: constatering kunnen herleidbaar zijn naar personen. overweeg om (bepaalde) constatering die herleidbaar zijn naar een persoon niet te registreren, maar (alleen) mondeling te bespreken tijdens de debriefing. Hierdoor voorkom je dat er meer persoonsgegevens worden verwerkt dan noodzakelijk is voor het doel van de interventie.	Een aantal partijen in het HEIT, zoals de Inspectie SZW, SZW en het UWV controleren op de naleving van sociale wetgeving en hierbij gaat het om het personeel. Het is niet mogelijk voor hen om samen te werken en helemaal geen persoonsinformatie uit te wisselen. Dat maakt een verhoor afnemen van medewerkers onmogelijk. Dit advies lijkt me daarom niet proportioneel en het antwoord vanuit VKA maakt niet inzichtelijk waarom dit een risico zou moeten zijn. Het advies om alleen tijdens een debriefing persoonsgegevens te delen is lastig en onwerkbaar omdat niet alle partijen altijd meegaan en bij de debriefing aanwezig zijn, terwijl ze deze informatie wel nodig hebben. Er wordt geenszins een inbreuk gemaakt op de privacy van betrokkenen aangezien alleen misstanden worden vastgelegd waar een of meerdere organisaties (bestuurlijke) opvolging aan moeten geven.	Dit risico heeft betrekking op de situatie dat het HEIT afgesplitst wordt van het RIEC. Voor het HEIT geldt dat, vanuit het oogpunt van dataminimalisatie, de informatie die wordt vastgelegd in het debriefingsdocument in PerfectView verder reikt dan het oorspronkelijke doel. Dit gaat namelijk verder dan het monitoren op welke acties partners voornemens zijn om uit te voeren. Dit is een privacyrisico en hoort daarom thuis in deze DPIA. Ik pas dit overeenkomstig aan in de rapportage.
--	---	---

Template DPIA rapportage

Versiebeheer

Versie	Datum	Wijzigingen	Wie
0.8	02-03-21	Oplevering concept (0.8)	5.1.2.e
0.9	13-04-2021	Oplevering concept (0.9)	5.1.2.e
1.0	03-06-2021	Oplevering definitieve versie	5.1.2.e

Inhoudsopgave

1. Inleiding	3
<i>Aanleiding en onderwerp van de DPIA</i>	<i>3</i>
<i>Doelstelling</i>	<i>3</i>
<i>Scope</i>	<i>3</i>
<i>Opbouw van de analyse</i>	<i>4</i>
2. Managementsamenvatting	5
3. Beschrijving Verwerking	7
<i>Systematische beschrijving van het proces</i>	<i>7</i>
<i>Systematische beschrijving van de verwerking</i>	<i>9</i>
<i>Persoonsgegevens</i>	<i>11</i>
4. Analyse privacy consequenties	12
<i>Inleiding</i>	<i>12</i>
4.1 Governance	12
<i>Inleiding</i>	<i>12</i>
<i>Feiten & analyse</i>	<i>12</i>
<i>Risico's en maatregelen</i>	<i>13</i>
4.2 Grondslag & Doelbinding	15
<i>Inleiding</i>	<i>15</i>
<i>Feiten & analyse</i>	<i>15</i>
<i>Rechtmatigheid van de verwerking</i>	<i>16</i>
<i>Risico's en maatregelen</i>	<i>16</i>
4.3 Juistheid	18
<i>Inleiding</i>	<i>18</i>
<i>Feiten & Analyse</i>	<i>18</i>

Risico's en maatregelen.....	18
<i>4.4 Dataminimalisatie</i>	19
Inleiding.....	19
Feiten & Analyse.....	19
Risico's en maatregelen.....	19
<i>4.5 Opslag</i>	21
Inleiding.....	21
Feiten & Analyse.....	21
Risico's en maatregelen.....	22
<i>4.6 Bescherming</i>	23
Inleiding.....	23
Feiten & Analyse.....	23
<i>4.7 Transparantie</i>	25
Inleiding.....	25
Feiten & Analyse.....	25
Tijdens een interventie door het HEIT wordt de betrokkene geïnformeerd door middel van een daartoe bestemde flyer. Op de flyer staat duidelijk beschreven wat het doel van de interventie is en welke ketenpartners daaraan deelnemen. De flyer wordt uitgereikt door het aangewezen aanspreekpunt voor de betrokkene.....	25
Risico's en maatregelen.....	25
<i>4.8 Cultuur</i>	27
Inleiding.....	27
Feiten & analyse.....	27
Risico's en maatregelen.....	27
5. Advies en accordering	28
Aanbevelingen voor vervolg.....	28
Advies FG.....	29
Accordering.....	30
Bijlage A	31
A1. Documentatie.....	31
A2. Geïnterviewden.....	31

1. Inleiding

Aanleiding en onderwerp van de DPIA

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens is de gemeente verplicht een DPIA uit te voeren voor verwerkingen die waarschijnlijk een verhoogd risico opleveren.

Voor het HEIT is vastgesteld dat een verhoogd risico bestaat, namelijk: er worden bijzondere persoonsgegevens verwerkt in samenwerkingsverband.

Een DPIA is een middel om in kaart te brengen welke persoonsgegevens in een proces, systeem of organisatie verwerkt worden en wat hiervan de risico's voor betrokkenen zijn. Op 11 en 17 februari 2021 is een DPIA-workshop gehouden om de benodigde informatie hiervoor op te halen. In Bijlage A is opgenomen welke personen aan deze bijeenkomst hebben deelgenomen. Dit rapport is het resultaat van deze DPIA.

Doelstelling

Deze DPIA rapportage schetst de eventuele privacy risico's van de onderhavige gegevensverwerking, en maatregelen die kunnen worden getroffen teneinde deze risico's te mitigeren.

In de DPIA wordt vooral gekeken naar de geplande maatregelen, waarborgen en mechanismen om de risico's te beperken, de persoonsgegevens te beschermen en aan te tonen dat aan de beginselen voor verwerking uit de AVG is voldaan. Deze DPIA is een momentopname. Bij nieuwe ontwikkelingen zoals wijzigingen in wetgeving, verandering van processen, inzet van nieuwe technologie e.d. moet de DPIA worden herhaald. Ook dienen uitgevoerde DPIA's periodiek te worden herijkt (iedere 3 jaar).

Scope

Deze DPIA wordt uitgevoerd ten aanzien van gegevensverwerkingen in het proces HEIT.

De scope van het proces heeft betrekking op de gegevensverwerking binnen het HEIT.

In deze DPIA vindt geen risico analyse plaats op de reguliere werkprocessen van de samenwerkingspartners (zoals politie of belastingdienst) waarin de geconstateerde onrechtmatigheden worden afgehandeld door middel van het opleggen van boetes, maatregelen of anderszins opvolging van acties of strafrechtelijk optreden (samengevat: actiepunten uit de interventie(s) van het HEIT). Er vindt ook geen risicoanalyse plaats op het proces van het Team Prostitutie waarin misstanden in de prostitutiebranche worden aangepakt. Dit betreft een ander werkproces. Deze processen zijn tijdens de plenaire bijeenkomst buiten scope van deze DPIA geplaatst.

Opbouw van de analyse

Dit document schetst de privacy risico's binnen bovengenoemde scope en de te nemen maatregelen die het betreffende risico kunnen mitigeren.

De uitvoering van deze DPIA verloopt via de zes beginselen waaraan elke verwerking moet voldoen. Deze zes beginselen zijn Juistheid, Data minimalisatie, Opslag, Bescherming, Transparantie en Grondslag & doelbinding. Daarnaast zijn ook de thema's 'Governance' en 'Privacycultuur' van belang.

Deze beginselen vormen de basis voor de uitvoering van deze analyse. Per thema worden eventuele risico's geanalyseerd en wordt de impact van deze risico's op de betrokkenen en de gemeente ingeschat. Daarnaast worden maatregelen die de eigenaar van de verwerking kan treffen om de risico's tot een acceptabel niveau terug te brengen, beschreven. Hierbij wordt rekening gehouden met de haalbaarheid en maakbaarheid van deze maatregelen binnen de context van de gemeentelijke organisatie. De eventuele acceptatie van risico's of restrisico's is de verantwoordelijkheid van de eigenaar van de verwerking.

Voor elk van de thema's zijn risico's geïnventariseerd die voor het onderhavige onderwerp relevant kunnen zijn voor de gegevensbescherming binnen de gemeentelijke organisatie. De belangrijkste risico's zijn benoemd en geclassificeerd volgens de onderstaande tabel.

Figuur 1

		Impact →		
		Laag	Midden	Hoog
↑ Kans	Hoog			
	Midden			
	Laag			

2. Managementsamenvatting

Wat zijn de belangrijkste (M-H) risico's die in de analyse zijn geconstateerd? Welke maatregelen zijn hierbij van toepassing?

Beginsel	Risico	Classificatie (L-M-H)	Maatregelen
Governance	Geen periodieke controle op verwerkersovereenkomsten met leveranciers van PerfectView, ViaDesk en Ibabs.	M	Beleg (functionele) verantwoordelijkheid voor beheer van de verwerkersovereenkomst en controle van de afspraken met de leveranciers van PerfectView, ViaDesk en Ibabs.
Governance	Het HEIT-proces is niet opgenomen in het register van verwerkingsactiviteiten.	M	Voeg het HEIT-proces toe aan het register van verwerkingsactiviteiten. Win hiervoor advies in bij een privacy officer van BSD.
Governance	Verwerkersovereenkomst met PerfectView ontbreekt.	<u>H</u>	Treed in gesprek met PerfectView over de ontbrekende verwerkersovereenkomst en zorg dat deze zo snel mogelijk wordt gesloten.
Grondslag en doelbinding	Er is geen wettelijke grondslag voor gegevensverwerking door het HEIT	M	Rond het HEIT convenant en bijbehorend privacy protocol af. Zoek uit of de doelstellingen van het HEIT en het RIEC verenigbaar zijn.
Datamini-malisatie	Constateringen kunnen herleidbaar zijn naar personen	L	Overweeg om (bepaalde) constateringen die herleidbaar zijn naar een persoon niet te registreren, maar (alleen) mondeling te bespreken tijdens de debriefing.
Opslag	Gegevens worden op veel plekken opgeslagen	M	Herontwerp de informatievoorziening van dit proces met als uitgangspunt dat gegevens niet op onnodige locaties worden opgeslagen.
Opslag	Handmatige verwijdering	<u>M</u>	Overweeg om over te gaan tot automatisering van dit proces.
Bescherming	Het is onduidelijk of er wordt gemonitord op de logging in systemen	<u>M</u>	Zoek uit hoe de logging en monitoring (binnen de gemeente) is geregeld en of dit voldoende waarborging biedt tegen ongeoorloofde en onjuiste activiteiten door medewerkers.

Trans- parantie	Geen informatie over gegevensverwerking door HEIT	M	Pas de informatievoorziening aan de betrokkenen aan.
--------------------	---	---	---

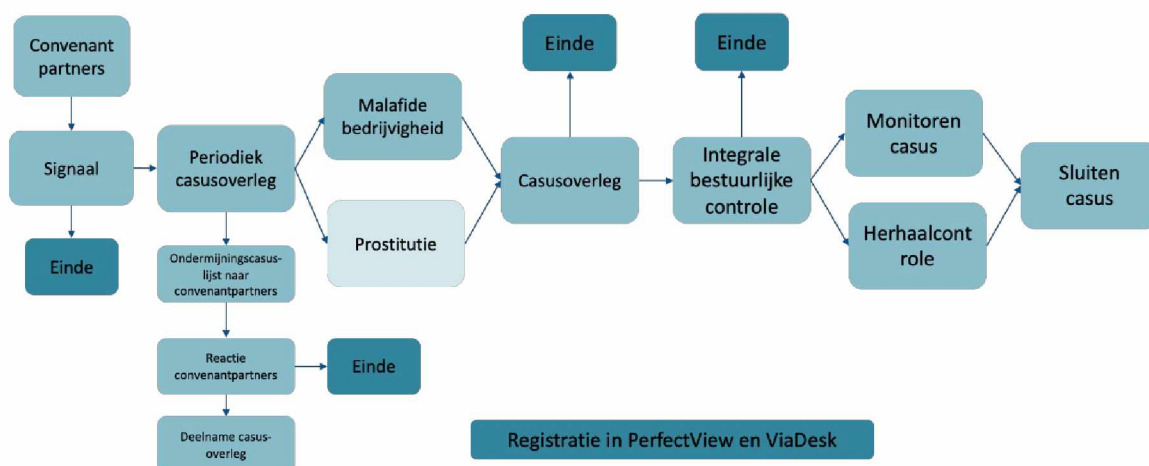
3. Beschrijving Verwerking

Dit hoofdstuk beschrijft het onderhavige proces en de verwerkingen van persoonsgegevens. De beschrijving van het proces en het inventariseren van de verwerkingen van persoonsgegevens zijn onderdeel geweest van de DPIA-workshop.

Systematische beschrijving van het proces

In het regionale interventieteam (HEIT) werken verschillende organisaties samen om malafide bedrijvigheid aan te pakken. In het HEIT werken gemeenten, politie, Belastingdienst, Douane, Inspectie SZW, de Nederlandse Voedsel- en Warenautoriteit (NVWA), het UWV en drie omgevingsdiensten (Haaglanden (ODH), Midden Holland (ODMH) en West Holland (oDWH)) samen. Het team valt onder de bestuurlijke verantwoordelijkheid van de burgemeester van Den Haag.

Het HEIT voert bestuurlijke controles (interventies) uit bij malafide ondernemingen op basis van meldingen en signalen van bewoners en organisaties over misstanden.



Signaal

Een signaal is (meestal) afkomstig van de politie of de gemeente en wordt vaak waargenomen tijdens reguliere werkzaamheden. Een signaal kan echter ook worden ingebracht door iedere convenantpartner. Een signaal wordt (veelal) mondeling ingebracht. Dit kan echter ook telefonisch of via e-mail (Outlook) plaatsvinden. Elk signaal dat niet monodisciplinair kan worden behandeld, wordt ingebracht bij het HEIT voor een integrale interventie. Voorbeelden hiervan zijn:

- belasting- en uitkeringsfraude
- zwartwerken
- illegale tewerkstelling
- illegaal gokken
- onderbetaling en uitbuiting
- overtreding van vergunningvoorwaarden

De beleidsmedewerker van de gemeente vult het signaal aan met gegevens uit het KvK. Uit het KvK worden de adresgegevens (van de onderneming), de naam en het BSN van de eigenaar gehaald en in PerfectView geregistreerd.

Een signaal (indien afkomstig van de politie) wordt soms ook door de politie veredeld (verrijkt) met politiegegevens uit politiesystemen, zoals Basisvoorziening Handhaving (BVH).

Periodiek casusoverleg

Er vindt periodiek overleg plaats tussen de gemeente (beleidsmedewerker afdeling OOV) en het basisteam van de politie. Dit periodieke overleg vindt één á tweemaal per twee maanden plaats. In dit periodieke casusoverleg worden alle door de gemeente ontvangen signalen en signalen van de politie besproken. Naar aanleiding van dit overleg wordt de naam en het adres van de onderneming waarover het signaal gaat, de naam eigenaar, het BSN van de eigenaar en de reden waarom het een signaal is op een ondermijningscasuslijst geplaatst. De ondermijningscasuslijst wordt opgesteld in Excel en opgeslagen op de g:schijf. Daarna wordt de ondermijningscasuslijst opgeslagen in ViaDesk. Een andere uitkomst is dat het signaal niet wordt behandeld door het HEIT. Het proces eindigt.

De Casuslijst wordt via ViaDesk gedeeld met de ketenpartners. De ketenpartners kunnen op het signaal reageren met 'ja' of 'nee'. Dit refereert aan de wens om wel/niet deel te nemen aan de interventie. Er wordt gesproken over een integrale interventie als er minimaal twee ketenpartners aansluiten bij de controle. Als er minder ketenpartners willen aansluiten, dan gaat het signaal terug naar het periodieke casusoverleg tussen het HEIT en de gemeente en de basisteams. De casus wordt afgesloten als er geen aanvullende informatie wordt aangeleverd vanuit de basisteams.

Casusoverleg

De deelnemende ketenpartners komen samen in een casusoverleg. Tijdens het casusoverleg wordt operationele informatie besproken. Dit ziet op afspraken over hoe de interventie planning technisch zal verlopen. Tijdens het casusoverleg kan ook worden besloten dat er geen interventie plaatsvindt, bijvoorbeeld omdat een onderneming inmiddels faillissement heeft aangevraagd.

Op basis van het casusoverleg wordt er, twee weken voor de bestuurlijke controle, een briefingsdocument gemaakt. Dit document bevat alle relevante informatie voor de bestuurlijke controle. Er staat onder andere in: adres, signaal, vergunningen (uit Key2Vergunningen). Het briefingsdocument wordt via ViaDesk gedeeld met de ketenpartners. Deze informatie wordt tevens bewaard in een (fysieke) operationele map, samen met de vergunningen. Deze map gaat mee tijdens een controle. Er loopt momenteel een pilot met ibabs om dit proces te digitaliseren.

Controle

Tijdens een controle voert iedere ketenpartner zijn eigen publiekrechtelijke bevoegdheden uit. Indien men op een strafbaar feit stuit, dan kunnen de bevoegde opsporingsinstanties gebruik maken van daarvoor bestemde bevoegdheden (dit wordt de voortgezette toepassing van bevoegdheden genoemd). Immers, als een opsporingsambtenaar tijdens de rechtmatige uitoefening van een bepaalde aan hem toegekende bevoegdheid het redelijke vermoeden krijgt dat er ook een ander strafbaar feit wordt begaan, hij deze bevoegdheid tevens mag gebruiken voor het opsporen van dat andere strafbare feit (HR 02 december 1935, NJ 1936, 250).

Na de controle vindt een mondelinge debriefing plaats. Hierin wordt o.a. besproken hoe de controle is verlopen, welke constatering er zijn gedaan en of de deelnemers zich veilig voelden. Als de deelnemers overwegen om over te gaan tot acties (bijvoorbeeld boetes), dan worden deze toegevoegd aan de casus in PerfectView.

Monitoren en herhaalcontrole

Er gaat meestal een flinke periode overheen voordat alle ketenpartners de acties hebben uitgezet. De casus wordt derhalve voor lange periode gemonitord. Tijdens het periodieke casusoverleg worden de resultaten van controles gemonitord. Tijdens dit overleg wordt bepaald of er aanleiding is om een hercontrole uit te voeren. Tijdens een controle kunnen tevens nieuwe signalen aan de orde komen die relevant zijn voor andere ketenpartners die niet hebben meegedaan aan de interventie, maar eventueel wel willen meedoen aan een hercontrole.

Shuiten casus

Een casus wordt gesloten indien de onderneming zich uitschrijft en plaatsmaakt voor een nieuwe onderneming met een andere dienstverlening. Een casus wordt tevens gesloten indien er gedurende een lange periode geen nieuwe signalen aan de orde zijn gekomen. Deze beslissing wordt tijdens het periodieke casusoverleg gemaakt.

Systematische beschrijving van de verwerking

Onderstaand een schematische weergave van de persoonsgegevens. Wat ontvang je (wat krijg je), wat verwerk je (wat doe je ermee) en wat verstrek je (wat geef je door).

Wat krijg je	Van wie	Hoe
<i>Signaal over onderneming (bestaat uit adresgegevens van onderneming)</i>	<i>Ketenpartner</i>	<i>Mondeling, telefoon of Outlook</i>
<i>Inkomsten, vermogen, en rekeningnummers en gegevens die bij controles verkregen worden</i>	<i>Belastingdienst</i>	<i>Nog n.v.t., mogelijk in de toekomst.</i>
<i>Constateringen tijdens een interventie: (zoals kasverschil, in beslag genomen goederen, illegale aanbouwing, muizenkeutels, illegale tewerkstelling. Heel soms worden namen van werknemers teruggekoppeld als een constatering hen betreft.</i>	<i>Ondernemer/onderneming</i>	<i>PerfectView</i>

Wat doe je ermee	Middelen
<i>Verrijking signaal door gemeente in HEIT met Naam- en achternaam, geboorteplaats, titulatuur, aliasen, BSN, adresgegevens van de eigenaar.</i>	<i>KvK</i>
<i>Verrijking signaal door gemeente in HEIT met vergunningen (inclusief handhavingsgeschiedenis) van de onderneming en namen van leidinggevendenden op de vergunningen.</i>	<i>Key2Vergunningen</i>
<i>Verrijking signaal door politie in HEIT met politiegegevens van eigenaar en/of leidinggevendenden (personen op de vergunning), zoals dat de eigenaar al eens veroordeeld is voor b.v. heling of hemel indien relevant voor de casus. (Politiegegevens)</i>	<i>Check in BVH</i>
<i>Ondermijningscasuslijst (signaal verrijkt met gegevens uit KvK)</i>	<i>Opgesteld in Excel, Excel wordt opgeslagen op G: schijf en in ViaDesk geupload</i>
<i>Briefingsdocument (met adres, signaal, en vergunningen)</i>	<i>Opgesteld in PerfectView en in ViaDesk geupload</i>
<i>Actiemap met briefingsdocument</i>	<i>Fysieke map (pilot: Ibabs)</i>
<i>Debriefingsdocument na een interventie (met constatering en acties)</i>	<i>Opgesteld in PerfectView en in ViaDesk geupload</i>

Wat geef je door	Aan wie	Hoe
Ondermijningscasuslijst	Ketenpartners	Viadesk
Briefingsdocument	Ketenpartners	ViaDesk
Debriefingsdocument	Ketenpartners	ViaDesk

Persoonsgegevens

Wij hanteren de classificatie zoals weergegeven in onderstaande figuur om te bepalen welke persoonsgegevens worden verwerkt. Er wordt onderscheid gemaakt tussen weinig gevoelige gegevens (algemene persoonsgegevens), door de aard of context extra gevoelige gegevens (gevoelige persoonsgegevens) en zeer gevoelige gegevens die wettelijk extra beschermd zijn (bijzondere persoonsgegevens). Al naar gelang de situatie kunnen gegevens in verschillende categorie worden geplaatst.



Binnen de scope van deze DPIA worden de volgende categorieën van persoonsgegevens verwerkt:

	Algemeen	Gevoelig	Bijzonder
Gestructureerd	• NAW-gegevens • Geboortedatum • Adresgegevens • Vergunningen	• BSN • Financiële gegevens (over inkomsten, vermogen en rekeningnummers)	• Antecedenten (politiegegevens)
Ongestructureerd		• Constateringen en waarnemingen	

4. Analyse privacy consequenties

Inleiding

Dit hoofdstuk beschrijft de resultaten uit de uitgevoerde DPIA per thema. Voor ieder thema geven we een korte toelichting en beschrijven wij de risico's, de impact van de risico's op de betrokkenen en de gemeente en de maatregelen die de gemeente kan treffen om de risico's tot een acceptabel niveau terug te brengen.

4.1 Governance

Inleiding

Is helder wie de verantwoordelijke en de verwerker zijn en hoe wordt toegezien op een adequate bescherming van persoonsgegevens? Is er beleid gemaakt ten aanzien van privacy en wordt er intern gecontroleerd op naleving van dit beleid? Is duidelijk wie binnen de organisatie verantwoordelijk is voor privacy?

Feiten & analyse

Het HEIT bestaat uit Gemeenten, Politie, Belastingdienst, Inspectie SZW, UWV, Douane, Nederlandse Voedsel- en Warenautoriteit en Omgevingsdiensten. De opdrachtgever van het HEIT is de Regiegroep. De regiegroep bestaat uit een afgevaardigde van elke partner. Het voorzitterschap van de regiegroep berust bij de Bestuursdienst van de gemeente Den Haag onder voorzitterschap van de coördinator HEIT.

Periodiek en/of jaarlijks wordt in de Regiegroep vastgesteld wat de capaciteit is die de participerende organisaties ter beschikking stellen. Hier wordt tevens bepaald op welke branches wordt ingezet.

Vanuit de gemeente Den Haag en de politie eenheid Den Haag wordt een vaste groep medewerkers beschikbaar gesteld voor het HEIT. Vanuit de politie ligt de taakstelling op de uitvoering van de bestuurlijke controles, en de analysefunctie vanuit Intelligence als voorbereiding op de bestuurlijke controles. De werkruimte van het HEIT wordt beschikbaar gesteld door de gemeente Den Haag.

De samenwerking tussen de partners in het HEIT is ontstaan in 2007. De informatie-uitwisseling van de partners ten behoeve van de werkzaamheden vindt plaats volgens de afspraken in het RIEC-LIEC convenant en bijbehorend Privacyprotocol RIEC'S-LIEC. In deze documenten staat nauwkeurig beschreven op welke wijze convenantpartners in het samenwerkingsverband persoonsgegevens delen. Daarnaast worden de verwerkingsverantwoordelijke(n) verplicht op transparante wijze hun verantwoordelijkheden voor de nakoming van de AVG vast te stellen, zoals de uitoefening van de rechten van betrokkenen. Er is tevens een meldplicht datalekken opgenomen waarin duidelijk staat beschreven op welke wijze de verwerkingsverantwoordelijke(n) dienen om te gaan met een (mogelijk) datalek.

Het wetsvoorstel: ‘Wet gegevensuitwisseling door samenwerkingsverbanden (Wgs)’ versterkt de juridische basis onder de systematische uitwisseling van informatie door samenwerkingsverbanden en het gezamenlijk verwerken daarvan. In de Wgs wordt het RIEC aangewezen als samenwerkingsverband in dit kader. Tijdens de plenaire sessie heeft de HEIT-coördinator aangegeven dat samenwerking in het HEIT onder het RIEC’s-LIEC convenant hierdoor onmogelijk wordt gemaakt. De HEIT-coördinator heeft benadrukt dat de doelstellingen weliswaar verenigbaar zijn, maar dat dit niet betekent dat het HEIT onder RIEC kan opereren. Dit is uitgezocht door Juridische Zaken. De samenwerking zal daarom, vanaf de inwerkingtreding van de Wgs, worden voortgezet onder het (hernieuwde) HEIT-convenant en bijhorend privacy protocol. Deze worden opgesteld en waren ten tijde van de plenaire bijeenkomst nog niet afgerond.

De partners zijn eenieder zelfstandig verwerkingsverantwoordelijk voor de verwerking van persoonsgegevens waar het de uitoefening van hun eigen (publiekrechtelijke) taken binnen de samenwerking betreft.

De partners in het HEIT maken gebruik van een drietal systemen: PerfectView, ViaDesk en Ibabs (pilotfase). Er zijn volgens de aanwezigen bij de plenaire sessie afspraken gemaakt in verwerkersovereenkomsten met de leveranciers van de systemen ViaDesk (Fellow Digital) en Ibabs (Ibabs). Er worden in de verwerkersovereenkomsten tevens eisen gesteld aan de (informatie-) systemen op grond van de BIO-normering. Functioneel beheer treedt hierover in gesprek met de leverancier(s). Er vindt nog geen periodieke audit plaats op de gesloten verwerkersovereenkomst ter controle van de daarin gemaakte afspraken. Momenteel wordt er, bij veranderingen in de organisatie, sporadisch beoordeeld of deze veranderingen impact hebben op de gesloten verwerkersovereenkomsten. Het is ons na de plenaire bijeenkomst ter oren gekomen dat er momenteel geen verwerkersovereenkomst aanwezig is tussen de gemeente Den Haag en de leverancier van PerfectView.

De gemeente houdt een register van verwerkingsactiviteiten bij (in iNavigator) waarin alle gemeentelijke processen zijn opgenomen. Het HEIT-proces maakt (nog) geen onderdeel uit van het register.

Risico's en maatregelen

Op basis van de analyse op het aspect *governance* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: verwerkersovereenkomst met PerfectView ontbreekt

Met een verwerkersovereenkomst sluit de verwerkingsverantwoordelijke uit dat de verwerker de persoonsgegevens voor eigen doelen mag verwerken. Als verwerkingsverantwoordelijke mag je alleen verwerkers inschakelen die voldoende garanties bieden dat zij aan de wettelijke vereisten voldoen. Je moet er bijvoorbeeld voor zorgen dat de verwerking voldoende veiligheidswaarborgen heeft. Het afsluiten van een verwerkersovereenkomst is een verplichting voor zowel de verwerkingsverantwoordelijke en de verwerker.

Maatregel:

Treed in gesprek met PerfectView over de ontbrekende verwerkersovereenkomst en zorg dat deze zo snel mogelijk wordt gesloten.

Risico: Geen periodieke controle op verwerkersovereenkomsten met leveranciers van PerfectView, ViaDesk en Ibabs.

De gemeente Den Haag mag alleen verwerkers inschakelen wanneer door de verwerker voldoende garanties worden geboden op het gebied van deskundigheid, betrouwbaarheid en passende (beveiligings-)maatregelen. Deze garanties worden vastgelegd in een verwerkersovereenkomst. De gemeente Den Haag heeft op dit moment het beheer van de afspraken in de verwerkersovereenkomst nog niet belegd. Concreet betekent dit dat een verwerkersovereenkomst niet standaard geüpdate wordt als er zich veranderingen in het proces voordoen en dat er geen periodieke controles worden uitgevoerd om te checken of de verwerker de afspraken uit de verwerkersovereenkomst naleeft. Hierdoor is onvoldoende zeker of de afspraken in de verwerkersovereenkomst worden nageleefd en ipso facto of voldoende beschermingsmaatregelen zijn getroffen.

Maatregel:

Beleg (functionele) verantwoordelijkheid voor beheer van de verwerkersovereenkomst en controle van de afspraken met de leveranciers van PerfectView, ViaDesk en Ibabs. Zorg dat periodiek getoetst wordt of de leveranciers de gemaakte afspraken nakomen (o.a. een check of certificering nog actueel is).

Risico: Het HEIT-proces is niet opgenomen in het register van verwerkingsactiviteiten.

De gemeente Den Haag heeft het HEIT-proces niet vastgelegd in het register van verwerkingsactiviteiten. De gemeente kan daardoor niet aantoonbaar voldoen aan de verantwoordingsplicht. Doordat het proces niet is vastgelegd in het register heeft de gemeente minder inzicht en grip op haar processen en kan niet (aantoonbaar) worden voldaan aan de beginselen uit de AVG.

Maatregel:

Voeg het HEIT-proces toe aan het register van verwerkingsactiviteiten (het verstrekken en ontvangen van persoonsgegevens aan/van deelnemers aan het HEIT). Win hiervoor advies in bij een privacy officer.

4.2 Grondslag & Doelbinding

Inleiding

Het moet helder zijn wat het doel van de gegevensverzameling is, op het moment dat de gemeente deze verzamelt. Het doel moet ook in overeenstemming zijn met de normale werkzaamheden van de gemeente en onderbouwd zijn door één of meer wettelijke grondslagen.¹

Feiten & analyse

Het doel van het HEIT wordt (in de toekomst) vastgelegd in het convenant en het privacy protocol. De samenwerking tussen de convenantpartners binnen het HEIT heeft als doel gezamenlijk invulling te geven aan het voorkomen en terugdringen van malafide bedrijvigheid in de vorm van belasting- en premiefraude, fraude met vergunningen, uitkeringsfraude, illegale tewerkstelling, uitbuiting en de daarmee samenhangende misstanden en criminele activiteiten. Daarnaast willen alle gemeenten in de Eenheid Den Haag eerlijk ondernemerschap stimuleren door oneerlijke concurrentie tegen te gaan. Ook beoogt het HEIT mee te werken aan het verbeteren van de leefbaarheid en veiligheid in de stad door ondermijnende criminaliteit tegen te gaan.

De verschillende partners in het HEIT verwerken persoonsgegevens op grond van hun eigen publiekrechtelijke wettelijke taken en bevoegdheden. De gemeente Den Haag heeft uiteenlopende taken en bevoegdheden die van belang zijn voor de doelstellingen van de samenwerking in het HEIT. Deze taken en bevoegdheden vinden hun grondslag in verschillende sectorale wetten, waaronder:

- Wet basisregistratie personen
- Besluit basisregistratie personen
- Artikel 13b Opiumwet
- Artikel 3, 38 en 41 Drank- en horecawet
- Artikel 34 Wet op de kansspelen
- Artikel 437 lid 2 Wetboek van Strafrecht
- Artikel 172 en 172a Gemeentewet
- Artikel 149 jo. Artikel 151a Gemeentewet
- Artikel 17 Woningwet
- Artikel 92 Woningwet jo. Wet algemene bepalingen omgevingsrecht
- Artikel 2 jo. Artikel 8 jo. Artikel 9 jo. Artikel 10 Huisvestingswet

Om de doeleinden te kunnen bereiken is het noodzakelijk dat informatie tussen de convenantpartners wordt uitgewisseld voor zover partners een potentiële betrokkenheid hebben bij de casus.

¹ De wettelijke grondslag is de rechtvaardiging om persoonsgegevens te mogen verwerken, zoals bedoeld in artikel 6 lid 1 e.v. van de Algemene Verordening Gegevensbescherming. De wettelijke grondslagen uit dit artikel zijn; toestemming, ter uitvoering van een overeenkomst, wettelijke plicht, vitale belang, taak van algemeen belang en het gerechtvaardigd belang.

De grondslag voor de verwerking van gegevens door de gemeente (een van de verwerkingsverantwoordelijken van het HEIT) wordt gevonden in artikel 6, eerste lid, onder e, van de AVG. De gegevensverwerking is noodzakelijk voor de vervulling van een taak van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze bevoegdheden worden gevonden in (sectorale) wetten zoals hierboven beschreven.

Het HEIT verwerkt gegevens in samenwerkingsverband. Er bestaat formeel (nog) geen wettelijke grondslag op basis waarvan gegevens kunnen worden verwerkt door het samenwerkingsverband. Samenwerkingsverbanden hebben immers geen wettelijke status. De wettelijke grondslag voor gegevensverwerking binnen samenwerkingsverbanden wordt in de toekomst gecreëerd in de Wgs.²

De gemeente Den Haag heeft advies ingewonnen bij het LIEC. Het LIEC heeft de gemeente geadviseerd om, na inwerkingtreding vna de Wgs, (wederom) onder het HEIT convenant en bijbehorend privacy protocol te opereren. Uit dit advies blijkt tevens dat het HEIT niet, via een juridische constructie, onder de Wgs kan vallen en daardoor gebruik kan maken van de juridische grondslag die daarin wordt gecreëerd voor het RIEC. Dit advies is niet met VKA gedeeld en kan daarom niet worden beoordeeld.

Rechtmatigheid van de verwerking

Op basis van de analyse wordt de gegevensverwerking binnen het HEIT als niet rechtmatig beoordeeld door het ontbreken van een juridische basis hiervoor.

Op basis van de analyse wordt de gegevensverwerking door de gemeente Den Haag als deelnemer aan het HEIT als rechtmatig beoordeeld. Hieronder valt bijvoorbeeld het verstrekken en ontvangen van gegevens aan/van deelnemers aan het HEIT.

Risico's en maatregelen

Op basis van de analyse op het aspect *grondslag en doelbinding* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Er is geen wettelijke grondslag voor gegevensuitwisseling binnen het HEIT

Er is geen juridische grondslag voor gegevensverwerking binnen het HEIT als samenwerkingsverband.

Dit risico geldt voor de gegevensverwerking binnen alle samenwerkingsverbanden waarin publieke partijen gezamenlijk gegevens verwerken. De Wgs beoogt een algemene juridische grondslag te geven voor gegevensverwerking door overheidsorganisaties voor het bestrijden van, onder andere, ernstige vormen van criminaliteit en ondermijning. Het HEIT wordt in de

² De Wgs is op 17 december jl. goedgekeurd. De commissie voor Justitie en Veiligheid gaat voorlichting aan de Afdeling advisering van de Raad van State en advies aan de Autoriteit Persoonsgegevens vragen wegens amendering van dit wetsvoorstel. Daarna zal dit wetsvoorstel worden voorgelegd aan de Eerste Kamer. Het is op dit moment onduidelijk binnen welke termijn dit verwacht mag worden. Het is onduidelijk wat de precieze impact van de Wgs op het HEIT is, omdat het huidige wetsvoorstel nog aan amendering onderhevig is.

Wgs niet aangewezen als samenwerkingsverband in deze context (anders dan bijvoorbeeld het RIEC).

Maatregel:

Rond het HEIT convenant en bijbehorend privacy protocol af. Onderzoek of blijvende samenwerking onder het RIEC convenant toch mogelijk is na inwerkingtreding van de Wgs. Onderzoek daarnaast hoe andere gemeente(n) dit organiseren.

4.3 Juistheid

Inleiding

Is de kwaliteit van de gegevens gewaarborgd (actueel, juist en volledig)? Hoe worden gegevens over de personen verwerkt (handmatig of automatisch?) Vindt er controle op de datakwaliteit plaats en zo ja wanneer?

Feiten & Analyse

Een signaal, afkomstig van één van de convenantpartners, is een (potentiele) misstand in de bedrijfsvoering van een onderneming die aanleiding geeft tot het uitvoeren van een integrale bestuurlijke controle.

Bij een signaal worden de naam en/of de adresgegevens van de onderneming genoemd. Het adres wordt gecontroleerd in het KvK. Uit het KvK worden de volgende gegevens gehaald: de naam van de onderneming, adres, NAW-gegevens van de eigenaar en het KvK-nummer. In sommige gevallen staan hier tevens de door de gemeente afgegeven vergunningen bij. De door de gemeente afgegeven vergunningen worden gecontroleerd in Key2Vergunningen. De juistheid van de gegevens uit de bronsystemen staat vast.

Dezelfde bronnen worden opnieuw geraadpleegd voordat de interventie plaatsvindt. Op deze manier wordt voorkomen dat een onderneming tussentijds een nieuwe eigenaar heeft gekregen zonder verband met de op de casus van toepassing zijnde signalen of dat de onderneming is uitgeschreven (uit het KvK). Het adres van de onderneming is hiervoor steeds leidend. Indien één van deze feiten aan het licht komen voor een interventie, wordt het signaal alsnog afgesloten. Dit wordt gedeeld met de deelnemende partners in ViaDesk.

Risico's en maatregelen

Er zijn geen risico's ten aanzien van dit thema gesignaleerd.

4.4 Dataminimalisatie

Inleiding

Kan er met bijvoorbeeld minder persoonsgegevens, of op een andere manier worden gewerkt zonder de functionaliteit van het proces en systeem aan te tasten? Zijn er rapportages waarin tot individuen herleidbare informatie is opgenomen? Worden alleen die gegevens vastgelegd die absoluut noodzakelijk zijn voor het doel van de verwerking? Welke zijn dat niet?

Feiten & Analyse

Een signaal bestaat uit adresgegevens van een (potentieel) malafide onderneming. De adresgegevens worden als signaal ingediend bij het HEIT.

Naar aanleiding van het periodieke casusoverleg tussen de gemeente en het basisteam van de politie wordt een ondermijningscasuslijst opgesteld in Excel. Hierin staat waar het signaal over gaat, de naam van de eigenaar, het BSN van de eigenaar en de reden waarom het een signaal is. De ondermijningscasuslijst wordt opgeslagen op de g:schijf en in ViaDesk. De casuslijst wordt via ViaDesk gedeeld met de ketenpartners. De gegevens op deze lijst zijn noodzakelijk voor de partners om te bepalen of zij willen deelnemen aan de interventie en mogelijk bevoegdheden kunnen inzetten tegen de (potentieel) malafide onderneming.

Er wordt geen gebruik gemaakt van een open tekstveld in de ondermijningscasuslijst waar de HEIT-medewerkers zijn of haar eigen interpretatie van het signaal kan opnemen.

De convenantpartners reageren alleen met ja/nee op het signaal. Dit is afhankelijk van of zij willen deelnemen aan de interventie. Er worden geen (overige) gegevens uitgewisseld. Dit wordt beperkt tot het absolute minimum.

Tijdens de debriefing worden o.a. de constatering van de deelnemers besproken. Deze blijven zoveel mogelijk algemeen. Constatering zijn bijvoorbeeld: kasverschil, in beslag genomen goederen, illegale aanbouwing, muizenkeutels, illegale tewerkstelling. In sommige gevallen zijn deze constatering echter herleidbaar naar personen. Dit is bijvoorbeeld het geval als er wordt geconstateerd dat er sprake is van illegale tewerkstelling en duidelijk is welke persoon dit betreft.

Risico's en maatregelen

Op basis van de analyse op het aspect *dataminimalisatie* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Aandachtspunt: constatering kunnen herleidbaar zijn naar personen

In sommige gevallen zijn constatering herleidbaar naar een persoon. Dit is bijvoorbeeld het geval als er constatering met betrekking tot illegale tewerkstelling of arbeidsuitbuiting worden gedeeld. Dit is noodzakelijk voor sommige partijen, maar mogelijk niet relevant voor alle deelnemers. Hierdoor ontstaat het risico dat er meer gegevens worden verwerkt dan noodzakelijk is voor het (primaire) doel.

Aanbeveling:

Overweeg om (bepaalde) constatering(en) die herleidbaar zijn naar een persoon niet te registreren, maar (alleen) mondeling te bespreken tijdens de debriefing indien dit noodzakelijk is. Hierdoor voorkom je dat er meer persoonsgegevens worden verwerkt dan noodzakelijk is voor het doel van de interventie.

4.5 Opslag

Inleiding

Welke bewaartermijnen zijn van toepassing? Hoe worden persoonsgegevens bewaard en worden persoonsgegevens die niet langer nodig zijn daadwerkelijk verwijderd? Worden op de middelen (desktop, pc, mobiele telefoon) zelf gegevens opgeslagen?

Feiten & Analyse

Persoonsgegevens worden binnen het HEIT op zes verschillende locaties opgeslagen, te weten in PerfectView, ViaDesk, Ibabs, g:schijf, Outlook en in fysieke mappen. De gegevens in PerfectView en ViaDesk worden opgeslagen in locaties binnen de Europese Unie. Er vindt momenteel een pilot met Ibabs plaats.

De gemeente moet voldoen aan de bewaartermijnen zoals vastgelegd in de Selectielijst van de VNG. Hierin zijn de bewaartermijnen van archiefbescheiden van gemeentelijke en intergemeentelijke organen vastgelegd. Een samenwerkingsverband zoals het HEIT staat niet tussen de processen op de Selectielijst van de VNG en zal derhalve zelfstandig een bewaartermijn moeten vastleggen.

Er wordt een bewaartermijn van twee jaar gehanteerd voor persoonsgegevens die in het kader van een casus worden verwerkt. De bewaartermijn is vastgelegd in een daarvoor bestemd beleidsdocument. De bewaartermijn start na het afsluiten van een casus. Een casus wordt afgesloten als er gedurende langere periode geen activiteit meer plaatsvindt. Dit wordt (periodiek) gemonitord tijdens het periodieke casusoverleg. Een casus kan tevens worden afgesloten wanneer een onderneming wordt uitgeschreven uit het KvK. Vernietiging van de gegevens uit PerfectView, ViaDesk en Ibabs vindt handmatig plaats.

HEIT-medewerkers schonen periodiek de mappen op de g:schijf en in Outlook op. De bewaartermijn wordt echter niet consistent toegepast. Op dit moment vindt opschoning (van Outlook) met name plaats wanneer de e-mail dreigt vol te lopen en het overzicht kwijt dreigt te raken. Andere medewerkers vinden het daarentegen prettig om (afgevoerde) signalen langer te bewaren, mochten deze op een later moment nog relevant worden. Er zijn nog geen richtlijnen voor het verwijderen van gegevens van netwerkschijven of uit Outlook.

Er wordt (nog) geen bewaartermijn gehanteerd voor de fysieke mappen waarin alle relevante documenten, zoals vergunningen en gegevens uit het KvK, voor een casus worden bewaard. De fysieke mappen worden na afloop van de bewaartermijn gearchiveerd en uiteindelijk verwijderd.

Er worden, ten behoeve van de werkzaamheden, documenten geprint en gescand met persoonsgegevens daarin. Het is onduidelijk of het apparaat een historie heeft en, zo ja, of deze (tijdig) wordt verwijderd. Tijdens de plenaire bijeenkomst is afgesproken dat de ISO van BSD gaat uitzoeken of er gemeentebreed beleid is vastgesteld hierover, omdat het over een generieke voorziening gaat.

Risico's en maatregelen

Ten aanzien van het beginsel *opslag* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Gegevens worden op veel plekken opgeslagen

Momenteel worden persoonsgegevens op zes verschillende plekken opgeslagen. Hierdoor ontstaan onnodige kopieën van gegevens en is het lastig om deze te beheren en tijdig te verwijderen. Daardoor worden gegevens, mogelijk, te lang bewaard waardoor niet wordt voldaan aan de bewaartermijn.

Herontwerp de informatievoorziening van dit proces met als uitgangspunt dat gegevens niet op onnodige locaties worden opgeslagen. Zorg dat er kritisch wordt gekeken naar de verschillende opslaglocaties. Zorg er voor dat de gegevens direct na verwerking worden verwijderd op alle plaatsen die niet behoren tot de informatievoorziening van dit proces (bijvoorbeeld: outlook, g:schijf).

Risico: Gegevens worden handmatig verwijderd

Er vindt op dit moment handmatige verwijdering van gegevens plaats. Zonder goed ingericht beheer hierop, is dit erg foutgevoelig waardoor gegevens mogelijk te lang worden bewaard (op verschillende plekken).

Maatregel

Overweeg om over te gaan tot automatisering van dit proces. Zorg er in de tussentijd voor dat bewaartermijnen goed beheerd worden, zodat gegevens voor het verlopen van de bewaartermijn verwijderd worden.

4.6 Bescherming

Inleiding

Persoonsgegevens moeten technisch en organisatorisch adequaat worden beschermd. Op welke wijze is de toegang tot gegevens afgeschermd? Is dit voldoende veilig in verhouding tot de gevoeligheid van de gegevens die verwerkt worden? Welke externe partijen hebben toegang tot de gegevens (leveranciers, samenwerkingspartners, dienstverleners) en hoe is de beveiliging daar geregeld?

Feiten & Analyse

Het HEIT team heeft verschillende rollen ingericht met bijbehorende autorisaties in de verschillende applicaties en de G:schijf. De verschillende rollen betreffen op dit moment: HEIT-medewerkers (14), actieleiders (2), beleidsmedewerkers (3) en infomedewerkers (2). De g:schijf is toegankelijk voor alle HEIT-medewerkers voor de uitvoering van dagelijkse werkzaamheden. Ibabs is toegankelijk voor de actieleiders, beleidsmedewerkers en infomedewerkers. PerfectView is beperkt toegankelijk voor tien medewerkers van de gemeente en politie. In ViaDesk wordt gewerkt met een mappensysteem op ketenpartnerniveau, waarbij elke ketenpartner alleen toegang heeft tot informatie in de eigen map.

De leveranciers van de applicaties zijn allemaal (minimaal) ISO 27001 gecertificeerd. Er wordt daarom in deze DPIA ervan uitgegaan dat de drie applicaties passend beveiligd zijn. Als kanttekening is opgemerkt door de security officer dat toezicht op de pentest(en) op applicaties en periodieke controles op ISO certificaten van leveranciers (nog) ontbreekt.

Binnen deze applicaties worden acties gelogd, echter is voor de aanwezigen bij de DPIA sessie niet duidelijk of er ook gemonitord wordt op de logging.

Fysieke documenten worden bewaard in een afgesloten kast in een afgesloten kamer op een afgesloten gang. Deze gang is alleen op uitnodiging toegankelijk voor buitenstaanders. Daarnaast zijn er veel informele regels afgesproken op het vlak van beveiliging. Zo wordt er een clean desk policy gehanteerd, mogen printjes de gang niet uit en wordt er zelfs afgestemd wanneer glazenwassers komen, zodat gegevens uit het zicht gehaald kunnen worden en geen “imposters” binnen komen op een ander moment.

Daarnaast is er een datalekprotocol voorhanden, welke bekend is gemaakt binnen de gemeente. Dit protocol is bij de medewerkers bekend en wordt gevolgd. Daarnaast is er een procedure ‘Meld een beveiligingsincident’. Het is onbekend of de medewerkers van het HEIT met dit document bekend zijn.

Medewerkers van het HEIT zijn in het bezit van een screening door de politie. Integriteit is tevens een belangrijk thema tijdens sollicitatiegesprekken. Het schoonmakend personeel is in het bezit van een VOG.

Risico's en maatregelen

Ten aanzien van het beginsel *bescherming* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: het is onduidelijk of er wordt gemonitord op de logging in systemen

Het is onduidelijk of er monitoring op logging plaatsvindt. Logging zorgt voor registratie van gebruikersactiviteiten. Door middel van logging kan je dus handelingen in bepaalde dossiers achterhalen. Op deze manier kan worden uitgesloten dat iemand, zonder aanleiding, bepaalde informatie heeft geraadpleegd. Monitoring is gericht op het onderkennen van eventuele afwijkingen op 'normaal' gedrag. Alleen logging is onvoldoende om afwijkingen in gebruikersactiviteiten te achterhalen.

Maatregel:

Zoek uit hoe de logging en monitoring (binnen de gemeente) is geregeld en of dit voldoende waarborging biedt tegen ongeoorloofde en onjuiste activiteiten door medewerkers.

4.7 Transparantie

Inleiding

De gemeente is helder in de gegevens die zij verwerkt. De betrokkene moet goed kunnen begrijpen welke persoonsgegevens worden verwerkt (en waarom) en heeft het recht en de mogelijkheid om in te grijpen. De betrokkene heeft het recht op informatie, inzage, correctie en verwijdering.

Feiten & Analyse

Tijdens een interventie door het HEIT wordt de betrokkene geïnformeerd door middel van een daartoe bestemde flyer. Op de flyer staat duidelijk beschreven wat het doel van de interventie is en welke ketenpartners daaraan deelnemen. De flyer wordt uitgereikt door het aangewezen aanspreekpunt voor de betrokkene.

Het HEIT heeft een eigen website waarop informatie wordt gegeven over de doelstelling(en) van het HEIT. Op de website wordt geen informatie gegeven over gegevensverwerking door het HEIT of rechten van betrokkenen. Hiervoor wordt verwezen naar de privacyverklaring van de gemeente.

De gemeente heeft op haar website een privacyverklaring staan. Betrokkenen kunnen een verzoek indienen door een e-mail te sturen naar gegevensbescherming@denhaag.nl. Een verzoek kan ook via andere routes worden ingediend zoals een dienst specifiek e-mailadres of per post.

Het HEIT heeft nog geen ervaring met verzoeken van betrokkenen. Het HEIT heeft wel een mogelijkheid voor betrokkene(n) om klachten in te dienen. Klachten kunnen worden ingediend via een algemeen e-mailadres.

Risico's en maatregelen

Ten aanzien van het beginsel *transparantie* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Geen informatie over gegevensverwerking door HEIT

Het HEIT informeert betrokkenen niet over de gegevensverwerking binnen het HEIT. Het is daarom niet duidelijk voor betrokkenen met welk doel bepaalde gegevens door het HEIT worden verwerkt. Daarnaast worden betrokkenen niet op hun rechten gewezen op de flyer of op de persoonlijke pagina van het HEIT.

Pas de informatievoorziening aan de betrokkenen aan. Dit kan bijvoorbeeld door betrokkene(n) op de flyer te informeren over zijn of haar rechten op grond van de AVG. Daarnaast kan op de website worden toegelicht met welk doel gegevensverwerking binnen het HEIT plaatsvindt en welke persoonsgegevens door het HEIT verwerkt worden.

Gemeente Den Haag

Ons kenmerk

BD/

4.8 Cultuur

Inleiding

Zijn medewerkers zich bewust van het belang van het beschermen van privacygevoelige gegevens? Gaat iedereen even zorgvuldig om met de gegevens, worden betrokkenen goed geïnformeerd over hoe men moet omgaan met die gegevens?

Feiten & analyse

Integriteit is een belangrijk thema binnen het HEIT. het waarborgen van de privacy van betrokkenen zit verweven in het proces. Privacy wordt niet als belemmerend ervaren. Er heerst een open aanspreekcultuur waarin medewerkers onderling verbeterpunten op het gebied van privacy en integriteit kunnen bespreken.

Er worden (nog) geen trainingen of e-learnings over privacy en informatiebeveiliging georganiseerd voor medewerkers.

Medewerkers worden gestimuleerd om een cleandesk policy te hanteren en zijn strenge afspraken over de toegang van de werkplek. Gegevens worden netjes opgeruimd na gebruik en worden vergrendeld bewaard.

Risico's en maatregelen

Er zijn ten aanzien van dit thema geen risico's geconstateerd.

5. Advies en accordering

In het risico overzicht dat als bijlage aan deze rapportage is toegevoegd wordt weergegeven welke privacy risico's de verwerking met zich meebrengt, welke beheersmaatregelen hiervoor nodig zijn en welke acties hieraan gekoppeld zijn. Dit overzicht wordt bewerkt zodra beheersmaatregelen worden uitgevoerd en risico's gemitigeerd, zo blijft de DPIA up to date ook na het uitvoeren van beheers acties.

Aanbevelingen voor vervolg

Wij adviseren om de hierboven genoemde risico's als volgt aan te pakken:

1. Benoem een business eigenaar van ieder risico in het risico overzicht en de bijbehorende maatregelen.
2. Geef de business eigenaar de opdracht de maatregelen in te voeren en daarmee het risico te mitigeren.
3. Geef elke 2 maanden een status update van de opvolging van deze aanbevelingen aan de FG en de Privacy Officer.

Gemeente Den Haag

Ons kenmerk

BD/

Advies FG

[GEBRUIK DEZE RUIMTE VOOR HET ADVIES VAN DE FG]

Naam: [NAAM FG]

Datum: [DATUM]

Accordering

Deze DPIA is opgeleverd aan:

5.1.2.e	5.1.2.e
Datum oplevering: [DATUM]	Datum oplevering: [DATUM]
Naam: 5.1.2.e	Naam: 5.1.2.e
Voor akkoord: [HANDTEKENING PROCESEIGENAAR]	Voor gezien: [HANDTEKENING FG]
Datum ondertekening: [DATUM]	Datum ondertekening: [DATUM]

Tekent voor gezien:

5.1.2.e
Datum oplevering: [DATUM]
Naam: 5.1.2.e
Tekent voor gezien: [HANDTEKENING PROCESSEIGENAAR]
Datum ondertekening: [DATUM]

Bijlage A

A1. Documentatie

De volgende documentatie is geraadpleegd.

Nr.	Documentnaam
1	HEIT Convenant 2020
2	Privacy protocol (concept)
3	Werkproces HEIT tbv nieuw convenant

A2. Geïnterviewden

De volgende personen hebben meegewerkt tijdens de DPIA sessie.

Datum	Geïnterviewden	Functie/Rol
11 23-02-2021	5.1.2.e	5.1.2.e
11 23-02-2021	5.1.2.e	5.1.2.e
11 23-02-2021	5.1.2.e	5.1.2.e
11 23-02-2021	5.1.2.e	5.1.2.e
11 23-02-2021	5.1.2.e	5.1.2.e
11 23-02-2021	5.1.2.e	5.1.2.e



DPIA rapportage

Versiebeheer

Versie	Datum	Wijzigingen	Wie
0.9	22-03-21	Oplevering concept	5.1.2.e
1.0	22-04-21	Oplevering definitieve versie	5.1.2.e

Inhoudsopgave

1. Inleiding	3
<i>Aanleiding en onderwerp van de DPIA.....</i>	<i>3</i>
<i>Doelstelling</i>	<i>3</i>
<i>Scope</i>	<i>3</i>
<i>Opbouw van de analyse.....</i>	<i>4</i>
2. Managementsamenvatting	5
3. Beschrijving Verwerking.....	7
<i>Systematische beschrijving van het proces</i>	<i>7</i>
<i>Systematische beschrijving van de verwerking</i>	<i>10</i>
<i>Persoonsgegevens</i>	<i>11</i>
4. Analyse privacy consequenties.....	14
<i>Inleiding</i>	<i>14</i>
4.1 Governance	14
<i>Inleiding.....</i>	<i>14</i>
<i>Feiten & analyse.....</i>	<i>14</i>
<i>Risico's en maatregelen.....</i>	<i>15</i>
4.2 Grondslag & Doelbinding.....	16
<i>Inleiding.....</i>	<i>16</i>
<i>Feiten & analyse.....</i>	<i>16</i>
<i>Rechtmatigheid van de verwerking</i>	<i>17</i>
<i>Risico's en maatregelen.....</i>	<i>18</i>
4.3 Juistheid	19
<i>Inleiding.....</i>	<i>19</i>
<i>Feiten & Analyse.....</i>	<i>19</i>
<i>Risico's en maatregelen.....</i>	<i>19</i>
4.4 Dataminimalisatie	20

Gemeente Den Haag

Ons kenmerk

BD/

Inleiding.....	20
Feiten & Analyse.....	20
Risico's en maatregelen.....	21
<i>4.5 Opslag.....</i>	<i>21</i>
Inleiding.....	21
Feiten & Analyse.....	21
Risico's en maatregelen.....	22
<i>4.6 Bescherming.....</i>	<i>23</i>
Inleiding.....	23
Feiten & Analyse.....	23
Risico's en maatregelen.....	23
<i>4.7 Transparantie.....</i>	<i>25</i>
Inleiding.....	25
Feiten & Analyse.....	25
Risico's en maatregelen.....	25
<i>4.8 Cultuur.....</i>	<i>27</i>
Inleiding.....	27
Feiten & analyse.....	27
Risico's en maatregelen.....	27
5. Advies en accordering.....	28
Aanbevelingen voor vervolg.....	28
Advies FG.....	29
Accordering.....	30
Bijlage A.....	31
A1. Documentatie.....	31
A2. Geïnterviewden.....	31

1. Inleiding

Aanleiding en onderwerp van de DPIA

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens is de gemeente verplicht een DPIA uit te voeren voor verwerkingen die waarschijnlijk een verhoogd risico opleveren.

Voor PGA lokaal is vastgesteld dat een verhoogd risico bestaat, namelijk: er worden bijzondere persoonsgegevens verwerkt in samenwerkingsverband.

Een DPIA is een middel om in kaart te brengen welke persoonsgegevens in een proces, systeem of organisatie verwerkt worden en wat hiervan de risico's voor betrokkenen zijn. Op 10 en 23 februari is een DPIA-workshop gehouden om de benodigde informatie hiervoor op te halen. In Bijlage A is opgenomen wie aan deze bijeenkomst hebben deelgenomen. Dit rapport is het resultaat van deze DPIA.

Doelstelling

Deze DPIA rapportage schetst de eventuele privacy risico's van de onderhavige gegevensverwerking, en maatregelen die kunnen worden getroffen teneinde deze risico's te mitigeren.

In de DPIA wordt vooral gekeken naar de geplande maatregelen, waarborgen en mechanismen om de risico's te beperken, de persoonsgegevens te beschermen en aan te tonen dat aan de beginselen voor verwerking uit de AVG is voldaan. Deze DPIA is een momentopname. Bij nieuwe ontwikkelingen zoals wijzigingen in wetgeving, verandering van processen, inzet van nieuwe technologie e.d. moet de DPIA worden herhaald. Ook dienen uitgevoerde DPIA's periodiek te worden herijkt (iedere 3 jaar).

Scope

Deze DPIA wordt uitgevoerd ten aanzien van de gegevensverwerking in het proces PGA Lokaal.

De scope van het proces heeft betrekking op de gegevensverwerking binnen het samenwerkingsverband de PGA-lokaal. Hieronder valt de aanmelding van casuïstiek bij de PGA-lokaal, het beoordelen van de casus, het opstellen van een persoonsgerichte aanpak in samenwerkingsverband, het monitoren van een casus en het eventueel op- of afschalen van een casus.

Tijdens de plenaire bijeenkomst zijn er een aantal onderdelen buiten scope geplaatst. Allereerst is de reguliere aanpak door de gemeente Den Haag geen onderdeel van deze DPIA. Daarnaast is de PGA binnen het Zorg- en Veiligheidshuis ook geen onderdeel van deze DPIA. De beoordeling van de generieke ICT die wordt gebruikt door de PGA-lokaal binnen de gemeente is ook buiten scope geplaatst.

Opbouw van de analyse

Dit document schetst de privacy risico's binnen bovengenoemde scope en de te nemen maatregelen die het betreffende risico kunnen mitigeren.

De uitvoering van deze DPIA verloopt via de zes beginselen waaraan elke verwerking moet voldoen. Deze zes beginselen zijn Juistheid, Data minimalisatie, Opslag, Bescherming, Transparantie en Grondslag & doelbinding. Daarnaast zijn ook de thema's 'Governance' en 'Privacycultuur' van belang.

Deze beginselen vormen de basis voor de uitvoering van deze analyse. Per thema worden eventuele risico's geanalyseerd en wordt de impact van deze risico's op de betrokkenen en de gemeente ingeschat. Daarnaast worden maatregelen die de eigenaar van de verwerking kan treffen om de risico's tot een acceptabel niveau terug te brengen beschreven. Hierbij wordt rekening gehouden met de haalbaarheid en maakbaarheid van deze maatregelen binnen de context van de gemeente. De eventuele acceptatie van risico's of restrisico's is de verantwoordelijkheid van de eigenaar van de verwerking.

Voor elk van de thema's zijn risico's geïnventariseerd die voor het onderhavige onderwerp relevant kunnen zijn voor de gegevensbescherming binnen de gemeente. De aanwezige deelnemers aan de workshop hebben tijdens het uitvoeren van de risicoanalyse de belangrijkste risico's benoemd en geclassificeerd volgens de onderstaande tabel.

Figuur 1

		Impact →		
		Laag	Midden	Hoog
Kans ↑	Hoog			
	Midden			
	Laag			

2. Managementsamenvatting

Wat zijn de belangrijkste (M-H) risico's die in de analyse zijn geconstateerd? Welke maatregelen zijn hierbij van toepassing.

Beginsel	Risico	Classificatie (L-M-H)	Maatregel (mogelijk)
Governance	Afspraken in Convenant zijn niet volledig	M	Maak duidelijke afspraken met partners over de gegevensverwerking bij het behandelen van casussen in de PGA-lokaal en leg deze vast in het convenant en het aanvullende privacy protocol.
Grondslag & doelbinding	Er is geen wettelijke grondslag voor gegevensverwerking binnen de PGA-lokaal	M	Beoordeel of de doestellingen van het PGA-lokaal en het Zorg- en Veiligheidshuis verenigbaar zijn en of samenwerking kan plaatsvinden in het Zorg- en Veiligheidshuis, zodat er in de Wgs een juridische grondslag wordt gegeven voor gegevensverwerking in de PGA-lokaal.
Opslag	Er is geen bewaartermijn vastgesteld voor verwerkingen binnen de PGA-lokaal	M	Leg de bewaartermijn vast in een daarvoor bestemd document en voer periodiek controles uit op bewaring en verwijdering.
Opslag	Gegevens worden handmatig verwijderd	M	Overweeg om over te gaan tot automatisering van dit proces (bijvoorbeeld door het aanschaffen van een zaakstroom). Zorg er in de tussentijd voor dat bewaartermijnen goed beheerd worden, zodat gegevens voor het verlopen van de bewaartermijn verwijderd worden.
Bescherming	Fysieke documenten onvoldoende afgeschermd	L	Bewaar de fysieke documenten in een afgesloten ladekast in een daarvoor bestemde en afgesloten (werk)kamer. Bewaar de sleutels op een veilige locatie waar alleen PGA-experts toegang tot hebben.
Transparantie	Informatievoorziening aan betrokkenen is niet volledig	H	Betrokkenen hebben het recht op informatie. Overweeg om betrokkenen meer informatie over de gegevensverwerking door de PGA-

Gemeente Den Haag

Ons kenmerk
BD/

			lokaal te geven in de notificatiebrief en/of de privacyverklaring op de website van de gemeente Den Haag uit te breiden met de informatie over de gegevensverwerking.
--	--	--	---

3. Beschrijving Verwerking

Dit hoofdstuk beschrijft het onderhavige proces en de verwerkingen van persoonsgegevens. De beschrijving van het proces en het inventariseren van de verwerkingen van persoonsgegevens zijn onderdeel geweest van de DPIA-workshop.

Systematische beschrijving van het proces

De PGA lokaal is een werkwijze bedoeld om regie te voeren op casuïstiek op het gebied groepen of individuen die ernstige overlast, openbare orde of veiligheidsproblematiek veroorzaken. De casuïstiek wordt integraal behandeld door de samenwerkingspartners door het opstellen en uitvoeren van een persoonsgerichte aanpak. De werkwijze is ontwikkeld om te komen tot een taakverdeling tussen de verschillende betrokken samenwerkingspartners ten behoeve van het aanpakken van de casuïstiek.

Via de PGA lokaal wordt een platform geboden voor integrale casuïstiekbespreking, die nog geen opschaling naar het Zorg- en Veiligheidshuis behoeven, maar waarbij wel degelijk zorgen zijn over een groep of subject. De PGA lokaal staat los van het Zorg- en Veiligheidshuis, maar heeft een vergelijkbare doelstelling. Als een casus intensievere behandeling behoeft, kan worden opgeschaald naar het Zorg- en Veiligheidshuis. Andersom kan een casus worden verwezen naar de PGA lokaal, omdat lokale behandeling beter aansluit op de casus. Er loopt op dit moment een aanbesteding voor een zaakstelsel (PGA-x). Dit stelsel zal zowel door het Zorg- en Veiligheidshuis als de PGA lokaal in gebruik worden genomen. Dit zal tevens aanleiding zijn om deze DPIA te actualiseren. Veel risico's die het gevolg zijn van (teveel) opslaglocaties, (handhaving) bewaartermijnen e.d. zullen daarmee worden verkleind.

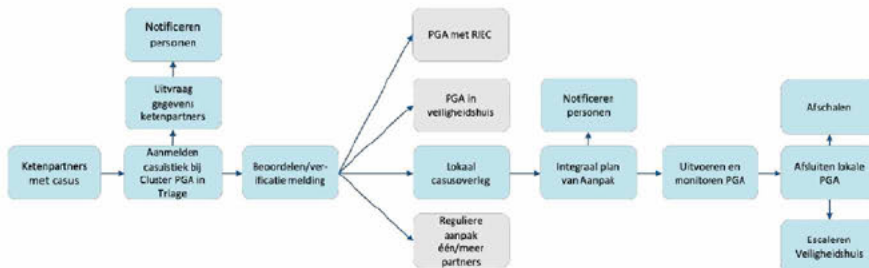
Casuïstiek voor de PGA lokaal heeft betrekking op veel verschillende onderwerpen en kan gebonden zijn aan een persoon of een groep (personen). Hierbij valt te denken aan:

- Jeugdige/volwassen veelplegers
- Overlastgevende personen
- Multiprobleem gezinnen (ketenoverstijgend)
- Ex-gedetineerden
- Huiselijk geweld
- Personen met verward en risicovol gedrag
- Problematische (jeugd)groepen

De PGA lokaal vindt plaats onder regie van de directie Veiligheid van de gemeente Den Haag. Het Cluster PGA, bestaande uit beleidsadviseurs (PGA-experts), werkt nauw samen met accounthouders. De gemeente Den Haag is verdeeld in drie politiedistricten (A, B, C). Aan elk van deze districten is een PGA-expert van het Cluster PGA van de directie Veiligheid van de gemeente Den Haag verbonden.

Gemeente Den Haag

Ons kenmerk
BD/



Start casus door melding

De PGA-cyclus start doordat er een melding wordt gedaan over een potentiële casus. Een melding kan gedaan worden door een wijkteam uit één van de politiedistricten of door een zorgpartner. In de meeste gevallen komt een melding vanuit de politie.

Een melding van een potentiële casus wordt meestal via de e-mail gedaan bij een PGA-expert of accounthouder. Dit sluit niet uit dat een melding ook via andere middelen kan worden ingebracht, zoals telefonisch of mondeling tijdens een overleg. Een melding bevat veelal de volgende persoonsgegevens van het subject (een subject is een persoon of personen die ernstige overlast, openbare orde of veiligheidsproblematiek veroorzaakt): voor- en achternaam, adres, geboortedatum, BSN en de aanleiding van de melding.

Commented [5.12e]: Maak gebruik van extra beveiligde mail en encrypt bijlagen. Dit betekent dat in mailboxen van medewerkers ook persoonsgegevens zitten. Gebruik een groepsmailbox of beter nog een zaaksysteem van waaruit beveiligd kan worden gemaild.

Beoordeling melding

De persoonsgegevens van het subject van de melding worden geverifieerd door raadpleging van de HaagseBron. De HaagseBron ontsluit gegevens uit het BRP, het KvK en het Kadaster. De PGA-expert kan in de HaagseBron ook de nationaliteit en verblijfstatus van het subject raadplegen. Deze gegevens worden niet vastgelegd, maar zijn relevant om uit te sluiten dat het een illegale vreemdeling betreft, dan eindigt het PGA-proces namelijk. In sommige gevallen wordt tevens de directe omgeving van subjecten geraadpleegd in de Haagse Bron of bij ketenpartners. Dit is bijvoorbeeld het geval bij een melding over een mogelijke onveilige thuissituatie. Deze informatie wordt vastgelegd in een matrix in een Excel-document. Dit document wordt opgeslagen op de g:schijf.

Commented [5.12e]: Wordt dit encrypt of bevaligd?

Commented [5.12e]: Tweede locatie voor persoonsgegevens: de g: schijf.

Uitvraag gegevens bij ketenpartners

Op basis van de ingebrachte casuïstiek wordt via Outlook een informatieverzoek gedaan bij de verschillende ketenpartners. In het informatieverzoek staan de NAW-gegevens, BSN en geboortedatum van het subject. De PGA-expert verzamelt de need to know door de ketenpartners ingebrachte gegevens in een Excel-document. Hierin staat in ieder geval of de

ketenpartner bekend is met het subject, wie de betrokken professional is en de deelbare informatie over het subject. Dit document wordt opgeslagen op de g:schijf.¹

Triage en casusoverleg

Elke twee weken vindt er een triage plaats tussen een vast aantal partners van de PGA-lokaal. De triage heeft, in beginsel, de volgende samenstelling: PGA-expert en accounthouder van de directie Veiligheid van de gemeente Den Haag, politie, Reclassering Nederland, Jeugdbescherming West. Op basis van de melding maakt de PGA-expert een professionele afweging welke ketenpartners eventueel aanvullend op de reeds bestaande deelnemers aan de triage moeten worden uitgenodigd. Deze ketenpartners ontvangen een uitnodiging via Outlook.

De triage wordt voorgezeten door de PGA-expert. Het subject wordt geïntroduceerd door de aanmelder. Vervolgens kunnen (overige) ketenpartners informatie over het subject inbrengen in het casusoverleg. Tijdens de triage wordt bepaald of de casus geschikt is voor de PGA lokaal of moet worden opgeschaald naar het Zorg- en Veiligheidshuis of afgeschaald naar een reguliere aanpak. De behandeling van casuïstiek door het Zorg- en Veiligheidshuis of in een reguliere handeling valt niet binnen de scope van dit proces.

Commented 5.1.2.ej: Wordt de informatie direct vernietigd als de PGA aanpak niet wordt voortgezet?

Tijdens de triage wordt de casus beoordeeld op basis van verschillende aspecten. In de probleemschets wordt beoordeeld of het subject ernstige overlast, openbare orde of veiligheidsproblematiek veroorzaakt waarop extra regie nodig is. Op basis van deze probleemschets wordt vervolgens beoordeeld waar dit probleem thuishoort en welk platform hiervoor het meest geschikt is. Een triage kan leiden tot verschillende uitkomsten. Allereerst kan de mogelijkheid zich voordoen dat de problematiek geen PGA lokaal casus betreft en in een ander gremium moet worden opgepakt. Daarnaast kan tevens worden beslist dat opschaling is vereist vanwege de complexiteit van de casus. In dat geval wordt de casus doorgezet naar het Zorg- en Veiligheidshuis. Tot slot kan worden besloten dat de casus een integrale groepsaanpak vereist. Dit wordt besloten in een ander proces waarin de groepsscan van de politie de basis is. Dit valt buiten de scope van deze DPIA. De casus wordt besproken in een lokaal casusoverleg. Een (nieuwe) uitnodiging voor een lokaal casusoverleg volgt via Outlook. Dit casusoverleg vindt spoedig na de triage plaats. Er wordt tijdens het casusoverleg een integraal plan van aanpak opgesteld (de persoonsgerichte aanpak). Dit plan van aanpak bestaat uit verschillende actiepunten voor de deelnemers aan de casuïstiek.

Elke PGA-expert wordt ondersteund door een beleidsondersteuner. De beleidsondersteuner voert de administratieve werkzaamheden voor de PGA-expert uit. Tijdens de triage wordt genotuleerd door de beleidsondersteuner. Deze notulen bevat tevens de acties van de (verschillende) ketenpartners. De PGA-expert ontvangt de notulen via Outlook of kan deze raadplegen op de g:schijf. De acties worden via Outlook uitgezet bij de betreffende ketenpartners. De ketenpartners ontvangen alleen de acties die aan hen gericht zijn. In de e-mail worden bijna geen gegevens over het subject verstrekt. Er wordt vaak verwezen naar subject middels naam of een letter van de voor- of achternaam.

¹ In de praktijk wordt de PGA-expert ondersteund door een beleidsondersteuner. De beleidsondersteuner voert de administratieve werkzaamheden voor de PGA-expert uit.

Notificeren personen

Het subject wordt voorafgaande of direct na de triage genotificeerd middels een notificatiebrief. De notificatiebrief wordt verzonden vanuit de directie Veiligheid van de gemeente en ondertekend namens de burgemeester of door de plaatsvervangend directeur van de Directie Veiligheid. In de notificatiebrief staat de aanleiding van prioritering vermeld, de aanpak van het PGA en wordt het subject gewezen op zijn rechten. Hierbij wordt verwezen naar de privacyverklaring op de website van de gemeente. De persoon in kwestie heeft recht op deze informatie tenzij er zwaarwegende redenen zijn om hiervan af te zien. Wanneer het een minderjarige (jonger dan 16 jaar) betreft worden de ouders of verzorgers van het kind geïnformeerd (dit is verplicht).

Monitoring

De acties uit het plan van aanpak die zijn uitgezet bij ketenpartners worden (periodiek) gemonitord door de beleidsondersteuner. De beleidsondersteuner heeft hiertoe telefonisch of per e-mail contact met de ketenpartners. Dit wordt ook bijgehouden in een Word-document en opgeslagen op de g:schijf. Op de g:schijf wordt het subjectdossier bijgehouden. Hierin staan de gegevens afkomstig van ketenpartners, de notulen van het casusoverleg (en/of triage), het plan van aanpak, de acties en de opvolging van de acties inclusief een eindafpraak (bijvoorbeeld dat de politie het subject blijft monitoren). In de periode waarin een subject wordt gemonitord kan (op basis van een nieuwe melding) aanleiding bestaan om het subject te her agenderen. De cyclus begint opnieuw.

Na een periode van twaalf maanden monitoren, en bij ernstige maatschappelijke onrust na maximaal twee jaar monitoren, wordt de casus op- of afgeschaald. De PGA wordt daarmee afgesloten.

Systematische beschrijving van de verwerking

Onderstaand een schematische weergave van de persoonsgegevens. Wat ontvang je (wat krijg je), wat verwerk je (wat doe je ermee) en wat verstrek je (wat geef je door).

Wat krijg je	Van wie	Hoe
<i>Melding met gegevens over subject:</i> - Voor- en achternaam - Adresgegevens - Geboortedatum - Aanleiding van de melding	Ketenpartners	E-mail, telefonisch of mondeling (mondeling tijdens periodiek overleg)
<i>Informatie uit informatieverzoek</i> - Is het subject bekend? - Betrokken professional - Deelbare informatie	Ketenpartners	Excel, E-mail
<i>Informatie uit triage:</i> - Gegevens over de activiteiten/omstandigheden die het risico op criminaliteit en overlast kunnen vergroten of verkleinen; - Gegevens over de hulpverlening van het individu dan wel zijn of haar systeem; - Gegevens over de omstandigheden in verband met werk, inkomen, huisvesting en schulden;	Ketenpartners	E-mail, telefonisch of mondeling (mondeling tijdens periodiek overleg)

Gemeente Den Haag

Ons kenmerk

BD/

- Gegevens over de woonsituatie, gezinssituatie en leefsituatie; - Gegevens over de schoolsituatie en schoolverzuim - Politiegegevens - Strafvorderlijke gegevens		
Resultaat triage: - Gegevens over de door de deelnemers (voorgenomen) maatregelen ter uitvoering van het plan van aanpak	Ketenpartners	Mondeling tijdens periodiek overleg

Wat doe je ermee	Middelen
Verificatie BSN van subject (en in sommige gevallen ook van de directe omgeving)	HaagseBron
Verrijking melding met gegevens over nationaliteit en verblijfstatus van subject	HaagseBron
Plan van aanpak	Excel, g:schijf, e-mail
Notulen	Word, g:schijf
Acties/maatregelen	Word, g:schijf, e-mail
Eindafspraak	G:schijf

Wat geef je door	Aan wie	Hoe
Informatieverzoek ketenpartners inclusief melding (hierin staat vermeld: NAW-gegevens en geboortedatum subject)	Ketenpartners	E-mail
Acties	Ketenpartners	E-mail
Notificatiebrief	Betrokkene	Brief (in persoon of per post)

Persoonsgegevens

Gemeente Den Haag

Ons kenmerk
BD/

Wij hanteren de classificatie zoals weergegeven in onderstaande figuur om te bepalen welke persoonsgegevens worden verwerkt. Er wordt onderscheid gemaakt tussen weinig gevoelige gegevens (algemene persoonsgegevens), door de aard of context extra gevoelige gegevens (gevoelige persoonsgegevens) en zeer gevoelige gegevens die wettelijk extra beschermd zijn (bijzondere persoonsgegevens). Al naar gelang de situatie kunnen gegevens in verschillende categorie worden geplaatst.



Binnen de scope van deze DPIA worden de volgende categorieën van persoonsgegevens verwerkt:

	Algemeen	Gevoelig	Bijzonder
Gestructureerd	• Voor- en achternaam • Adresgegevens • Geboortedatum	• BSN • Gegevens over de hulpverlening van het individu dan wel zijn of haar systeem; • Gegevens over de omstandigheden in verband met werk, inkomen, huisvesting en schulden; • Gegevens over de woonsituatie, gezinssituatie en leefsituatie;	• Politiegegevens • Strafvorderlijke gegevens

Gemeente Den Haag

Ons kenmerk
BD/

		• Gegevens over de schoolsituatie en schoolverzuim	
Ongestructureerd	• N.v.t.	• Gegevens over de activiteiten/omstandigheden die het risico op criminaliteit en overlast kunnen vergroten of verkleinen;	• N.v.t.

4. Analyse privacy consequenties

Inleiding

Dit hoofdstuk beschrijft de resultaten uit de uitgevoerde DPIA per thema. Voor ieder thema geven we een korte toelichting en beschrijven wij de risico's, de impact van de risico's op de betrokkenen en de gemeente en de maatregelen die de gemeente kan treffen om de risico's tot een acceptabel niveau terug te brengen. Daarnaast worden ook de ethische aspecten die mogelijk spelen in dit hoofdstuk besproken.

4.1 Governance

Inleiding

Is helder wie de verantwoordelijke en de verwerker zijn en hoe wordt toegezien op een adequate bescherming van persoonsgegevens? Is er beleid gemaakt ten aanzien van privacy en wordt er intern gecontroleerd op naleving van dit beleid? Is duidelijk wie binnen de organisatie verantwoordelijk is voor privacy?

Feiten & analyse

De PGA-lokaal bestaat uit de gemeente Den Haag, politie, OM, Stichting Reclassering Nederland, Stichting Leger des Heils, Fivoor B.V., Stichting Jeugdbescherming, Stichting Halt, Stichting Middin, Parnassia Groep B.V., Stichting William Schrikker Groep en Stichting Xtra+. De PGA lokaal vindt plaats onder regie van de directie Veiligheid van de gemeente Den Haag.

De samenwerking in de PGA-lokaal is vrij recent ontstaan in juli 2020. Samenwerking verliep daarvoor in het Zorg- en Veiligheidshuis. In het Zorg- en Veiligheidshuis werken meer zorgpartners samen om complexere casuïstiek te behandelen.

De informatie-uitwisseling van de partners ten behoeve van de doelstelling(en) van de PGA-lokaal vindt plaats volgens de afspraken in de PGA-lokaal convenant. Dit convenant is getekend door alle deelnemers. Het document regelt de inbedding van het samenwerkingsverband PGA-lokaal en de afspraken daarover op organisatieniveau, zoals het doel en de functie van de PGA-lokaal, de structuur en procesgang. Daarnaast worden een aantal eisen vanuit de privacywetgeving geregeld, zoals wie verwerkingsverantwoordelijke is voor de gegevensverwerking en het behandelen van rechten van betrokkenen. In het convenant zijn geen afspraken gemaakt over de volgende thema's: grondslag, categorieën persoonsgegevens die worden verwerkt, dataminimalisatie en wat partners doen bij een datalek (protocol datalekken). Informeel is dit laatste belegd bij de Functionaris Gegevensbescherming van de gemeente Den Haag.

De partners zijn eenieder zelfstandig verwerkingsverantwoordelijk voor de verwerking van persoonsgegevens waar het de uitoefening van hun eigen (publiekrechtelijke) taken binnen de samenwerking betreft. De partners zijn gezamenlijk verwerkingsverantwoordelijk voor de verwerking van gegevens in samenwerkingsverband. De directie Veiligheid van de gemeente

Commented 5.1.2e]: Zelfstandige en gezamenlijke verwerkingsverantwoordelijkheid

Den Haag is als hoofdverwerkingsverantwoordelijke aangewezen. Hier wordt namelijk doel en middelen bepaald van de gezamenlijke aanpak PGA lokaal.

De gemeente houdt een register van verwerkingsactiviteiten bij (in iNavigator) waarin alle gemeentelijke processen zijn opgenomen. Het PGA-lokaal proces maakt (nog) geen onderdeel uit van het register.

Commented 5.1.2.e]: Neem PGA lokaal op in het register van verwerkingen

De PGA-lokaal maakt geen gebruik van systemen. Er vindt momenteel een aanbesteding plaats voor de aanschaf van een systeem (PGA-X). Voor ingebruikname hiervan moeten afspraken worden gemaakt met de leverancier in een verwerkersovereenkomst.

Risico's en maatregelen

Op basis van de analyse op het aspect *governance* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: afspraken in convenant zijn niet volledig

In het Convenant PGA-lokaal zijn onvoldoende afspraken gemaakt over zorgvuldige gegevensverwerking door partners in het samenwerkingsverband. Hierdoor ontstaat allereerst een compliance risico. Er wordt immers niet aantoonbaar voldaan aan de eisen uit de AVG. Daarnaast is de kans op een risico voor de betrokkene(n) groter, omdat er geen duidelijke afspraken zijn gemaakt over bijvoorbeeld welke gegevens er worden verwerkt door het samenwerkingsverband, hoe de gegevens worden beschermd en wat het protocol is bij een datalek in het samenwerkingsverband. De volgende thema's ontbreken in ieder geval:

- Grondslag voor het verwerken en verstrekken van persoonsgegevens ten behoeve van het behandelen van een casus en de van toepassing zijnde taken van partijen;
- Beschrijving categorieën persoonsgegevens die worden verwerkt in het kader van de samenwerking;
- Dataminimalisatie (er worden niet meer persoonsgegevens verwerkt dan noodzakelijk voor de doeleinden zoals omschreven in het convenant);
- Bewaren en vernietigen;
- Beveiliging (passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen verlies of enige vorm van onrechtmatige verwerking);
- Datalekken (procedures voor het omgaan met datalekken door partijen)

Maatregel:

Maak duidelijke afspraken met partners over de gegevensverwerking bij het behandelen van casussen in de PGA-lokaal en leg deze vast in het convenant. Het convenant dient minimaal aangevuld te worden met bovenstaande onderwerpen. Overweeg bovenstaande eisen vast te leggen in bijbehorend privacy protocol. Neem voorbeeld aan de afspraken die het Zorg- en Veiligheidshuis heeft gemaakt. Deze biedt tevens modeldocumenten aan.

4.2 Grondslag & Doelbinding

Inleiding

Het moet helder zijn wat het doel van de gegevensverzameling is, op het moment dat de gemeente deze verzamelt. Het doel moet ook in overeenstemming zijn met de normale werkzaamheden van de gemeente en onderbouwd zijn door één of meer wettelijke grondslagen.²

Feiten & analyse

Het doel van de PGA-lokaal is vastgelegd in het convenant. De samenwerking tussen de convenantpartners binnen de PGA-lokaal heeft als doel het aanpakken van casuïstiek die de openbare orde aantast of maatschappelijke onrust kan veroorzaken, het voorkomen van (verder) crimineel en/of overlast-gevend gedrag of verder afglijden van die personen, het oplossen van ernstige lokale of gebiedsgebonden veiligheidsproblematiek en het op effectieve en integrale wijze aanpakken en terugdringen criminaliteit en overlast door de jongeren, hun sociale positie versterken en hen perspectief bieden, de negatieve groepsdynamiek verstoren en aanwas voorkomen.

De verschillende partners in de PGA-lokaal verwerken persoonsgegevens op grond van hun eigen publiekrechtelijke wettelijke taken en bevoegdheden. De gemeente Den Haag heeft uiteenlopende taken en bevoegdheden die van belang zijn voor de doelstellingen van de samenwerking in de PGA-lokaal. Deze taken en bevoegdheden vinden hun grondslag in de Gemeentewet en verschillende sectorale wetten, waaronder:

- de burgemeester voor de uitoefening van zijn wettelijke taken en bevoegdheden op het terrein van de handhaving van de openbare orde bij of krachtens hoofdstuk XI van titel III van de Gemeentewet, paragraaf 2.3 van de Politiewet 2012, artikel 13b van de Opiumwet of een gemeentelijke verordening en voor de uitoefening van zijn wettelijke taken en bevoegdheden bij of krachtens de Wet tijdelijk huisverbod en de artikelen 1, 7:2, 7:4 en 8:1 van de Wet verplichte geestelijke gezondheidszorg en de artikelen 29 tot en met 36 van de Wet zorg en dwang psychogeriatrische en verstandelijke gehandicapte cliënten;
- het college van burgemeester en wethouders voor de uitoefening van zijn wettelijke taken en bevoegdheden bij of krachtens de artikelen 2.1.1, eerste lid, 2.1.7, 2.3.6, 2.3.9, 2.3.10 en 2.4.1 van de Wet maatschappelijke ondersteuning 2015, de artikelen 2.3 en 2.4 van de Jeugdwet, artikel 7 van de Participatiewet, artikel 3 van de Wet gemeentelijke schuldhulpverlening, artikel 16 van de Leerplicht wet 1969 en de wettelijke taken en bevoegdheden bedoeld in de artikelen 5:1, 5:2, 5:3 en 5:16 van de Wet verplichte geestelijke gezondheidszorg, artikel 28c van de Wet zorg en dwang psychogeriatrische en verstandelijke gehandicapte cliënten; en artikel 2:7 van het besluit tenuitvoerlegging strafrechtelijke beslissingen.

² De wettelijke grondslag is de rechtvaardiging om persoonsgegevens te mogen verwerken, zoals bedoeld in artikel 6 lid 1 e.v. van de Algemene Verordening Gegevensbescherming. De wettelijke grondslagen uit dit artikel zijn; toestemming, ter uitvoering van een overeenkomst, wettelijke plicht, vitale belang, taak van algemeen belang en het gerechtvaardigd belang.

- de goede uitvoering van taken en de uitoefening van bevoegdheden van de burgemeester, waaronder in het bijzonder taken en bevoegdheden op het gebied van Openbare Orde en Veiligheid zoals neergelegd in de Gemeentewet artikel 172.
- goede uitvoering van taken van het College van B&W, waaronder in het bijzonder taken in het sociaal domein zoals bedoeld in de WMO artikel 2.3.1 t/m 2.3.5, de Jeugdwet artikel 2,3 en 2.4, de Participatiewet artikel 7.1, en de wet schuldhulpverlening artikel 3.

De grondslag voor de verwerking van gegevens door de gemeente, waaronder het verstrekken en ontvangen van persoonsgegevens aan/van partners in de PGA lokaal, wordt gevonden in artikel 6, eerste lid, onder e, van de AVG. De gegevensverwerking is noodzakelijk voor de vervulling van een taak van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze bevoegdheden worden gevonden in (sectorale) wetten zoals hierboven beschreven.

De PGA-lokaal verwerkt gegevens in samenwerkingsverband (zoals de melding bestaande uit voor- en achternaam, adresgegevens, geboortedatum, BSN en aanleiding van de melding, maar ook gegevens ontvangen op basis van het informatieverzoek en in de triage met partners). Er bestaat formeel (nog) geen wettelijke grondslag op basis waarvan gegevens kunnen verwerkt door het samenwerkingsverband. De wettelijke grondslag voor gegevensverwerking binnen samenwerkingsverbanden wordt in de toekomst gecreëerd in de Wgs. De Wgs is op 17 december jl. goedgekeurd. De commissie voor Justitie en Veiligheid gaat voorlichting aan de Afdeling advisering van de Raad van State en advies aan de Autoriteit Persoonsgegevens vragen wegens amendering van dit wetsvoorstel. Daarna zal dit wetsvoorstel worden voorgelegd aan de Eerste Kamer. Het is op dit moment onduidelijk binnen welke termijn dit verwacht mag worden.

In hoofdstuk 2 van de Wgs worden een aantal samenwerkingsverbanden aangewezen als samenwerkingsverband in de zin van de Wgs. Gegevensverwerking binnen deze samenwerkingsverbanden wordt aangemerkt als noodzakelijk ten behoeve van een doelstelling van zwaarwegend algemeen belang.

De Zorg- en Veiligheidshuizen zijn in de Wgs aangewezen als samenwerkingsverband in de zin van de Wgs. De PGA-lokaal, als afzonderlijk samenwerkingsverband, is dat niet. Het is daarom nog onduidelijk wat de precieze impact van de Wgs op de PGA-lokaal is, omdat het huidige wetsvoorstel nog aan amendering onderhevig is.

Rechtmatigheid van de verwerking

Op basis van de analyse wordt de gegevensverwerking binnen de PGA-lokaal als niet rechtmatig beoordeeld door het ontbreken van een juridische basis hiervoor.

Op basis van de analyse wordt de gegevensverwerking door de gemeente Den Haag, waaronder het verstrekken en ontvangen van persoonsgegevens aan/van partners in de PGA lokaal, als rechtmatig beoordeeld.

Commented 5.12.20: Oh, lekker verwarrend. Is het ALLEBEI waar?

Risico's en maatregelen

Op basis van de analyse op het aspect *grondslag en doelbinding* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Er is geen wettelijke grondslag voor gegevensverwerking binnen de PGA-lokaal

Er is geen juridische basis voor gegevensverwerking binnen (het samenwerkingsverband) de PGA-lokaal. Hierdoor ontstaat het risico op onrechtmatige gegevensverwerking.

Dit risico geldt voor de gegevensverwerking door alle samenwerkingsverbanden waarin publieke (en private partijen) gezamenlijk gegevens verwerken. De Wgs beoogt een algemene juridische grondslag te geven voor gegevensverwerking noodzakelijk ten behoeve van zwaarwegende algemene belangen. De PGA-lokaal wordt in de Wgs niet aangewezen als samenwerkingsverband in deze context (anders dan bijvoorbeeld het Zorg- en Veiligheidshuis).

Maatregel:

Onderzoek of alle deelnemers aan de PGA-lokaal tevens deelnemer zijn van het Zorg- en Veiligheidshuis. Beoordeel of de doestellingen van het PGA-lokaal en het Zorg- en Veiligheidshuis overeenkomstig zijn en of samenwerking kan plaatsvinden in het Zorg- en Veiligheidshuis, zodat er in de Wgs een juridische grondslag wordt gegeven voor gegevensverwerking in de PGA-lokaal.

4.3 Juistheid

Inleiding

Is de kwaliteit van de gegevens gewaarborgd (actueel, juist en volledig)? Hoe worden gegevens over de personen verwerkt (handmatig of automatisch?) Vindt er controle op de datakwaliteit plaats en zo ja wanneer?

Feiten & Analyse

Een melding kan door elke partner worden gedaan en geeft aan dat er zorgen zijn over een bepaald subject waarbij mogelijk sprake is van openbare orde problematiek, veiligheid, maatschappelijke onrust of overlast. Hierbij wordt door partners duidelijk onderscheid gemaakt tussen feiten en vermoedens.

In een melding worden de voor- en achternaam, adresgegevens, geboortedatum en BSN van het subject vermeld. Deze gegevens worden wel eens foutief aangeleverd door een partner. Daarom wordt de identiteit van het subject altijd geverifieerd in de HaagseBron door een PGA-expert. De juistheid van de gegevens uit de bronsystemen die door HaagseBron worden ontsloten staat vast.

Als er foutieve gegevens worden ontdekt dan geeft de PGA-expert een terugkoppeling hiervan aan de partner, zodat de partner de gegevens kan wijzigen. Op deze manier wordt samen gewerkt aan een betere datakwaliteit.

Risico's en maatregelen

Er zijn ten aanzien van het beginsel *Juistheid* geen risico's geïdentificeerd.

4.4 Dataminimalisatie

Inleiding

Kan er met bijvoorbeeld minder persoonsgegevens, of op een andere manier worden gewerkt zonder de functionaliteit van het proces en systeem aan te tasten? Zijn er rapportages waarin tot individuen herleidbare informatie is opgenomen? Worden alleen die gegevens vastgelegd die absoluut noodzakelijk zijn voor het doel van de verwerking? Welke zijn dat niet?

Feiten & Analyse

Een melding bestaat uit voor- en achternaam, adresgegevens, geboortedatum en BSN van het subject. Deze gegevens worden als melding ingediend bij de PGA-expert of accounthouder. De PGA-expert maakt op basis van de melding een professionele afweging of de melding in samenwerkingsverband moet worden opgepakt of dat een reguliere aanpak volstaat.

Ten tijde van de plenaire bijeenkomst werd het BSN van de betrokkenen verwerkt door de PGA lokaal. Dit werd verstrekt aan alle deelnemers van de PGA lokaal, omdat het BSN voor sommige partners (zoals het JMO) noodzakelijk was om de identiteit van subjecten te verifiëren om verwarring/verwisseling van personen te voorkomen. Dit is in de tijd tussen de plenaire bijeenkomst en het opleveren van de definitieve rapportage van deze DPIA aangepast. **Het BSN wordt niet langer gevraagd en/of gedeeld met partners in de PGA lokaal.**

De geboortedatum is noodzakelijk omdat de leeftijd van het subject relevant is voor de aanpak (leeftijdsgrens 16, 18, en 21).

De PGA-expert of accounthouder verifieert de gegevens door raadpleging van de HaagseBron. Indien noodzakelijk worden de gegevens aangevuld. Als er sprake is van een onveilige thuissituatie kan, in voorkomende gevallen, ook de directe omgeving van de betrokkene worden geraadpleegd in de HaagseBron of bij ketenpartners. In de HaagseBron wordt tevens uitgesloten dat het subject een illegale vreemdeling betreft. In dat geval stopt de casus. Gegevens over de nationaliteit worden niet vastgelegd.

In de triage worden bijzondere gegevens gedeeld door partners over het subject. Dit zijn bijvoorbeeld gegevens over strafvorderlijke gegevens of politiegegevens. Deze gegevens zijn noodzakelijk voor het opstellen van een gezamenlijk plan van aanpak. Deze gegevens worden vastgelegd in de notulen. De notulen worden na afloop van het casusoverleg niet met partners gedeeld. Partners in het overleg nemen alleen kennis van persoonsgegevens van andere partijen voor zover dit noodzakelijk is ter beoordeling van de situatie en/of om te komen tot een adequaat integraal beeld.

De acties uit het casusoverleg worden verstuurd naar de deelnemende partners. De partners ontvangen alleen de actie waarvoor zij verantwoordelijk zijn.

De PGA-lokaal voert rapportages op geaggregeerd niveau uit en deelt deze met de gemeenteraad. Hierin staan geen persoonsgegevens.

Risico's en maatregelen

Er zijn ten aanzien van het beginsel *dataminimalisatie* geen risico's geïdentificeerd.

4.5 Opslag

Inleiding

Welke bewaartermijnen zijn van toepassing? Hoe worden persoonsgegevens bewaard en worden persoonsgegevens die niet langer nodig zijn daadwerkelijk verwijderd? Worden op de middelen (desktop, pc, mobiele telefoon) zelf gegevens opgeslagen?

Feiten & Analyse

Persoonsgegevens worden binnen de PGA-lokaal op een aantal verschillende plekken opgeslagen, te weten de g:schijf en Outlook. Daarnaast wordt er in sommige gevallen ook met fysieke documenten gewerkt. Bijvoorbeeld als deze voor ondertekening naar de burgemeester moeten. Deze worden bewaard in een afgesloten ladekast. Er wordt (nog) geen gebruik gemaakt van een zaakstelsel.

De gemeente moet voldoen aan bewaartermijnen zoals vastgelegd in de Selectielijst van de VNG. Hierin zijn de bewaartermijnen van archiefbescheiden van gemeentelijke en intergemeentelijke organen vastgelegd. Een samenwerkingsverband zoals de PGA-lokaal staat niet tussen de processen op de Selectielijst van de VNG en zal derhalve zelfstandig een bewaartermijn moeten vastleggen.

Er wordt een bewaartermijn van een jaar, en bij maatschappelijke onrust twee jaar, gehanteerd voor persoonsgegevens die in het kader van een casus worden verwerkt. Deze bewaartermijn is (nog) niet vastgelegd. De bewaartermijn start na het op- of afschalen van een casus. Een casus wordt afgeschaald na een periode van monitoring op acties uit het plan van aanpak van het subject. Deze periode duurt gemiddeld zes maanden tot twee jaar. Vernietiging van de gegevens is vanwege de korte looptijd van de PGA-lokaal nog niet aan de orde. Als de bewaartermijn wordt bereikt zullen de gegevens handmatig worden vernietigd. Hiervoor is (nog) geen notificatie ingesteld. De verwachting is dat er een zaakstelsel komt waarin de bewaartermijnen worden gemonitord en gegevens automatisch worden vernietigd na het verlopen van de bewaartermijn.

Er worden, ten behoeve van de werkzaamheden, documenten geprint en gescand met persoonsgegevens daarin. Het is onduidelijk of het apparaat een historie heeft en, zo ja, of deze (tijdig) wordt verwijderd. Dit wordt gemeentebreed uitgezocht, omdat het om een generieke voorziening gaat.

Risico's en maatregelen

Ten aanzien van het beginsel *opslag* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Er is geen bewaartermijn vastgesteld voor verwerkingen door de PGA-lokaal

De PGA-lokaal staat niet tussen de processen op de Selectielijst van de VNG. De PGA-lokaal zal derhalve zelfstandig een bewaartermijn moeten vastleggen. Er wordt een bewaartermijn van maximaal twee jaren gehanteerd door de PGA-lokaal. Vastlegging hiervan ontbreekt nog. Hierdoor ontstaat het risico dat het bewaartermijn niet (consistent) wordt toegepast en gegevens langer worden bewaard dan noodzakelijk is. Bij een datalek zorgt dit voor onnodig grote impact.

Maatregel:

Leg de bewaartermijn vast in een daarvoor bestemd document en voer periodiek controles uit op bewaring en verwijdering. De bewaartermijn kan bijvoorbeeld worden opgenomen in het register van verwerkingsactiviteiten.

Risico: Gegevens worden handmatig verwijderd

Er vindt op dit moment handmatige verwijdering van gegevens plaats en er vinden geen automatische reminders plaats bij het verlopen van de bewaartermijn. Zonder goed ingericht beheer hierop, is dit erg foutgevoelig waardoor gegevens mogelijk te lang worden bewaard (op verschillende plekken).

Maatregel

Overweeg om over te gaan tot automatisering van dit proces (bijvoorbeeld door het aanschaffen van een zaaksysteem). Zorg er in de tussentijd voor dat bewaartermijnen goed beheerd worden, zodat gegevens voor het verlopen van de bewaartermijn verwijderd worden.

4.6 Bescherming

Inleiding

Persoonsgegevens moeten technisch en organisatorisch adequaat worden beschermd. Op welke wijze is de toegang tot gegevens afgeschermd? Is dit voldoende veilig in verhouding tot de gevoeligheid van de gegevens die verwerkt worden? Welke externe partijen hebben toegang tot de gegevens (leveranciers, samenwerkingspartners, dienstverleners) en hoe is de beveiliging daar geregeld?

Feiten & Analyse

Tijdens de plenaire bijeenkomst hebben we de generieke ICT buiten scope geplaatst. We gaan ervan uit dat de generieke ICT (Microsoft producten, g:schijf, thuiswerkomgeving, scanappartuur etc) als veilig mag worden beschouwd binnen deze DPIA.

De g: schijf is afgeschermd en alleen toegankelijk voor het cluster PGA. Dit betreft in totaal tien personen. Op de g: schijf is een aparte map voor de PGA-lokaal. Deze map is toegankelijk op basis van autorisaties. Er hebben op dit moment acht personen toegang tot deze map.

De fysieke documenten worden bewaard in afgesloten ladekasten in de werkkamers van de PGA-experts. De sleutel waarmee de kast kan worden geopend wordt op een voor PGA-experts bekende plek in de werkkamer bewaard. De werkkamers zijn gereserveerd voor PGA-experts, maar betreffen flexibele werkplekken.

Alle medewerkers van het Cluster PGA-lokaal zijn in het bezit van een verklaring omtrent gedrag (VOG). Integriteit is tevens een belangrijk thema binnen het cluster.

Er is een gemeentebreed datalekprotocol voorhanden. Dit protocol is bij de medewerkers bekend en wordt gevolgd.

Risico's en maatregelen

Ten aanzien van het beginsel *bescherming* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Fysieke documenten onvoldoende afgeschermd

De afgesloten ladekasten waarin de fysieke documenten worden bewaard kunnen worden geopend met een sleutel die is verstopt in de werkkamer. Doordat de werkkamer is bestemd als flexibele werkplek kan niet worden gegarandeerd dat de werkkamer uitsluitend wordt gebruikt door (PGA)werknemers die betrokken zijn bij de casus. Hierdoor ontstaat het risico dat de fysieke documenten worden geraadpleegd door onbevoegden. Dit vergroot het risico op een datalek. Bovendien betreft het gevoelige gegevens, waardoor de impact van een datalek voor de betrokkene erg groot is.

Maatregel:

Gemeente Den Haag

Ons kenmerk

BD/

Bewaar de fysieke documenten in een afgesloten ladekast in een daarvoor bestemde en afgesloten (werk)kamer. Bewaar de sleutels op een veilige locatie waar alleen PGA-experts toegang tot hebben.

4.7 Transparantie

Inleiding

De gemeente is helder in de gegevens die zij verwerkt. De betrokkene moet goed kunnen begrijpen welke persoonsgegevens worden verwerkt (en waarom) en heeft het recht en de mogelijkheid om in te grijpen. De betrokkene heeft het recht op informatie, inzage, correctie en verwijdering.

Feiten & Analyse

Een betrokkene wordt voorafgaand of direct na de triage geïnformeerd door middel van een notificatiebrief. Deze wordt ondertekend namens de burgemeester door de plaatsvervangend directeur van de directie Veiligheid. De brief wordt meestal uitgereikt in persoon aan de betrokkene (bijvoorbeeld door een wijkagent). Als dit niet het geval is, wordt de brief per post verstuurd.

In de notificatiebrief wordt de betrokkene op de hoogte gebracht van de verwerking van persoonsgegevens in het kader van de PGA. Er wordt tevens verwezen naar de privacyverklaring op de website van de gemeente Den Haag waarop de rechten van betrokkenen worden toegelicht. In de brief staan ook contactgegevens van de PGA-lokaal, zodat de betrokkene telefonisch of via e-mail contact kan opnemen bij vragen, opmerkingen of klachten.

Zoals hierboven gezegd heeft de gemeente op haar website een privacyverklaring staan. Betrokkenen kunnen een verzoek indienen door een e-mail te sturen naar gegevensbescherming@denhaag.nl. De PGA-lokaal heeft nog geen ervaring met verzoeken van betrokkenen. De partners binnen de PGA-lokaal hebben afgesproken dat een door een betrokkene ingediend verzoek, bestemd voor een andere partner, via het FG-netwerk wordt doorgezet naar de juiste partner.

Risico's en maatregelen

Ten aanzien van het beginsel *transparantie* zijn de volgende risico's geïdentificeerd.

Risico: informatievoorziening aan betrokkene(n) is niet volledig

De betrokkenen worden op dit moment beperkt geïnformeerd over de gegevensverwerking door PGA-lokaal. In de notificatiebrief worden betrokkenen gewezen op de gegevensverwerking in het kader van de prioritering door de PGA-lokaal en verwezen naar de privacyverklaring op de website van de gemeente. Daarin staat echter niet alle noodzakelijke informatie opgenomen. De betrokkenen worden op dit moment bijvoorbeeld niet geïnformeerd over het doel (en de grondslag) van de verwerking, welke persoonsgegevens worden verwerkt door de PGA-lokaal en met wie deze gegevens worden gedeeld.

Maatregel:

Gemeente Den Haag

Ons kenmerk

BD/

Betrokkenen hebben het recht op informatie. Overweeg om betrokkenen meer informatie over de gegevensverwerking door de PGA-lokaal te geven in de notificatiebrief en/of de privacyverklaring op de website van de gemeente Den Haag uit te breiden met de informatie over de gegevensverwerking. Hierbij moet minimaal worden gedacht aan bovengenoemde thema's.

4.8 Cultuur

Inleiding

Zijn medewerkers zich bewust van het belang van het beschermen van privacygevoelige gegevens? Gaat iedereen even zorgvuldig om met de gegevens, worden betrokkenen goed geïnformeerd over hoe men moet omgaan met die gegevens?

Feiten & analyse

Privacy is een belangrijk thema binnen het proces van de PGA-lokaal.

Er worden trainingen of e-learnings over privacy of informatiebeveiliging georganiseerd voor (geselecteerde) medewerkers. Zo heeft een aantal medewerkers deelgenomen aan de training 'Gegevensverwerking bij het behandelen van casussen in het Zorg- en Veiligheidshuis' van het VLOT van de VNG. Binnenkort nemen een aantal medewerkers deel aan de leergang 'Privacy en gegevensdeling' van het VLOT. Een aantal medewerkers zal binnenkort deelnemen. Er worden af en toe lunchsessies georganiseerd waarbij de FG aanschuift om de bewustwording te vergroten. Dit heeft tot nu toe één keer plaatsgevonden en dit is meerdere jaren geleden. Er wordt echter gemeentebreed een bewustwordingscampagne uitgevoerd op het gebied van privacy. In dit kader worden activiteiten georganiseerd voor medewerkers van de gemeente om bewustwording te vergroten. De activiteiten in het kader van de bewustwordingscampagne worden in deze DPIA niet inhoudelijk beoordeeld.

Medewerkers worden gestimuleerd om een cleandesk policy te hanteren en om computerschermen te vergrendelen bij het weglopen van de werkplek. Na gebruik worden (fysieke) documenten opgeruimd in afgesloten (digitale) locaties. Er heerst een open aanspreekcultuur waarin medewerkers onderling verbeterpunten op het gebied van privacy en integriteit kunnen bespreken.

Risico's en maatregelen

Er zijn ten aanzien van het aspect *governance* geen risico's geïdentificeerd.

5. Advies en accordering

In het risico overzicht dat als bijlage aan deze rapportage is toegevoegd wordt weergegeven welke privacy risico's de verwerking met zich meebrengt, welke beheersmaatregelen hiervoor nodig zijn en welke acties hieraan gekoppeld zijn. Dit overzicht wordt bewerkt zodra beheersmaatregelen worden uitgevoerd en risico's gemitigeerd, zo blijft de DPIA up to date ook na het uitvoeren van beheers acties.

Aanbevelingen voor vervolg

Wij adviseren om de hierboven genoemde risico's als volgt aan te pakken:

1. Benoem een business eigenaar van ieder risico in het risico overzicht en de bijbehorende maatregelen.
2. Geef de business eigenaar de opdracht de maatregelen in te voeren en daarmee het risico te mitigeren.
3. Geef elke 2 maanden een status update van de opvolging van deze aanbevelingen aan de FG en de Privacy Officer.

Gemeente Den Haag

Ons kenmerk
BD/

Advies FG

[GEBRUIK DEZE RUIMTE VOOR HET ADVIES VAN DE FG]

Naam: [NAAM FG]

Datum: [DATUM]

Gemeente Den Haag

Ons kenmerk
BD/

Accordering

Deze DPIA is opgeleverd aan:

5.1.2.e	Cluster PGA	Functionaris Gegevensbescherming
Datum oplevering: 22-04-2021		Datum oplevering: 22-04-2021
Naam: 5.1.2.e		Naam: 5.1.2.e
Voor akkoord: [HANDTEKENING PROCESEIGENAAR]		Voor gezien: [HANDTEKENING FG]
Datum ondertekening: [DATUM]		Datum ondertekening: [DATUM]

Tekent voor gezien:

(Algemeen) Directeur [DIENST]
Datum oplevering: 22-04-2021
Naam: 5.1.2.e
Tekent voor gezien: [HANDTEKENING PROCESSEIGENAAR]
Datum ondertekening: [DATUM]

Bijlage A**A1. Documentatie**

De volgende documentatie is geraadpleegd.

Nr.	Documentnaam	Link
1	Convenant PGA lokaal versie 25 september 2020	

A2. Geïnterviewden

De volgende personen hebben meegewerkt tijdens de DPIA sessie.

Datum	Geïnterviewden	Functie/Rol
10 en 23 februari	5.1.2.e	5.1.2.e 5.1.2.e 5.1.2.e
10 en 23 februari	5.1.2.e	5.1.2.e
10 en 23 februari	5.1.2.e	5.1.2.e 5.1.2.e
		5.1.2.e
10 en 23 februari	5.1.2.e	5.1.2.e 5.1.2.e 5.1.2.e
		5.1.2.e
10 en 23 februari	5.1.2.e	5.1.2.e 5.1.2.e
10 en 23 februari	5.1.2.e	5.1.2.e 5.1.2.e 5.1.2.e
10 en 23 februari	5.1.2.e	5.1.2.e

1. Inleiding

De PGA lokaal is een werkwijze bedoeld om regie te voeren op casuïstiek op het gebied groepen of individuen die ernstige overlast, openbare orde of veiligheidsproblematiek veroorzaken. De casuïstiek wordt integraal behandeld door de samenwerkingspartners door het opstellen en uitvoeren van een persoonsgerichte aanpak.

Via de PGA lokaal wordt een platform geboden voor integrale casuïstiekbepreking, die nog geen opschaling naar het Zorg- en Veiligheidshuis behoeven, maar waarbij wel degelijk zorgen zijn over een groep of subject. De PGA lokaal staat los van het Zorg- en Veiligheidshuis, maar heeft een vergelijkbare doelstelling.

De PGA lokaal vindt plaats onder regie van de directie Veiligheid van de gemeente Den Haag. Het Cluster PGA, bestaande uit beleidsadviseurs (PGA-experts), werkt nauw samen met accounthouders. De gemeente Den Haag is verdeeld in drie politiedistricten (A, B, C). Aan elk van deze districten is een PGA-expert van het Cluster PGA van de directie Veiligheid van de gemeente Den Haag verbonden.

2. Advies

Als FG onderschrijf ik de DPIA. Er wordt gewezen op een verhoogd risico, omdat bijzondere persoonsgegevens worden verwerkt (politiegegevens en strafvorderlijke gegevens), die maakt dat de adviezen in deze DPIA met extra zorg moeten worden opgevolgd.

Daarnaast stelt de DPIA dat de gegevensverwerking binnen de PGA lokaal niet rechtmatig is, wegens het ontbreken van een juridische basis. Op dit punt wil ik apart ingaan.

Daarnaast wil ik nog de volgende adviezen toevoegen. Uit een bespreking op 28 september 2021 blijkt, dat een groot aantal van deze adviezen al is of wordt opgevolgd. De stukken waaruit dit blijkt, kunnen aan dit advies worden toegevoegd zodat een compleet overzicht ontstaat.

De situatie t.a.v. PGA Lokaal is vergelijkbaar met het HEIT, in die zin dat PGA Lokaal geen juridische status heeft, maar een samenwerkingsverband of overlegorgaan is.

- Vanuit privacy is de kernvraag op grond waarvan de deelnemende organisaties persoonsgegevens met elkaar mogen uitwisselen, met andere woorden wat de wettelijke grondslag voor de (verdere) gegevensverwerking is.
- Een tweede vraag is, of de gezamenlijke verwerkingsverantwoordelijkheid voldoende duidelijk is vormgegeven.

2.1 Voltooi het convenant alvorens de samenwerking te hervatten

De samenwerking in PGA lokaal is vrij recent ontstaan in juli 2020. De DPIA is echter niet voorafgaand aan de start van deze samenwerking uitgevoerd, maar nadat de samenwerking al in gang was gezet. De partners zijn eenieder zelfstandig verwerkingsverantwoordelijk voor de verwerking van persoonsgegevens waar het de uitoefening van hun eigen (publiekrechtelijke) taken binnen de

samenwerking betreft. De partners zijn gezamenlijk verwerkingsverantwoordelijk voor de verwerking van gegevens in samenwerkingsverband

O.a. vanuit het oogpunt van transparantie en de rechten van betrokkenen is het een groot probleem dat het Convenant als onvolledig wordt beoordeeld. Ik adviseer om de samenwerking in PGA lokaal pas te hervatten, wanneer het Convenant conform de adviezen uit de DPIA is aangevuld en ondertekend door de deelnemende partijen.

De DPIA somt de volgende tekortkomingen op: “In het convenant zijn geen afspraken gemaakt over de volgende thema’s: grondslag, categorieën persoonsgegevens die worden verwerkt, dataminimalisatie en wat partners doen bij een datalek (protocol datalekken). Informeel is dit laatste belegd bij de Functionaris Gegevensbescherming van de gemeente Den Haag.”

Ten aanzien van dit laatste punt adviseer ik na te gaan of binnen OOV in het algemeen en binnen PGA in het bijzonder voldoende duidelijk is wat een datalek is en welke procedure moet worden gevolgd.

Ook dient het convenant de afspraken met betrekking tot de gezamenlijke verwerkingsverantwoordelijkheid zoals bedoeld in artikel 26 AVG tot uitdrukking te brengen.

2.2 Verwerkingsverantwoordelijkheid en gezamenlijke verwerkingsverantwoordelijkheid

De directie Veiligheid wordt in de DPIA bestempeld als hoofdverwerkingsverantwoordelijke, omdat de directie Veiligheid het doel en de middelen van PGA lokaal bepaalt. Het is niet duidelijk wat juridisch de betekenis is van het begrip hoofdverantwoordelijke. Deze term kan beter vermeden worden. Het risico is dat de gemeente Den Haag ten onrechte juridisch een te grote rol toebedeeld krijgt. Een meer juiste omschrijving is dat de gemeente Den Haag de PGA faciliteert of optreedt als beheersorganisatie of iets dergelijks.

Artikel 26 AVG bepaalt dat gezamenlijke verwerkingsverantwoordelijken ervoor moeten zorgen dat hun respectievelijke verantwoordelijkheden transparant zijn voor de betrokkenen wier gegevens worden verwerkt. Omdat dit artikel ook bepaalt dat de betrokkene zijn rechten jegens elke verantwoordelijke kan uitoefenen, is het van belang dat duidelijke procedures worden vastgelegd voor het uitoefenen van de rechten van verantwoordelijke. Ook daarom is het van belang dat het convenant volledig is, voordat de samenwerking van start gaat.

Daarnaast adviseer ik OVV om een standaard-convenant te ontwikkelen, dat bij alle samenwerkingsvormen als uitgangspunt kan dienen. De samenwerkingsverbanden wisselen in grote lijnen dezelfde (persoons)gegevens uit voor vergelijkbare doelen. Aangezien het ZVH modeldocumenten aanbiedt, kunnen deze een goed uitgangspunt vormen.

2.3 Wet Gegevensverwerking Samenwerkingsverbanden (WGS)

De DPIA stelt dat op dit moment een grondslag voor gegevensverwerking binnen de PGA als zodanig ontbreekt en dat deze gegevensverwerking daarmee onrechtmatig is. Hierop past een nuancering. De PGA is geen zelfstandige juridische entiteit, maar moet worden beschouwd als een overlegstructuur. Binnen deze overlegstructuur moeten de ketenpartners telkens opnieuw per casus bezien en vastleggen of er een mogelijkheid bestaat voor verdere gegevensverwerking en hoever deze reikt, juist vanwege het ontbreken van zelfstandige bevoegdheden van de PGA.

Nu de PGA niet valt onder de WGS, blijft voor het delen van persoonsgegevens slechts de optie over, dat alle ketenpartners van hun eigen bevoegdheden gebruikmaken op grond van sectorale wetten. Een eventuele bevoegdheid tot het verder verwerken van persoonsgegevens zal dan ook in deze sectorale wetten moeten worden gevonden.

Dit betekent naar mijn mening niet dat alle gegevensverwerking door ketenpartners binnen de PGA per se onrechtmatig is. De rechtmatigheid van de gegevensverwerking dient echter wel per proces van tevoren te worden vastgesteld en vastgelegd. Deze conclusie sluit ook aan bij hetgeen hierover wordt gezegd in Handboek Privacy IKO infodesk (paragraaf 4.2.3.).

Daarnaast is van belang dat in de werkprocessen duidelijk wordt vastgelegd, dat uitsluitend noodzakelijke informatie wordt uitgewisseld en dit alleen met de voor de casus relevante partner(s).

2.4 Handboek privacy IKO infodesk

In het handboek privacy IKO infodesk is het proces PGA Lokaal niet beschreven. Als gevolg hiervan is niet duidelijk of in dit kader raadpleging van de Haagse Bron is geoorloofd. Het advies is om dit te onderzoeken en vast te leggen in het Handboek privacy IKO infodesk.

2.5 Ga voorlopig over op veilige communicatie totdat een zaaksysteem in gebruik genomen wordt

In de DPIA wordt benoemd dat communicatie tussen de partners plaatsvindt via Outlook en dat informatie wordt vastgelegd in excelsheets op de g-schijf. Advies is om per direct over te gaan op het gebruik van zorgmail en om bijlagen uitsluitend encrypted mee te sturen.

De DPIA adviseert om over te gaan op een zaaksysteem. Aanvullend hierop zou ik adviseren om een systeem te zoeken van waaruit door de deelnemende partijen kan worden gemaild en waar de deelnemende partijen toegang hebben tot de dossiers, zodat er geen bijlagen met persoonsgegevens meer hoeven te worden gemaild. Het zaaksysteem zou daarnaast de mogelijkheid moeten bieden om na een van te voren ingestelde bewaartermijn stukken automatisch te vernietigen. De bevindingen uit deze DPIA moeten het uitgangspunt vormen bij het selecteren van het zaaksysteem. Daarbij zou het de voorkeur verdienen om aan te sluiten bij het VIK zodat hier zoveel mogelijk processen op aan kunnen sluiten.

Totdat sprake is van een gedeeld zaaksysteem zullen alle partijen zelf invulling moeten geven aan hun eigen verwerkingsverantwoordelijkheid. Er wordt – terecht – aangegeven dat er voor het gehele proces daarnaast een gezamenlijke verwerkingsverantwoordelijkheid bestaat.

Bij andere onderdelen van OOV wordt de overgang voorbereid naar het VIK. In de DPIA wordt aangegeven dat voor PGA Lokaal momenteel een aanbesteding wordt georganiseerd voor een eigen systeem PGA-x. Ik adviseer duidelijk te motiveren waarom voor PGA Lokaal een apart systeem nodig is en een i-adviseur in te schakelen. Dit brengt immers extra kosten met zich mee, noodzaakt tot aparte beveiligingsmaatregelen en kan in de toekomst de samenwerking of het uitwisselen van informatie met andere onderdelen van OOV of de gemeente moeilijker maken.

2.6 Hanteer bewaar- en vernietigingstermijnen

Er wordt aangegeven dat na een melding een triage plaatsvindt die ertoe kan leiden dat wordt besloten dat een casus niet verder wordt behandeld in PGA lokaal. Advies aan de verantwoordelijke is om alsdan alle stukken – of in elk geval alle persoonsgegevens - over deze casus te vernietigen.

2.7 Evalueer de werkprocessen tussen nu en anderhalf jaar

Om na te gaan of de werkprocessen worden gevolgd en of zij voldoen aan de eisen van de AVG, is het belang om van tijd tot tijd een evaluatie uit te voeren. Ik adviseer om over ongeveer anderhalf jaar een representatieve steekproef te (laten) trekken uit de verschillende verwerkingen, deze te vergelijken met de vastgelegde werkprocessen en indien nodig aanpassingen door te voeren.

Naam: 5.1.2.e

Datum: 29-09-2021

DPIA rapportage gemeentesignalen

Versiebeheer

Versie	Datum	Wijzigingen	Wie
0.9	29-07-21	Oplevering concept	5.1.2.e
1.0	04-10-21	Oplevering definitieve versie	5.1.2.e
1.1	10-01-22	Aanpassing definitieve versie nav advies FG	5.1.2.e

Inhoudsopgave

1. Inleiding	3
<i>Aanleiding en onderwerp van de DPIA</i>	3
<i>Doelstelling</i>	3
<i>Scope</i>	3
<i>Opbouw van de analyse</i>	4
2. Managementsamenvatting	5
3. Beschrijving Verwerking	7
<i>Systematische beschrijving van het proces</i>	7
<i>Systematische beschrijving van de verwerking</i>	10
<i>Persoonsgegevens</i>	11
4. Analyse privacy consequenties	13
<i>Inleiding</i>	13
4.1 Governance	13
<i>Inleiding</i>	13
<i>Feiten & analyse</i>	13
<i>Risico's en maatregelen</i>	14
4.2 Grondslag & Doelbinding	16
<i>Inleiding</i>	16
<i>Feiten & analyse</i>	16
<i>Rechtmatigheid van de verwerking</i>	17
<i>Risico's en maatregelen</i>	17
4.3 Juistheid	19
<i>Inleiding</i>	19
<i>Feiten & Analyse</i>	19
<i>Risico's en maatregelen</i>	20
4.4 Dataminimalisatie	20

Inleiding.....	20
Feiten & Analyse.....	20
Risico's en maatregelen	21
4.5 Opslag.....	22
Inleiding.....	22
Feiten & Analyse.....	22
Risico's en maatregelen	22
4.6 Bescherming.....	24
Inleiding.....	24
Feiten & Analyse.....	24
Risico's en maatregelen	24
4.7 Transparantie.....	26
Inleiding.....	26
Feiten & Analyse.....	26
Risico's en maatregelen	26
4.8 Cultuur.....	28
Inleiding.....	28
Feiten & analyse.....	28
Risico's en maatregelen	28
5. Advies en accordering.....	30
Aanbevelingen voor vervolg	30
<i>Advies FG</i>	31
<i>Accordering</i>	32
Bijlage A.....	33
A1. Documentatie	33
A2. Geïnterviewden.....	33

1. Inleiding

Aanleiding en onderwerp van de DPIA

Vanuit het oogpunt van een zorgvuldige omgang met persoonsgegevens is de gemeente verplicht een DPIA uit te voeren voor verwerkingen die waarschijnlijk een verhoogd risico opleveren.

Voor het proces gemeentesignalen is vastgesteld dat een verhoogd risico voor betrokkenen bestaat. Er worden namelijk signalen met daarin persoonsgegevens van gevoelige aard gedeeld tussen verschillende diensten van de gemeente en mogelijk gedeeld met externe partijen, zoals de politie, de AVIM, het RIEC of het ISZW. Deze gegevensverwerking levert daarmee waarschijnlijk een verhoogd privacyrisico op.

Een DPIA is een middel om in kaart te brengen welke persoonsgegevens in een proces, systeem of organisatie verwerkt worden en wat hiervan de risico's voor betrokkenen zijn. Op donderdag 22 juli 2021 is een DPIA-workshop gehouden om de benodigde informatie hiervoor op te halen. In Bijlage A is opgenomen wie aan deze bijeenkomst hebben deelgenomen. Dit rapport is het resultaat van deze DPIA.

Doelstelling

Deze DPIA rapportage schetst de eventuele privacy risico's van de onderhavige gegevensverwerking, en maatregelen die kunnen worden getroffen teneinde deze risico's te mitigeren.

In de DPIA wordt vooral gekeken naar de geplande maatregelen, waarborgen en mechanismen om de risico's te beperken, de persoonsgegevens te beschermen en aan te tonen dat aan de beginselen voor verwerking uit de AVG is voldaan. Deze DPIA is een momentopname. Bij nieuwe ontwikkelingen zoals wijzigingen in wetgeving, verandering van processen, inzet van nieuwe technologie e.d. moet de DPIA worden herhaald. Ook dienen uitgevoerde DPIA's periodiek te worden herijkt (iedere 3 jaar).

Scope

Deze DPIA wordt uitgevoerd ten aanzien van gegevensverwerkingen in het proces gemeentesignalen. Het gaat daarbij om het ontvangen, routeren en verrijken van gemeentesignalen. Daarnaast valt binnen scope van deze DPIA het casusoverleg tussen afgevaardigden van aan een casus deelnemende diensten van de gemeente, waarin acties worden belegd en de monitoring daarvan plaatsvindt. Binnen de scope is ook het systeem PGA-x waarin het proces gemeentesignalen wordt geïmplementeerd.

Het Bibob- en het gemeentesignalen proces worden behandeld in een afzonderlijke DPIA en zijn geen onderdeel van deze DPIA.

In sommige gevallen wordt in dit proces gebruik gemaakt van de reguliere voorzieningen van de Gemeente (netwerk, fysieke werkplek, inlogvoorziening). Waar het centrale proces van de

Gemeente wordt gevolgd, zijn deze geen onderdeel van de DPIA. In dat soort gevallen wordt duidelijk vermeld dat deze buiten scope van deze DPIA blijven.

Opbouw van de analyse

Dit document schetst de privacy risico's binnen bovengenoemde scope en de te nemen maatregelen die het betreffende risico kunnen mitigeren.

De uitvoering van deze DPIA verloopt via de zes beginselen waaraan elke verwerking moet voldoen. Deze zes beginselen zijn Juistheid, Data minimalisatie, Opslag, Bescherming, Transparantie en Grondslag & doelbinding. Daarnaast zijn ook de thema's 'Governance' en 'Privacycultuur' van belang.

Deze beginselen vormen de basis voor de uitvoering van deze analyse. Per thema worden eventuele risico's geanalyseerd en wordt de impact van deze risico's op de betrokkenen en de gemeente ingeschat. Daarnaast worden maatregelen die de eigenaar van de verwerking kan treffen om de risico's tot een acceptabel niveau terug te brengen beschreven. Hierbij wordt rekening gehouden met de haalbaarheid en maakbaarheid van deze maatregelen binnen de context van de gemeente. De eventuele acceptatie van risico's of restrisico's is de verantwoordelijkheid van de eigenaar van de verwerking.

Voor elk van de thema's zijn risico's geïnventariseerd die voor het onderhavige onderwerp relevant kunnen zijn voor de gegevensbescherming binnen de gemeente. De aanwezige deelnemers aan de workshop hebben tijdens het uitvoeren van de risicoanalyse de belangrijkste risico's benoemd en geclassificeerd volgens de onderstaande tabel.

Figuur 1

		Impact →		
		Laag	Midden	Hoog
↑ Kans	Hoog			
	Midden			
	Laag			

2. Managementsamenvatting

Wat zijn de belangrijkste (M-H) risico's die in de analyse zijn geconstateerd? Welke maatregelen zijn hierbij van toepassing.

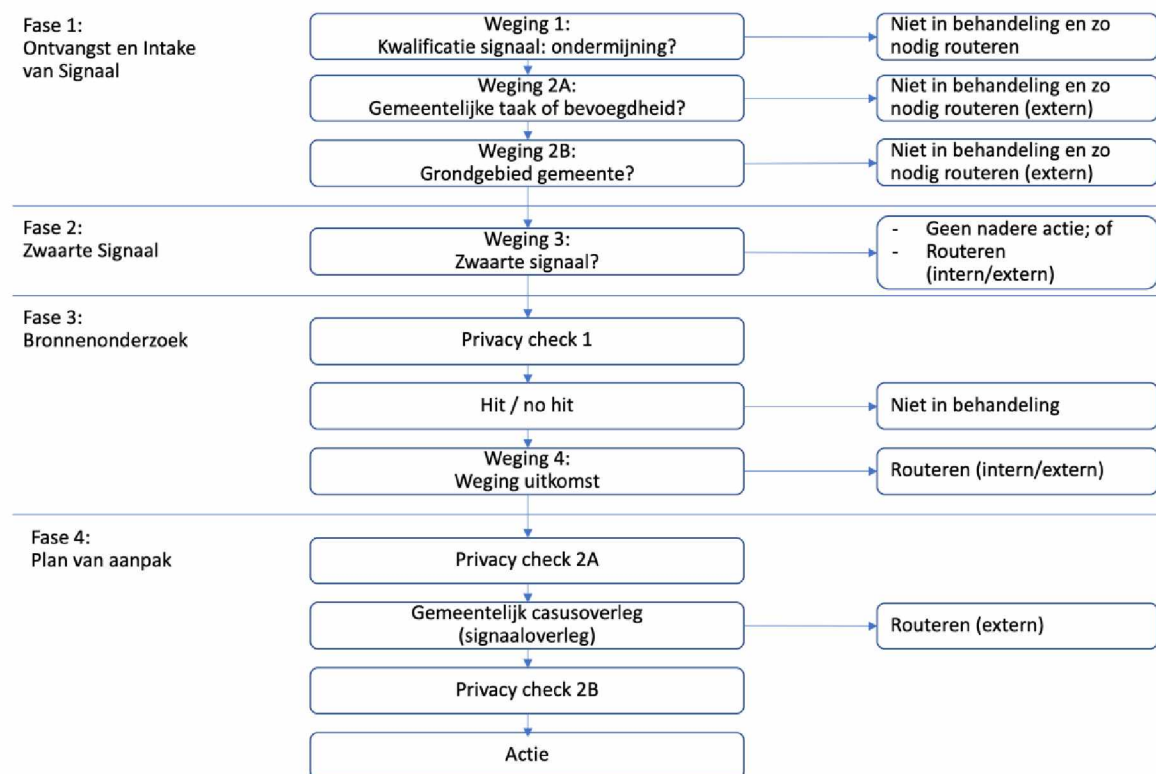
Beginnel	Risico	Classificatie (L-M-H)	Maatregel (mogelijk)
Governance	Er zijn geen goede inhoudelijke afspraken gemaakt over de passende omgang met (persoons-)gegevens met ^{5.1.2.f} , waardoor er onvoldoende waarborgen zijn dat zorgvuldig met gegevens wordt omgegaan.	M	Er moet zo snel mogelijk en uiterlijk voor de ingebruikname van PGA-x een overeenkomst met ^{5.1.2.f} worden gesloten. Lukt dit niet? Zorg dan dat alle onderstaande afspraken op een andere manier worden geborgd. In de verwerkersovereenkomst moet in ieder geval het volgende worden vastgelegd: algemene beschrijving, instructies, geheimhoudingsplicht, beveiliging, subverwerkers, privacy rechten, gegevens verwijderen en audits. Zorg er daarnaast voor dat er een mechanisme wordt gevonden waarbij structureel en periodiek wordt gestuurd op de nakoming en effectiviteit van deze maatregel.
Governance	Medewerkers herkennen datalekken niet.	M	Organiseer een specifieke datalektraining voor iedere medewerker, inclusief spoorhouders, in dit proces (of directie breed). Zorg ervoor dat in deze training wordt stilgestaan bij het herkennen en melden van beveiligingsincidenten en datalekken.
Governance	Te weinig capaciteit en competenties beschikbaar voor privacy ondersteuning waardoor aandachtspunten en issues niet tijdig worden opgepakt.	M	Draag zorg voor een vaste privacy officer, met voldoende kennis en ervaring van privacy- en gerelateerde wetgeving, die de medewerkers structurele ondersteuning kan bieden, privacy kaders kan stellen en toezicht kan houden op de gegevensverwerking. Afhankelijk van het takenpakket wordt geadviseerd om minimaal 0.6 fte beschikbaar te stellen voor de privacy officer van de directie Veiligheid. Het is belangrijk dat het verantwoordelijke managementniveau binnen de gemeente wordt geïnformeerd over deze noodzaak.
Governance	Verwerking niet opgenomen in het register van verwerkingsactiviteiten	L	Voeg deze verwerking toe aan het register van verwerkingsactiviteiten in iNavigator. De privacy officer kan

	waardoor niet wordt voldaan aan verantwoordingsplicht.		hierover adviseren. Het is bijvoorbeeld belangrijk dat er een duidelijke beschrijving van de grondslag en het doel van de verwerkingsactiviteit wordt vastgelegd (en goedgekeurd).
Grondslag & doelbinding	Spoorhouders weten niet altijd of ze gegevens mogen delen met de IKO-medewerker, hierdoor bestaat het risico dat er geen of meer gegevens gedeeld worden dan noodzakelijk.	M	Zorg dat de kaders voor de gegevensuitwisseling bekend zijn bij de spoorhouders (of ondersteunende privacy officers). Daarnaast moet de RIEC-liaison alle irrelevante gegevens afkomstig van spoorhouders verwijderen of anonimiseren, voordat de gegevens worden gedeeld met het RIEC. 5.1.2f heeft tijdens de workshop aangegeven dat er een e-learning ontwikkeld kan worden voor gebruikers van PGA-x over privacy en gegevensbescherming in het kader van ondermijning. Beoordeel en overweeg de privacy module in PGA-x te implementeren en zorg ervoor dat medewerkers deze uitvoeren voordat zij aan de slag gaan met het systeem.
Transparantie	Betrokkenen worden onvoldoende geïnformeerd	M	Informeer betrokkenen over de gegevensverwerking. Het uitgangspunt is dat betrokkenen zo snel en volledig mogelijk worden geïnformeerd. Dit is in het kader van het onderzoek niet altijd mogelijk. De algemene informatievoorziening aan de burger kan wel worden verbeterd, bijvoorbeeld bij het in eerste instantie verzamelen van gegevens bij de betrokkene. Tijdens interventies kan er een flyer worden uitgedeeld waarin betrokkene wordt geïnformeerd. Pas de privacyverklaring van de gemeente Den Haag aan. Neem een onderdeel op over de IKO-infodesk. Vul deze ook aan met andere verplichte informatie.
Cultuur	Er is te weinig aandacht voor privacy geweest waardoor medewerkers onvoldoende getraind zijn in het herkennen van privacy risico's in dit proces	M	Train medewerkers in het herkennen van privacy risico's. Besteed meer aandacht aan de bewustwording van medewerkers op het gebied van privacy.

3. Beschrijving Verwerking

Dit hoofdstuk beschrijft het onderhavige proces en de verwerkingen van persoonsgegevens. De beschrijving van het proces en het inventariseren van de verwerkingen van persoonsgegevens zijn onderdeel geweest van de DPIA-workshop.

Systematische beschrijving van het proces



Het proces start met de binnenkomst van een signaal bij de IKO-Infodesk. Dit signaal kan afkomstig zijn van burgers of organisaties uit een verscheidenheid aan bronnen, zoals:

- Meld Misdaad Anoniem-meldingen;
- Via de Meld een Vermoeden applicatie;
- 5.1.2.e @denhaag.nl;
- Via een binnengemeentelijk signaal: een melding van een van de spoorhouders, iemand anders binnen de gemeente die zijn/haar weg richting de spoorhouders niet wist te vinden of via de RIEC-Liaison.

Het signaal wordt bij binnenkomst geregistreerd in PGA-x.¹ Er zijn op dit moment nog geen afspraken gemaakt over welke gegevens van het signaal standaard in PGA-x worden geregistreerd. Het is ook nog niet bekend of overbodig beoordeelde informatie (zoals bepaalde documenten) wordt verwijderd of wordt opgeslagen voor rapportagedoeleinden.

De signalen komen in volgorde van binnenkomst terecht op het centrale dashboard in PGA-x. Op dit dashboard is tevens te zien welke signalen open staan en welke zijn gesloten.

Na de ontvangst van het signaal kan het proces worden ingedeeld in vier fases:

1. De ontvangst en de intake van het signaal
2. Het bepalen van de zwaarte & toewijzing van het signaal
3. Het verrijken van de melding via een bronnenonderzoek
4. Het opstellen van een plan van aanpak om het signaal te behandelen

Fase 1: de ontvangst en intake van het signaal

Na de binnenkomst van het signaal wordt allereerst overgegaan tot registratie en het kwalificeren ervan. Dit houdt in dat er wordt getoetst of het signaal ziet op ondermijning. Voor het bepalen of hiervan sprake is wordt gebruik gemaakt van een vooraf gedefinieerde checklist.¹ Er is sprake van ondermijning wanneer het signaal kwalificeert als georganiseerde of zware criminaliteit, waarbij misbruik wordt gemaakt van een overheidsinstantie (strafrechtelijke handhaving), of wanneer het signaal ziet op misbruik van gemeentelijke voorzieningen en faciliteiten (bestuursrechtelijke handhaving).

Wanneer geoordeeld is dat er geen sprake is van ondermijning, dan wordt het signaal afgesloten en eventueel teruggestuurd naar de melder, of naar een andere afdeling van de gemeente gerouteerd. De niet te kwalificeren signalen worden maximaal 1 jaar bewaard in PGA-x en vervolgens automatisch verwijderd. Het routeren naar een andere afdeling of gemeente kan zowel via PGA-x, als buiten PGA-x om. In het geval het signaal gerouteerd wordt naar een afdeling met een spoorhouder die toegang heeft tot PGA-x, zal dit via PGA-x gebeuren. Andere gemeenten die geen PGA-x gebruiken, ontvangen het signaal via een andere weg.

In het geval er is geoordeeld dat er inderdaad sprake is van ondermijning, wordt een volgende controle uitgevoerd. Er wordt gecontroleerd of het signaal valt binnen de bevoegdheid en het grondgebied van de gemeente Den Haag. Wanneer dit niet het geval is en het signaal bijvoorbeeld valt onder de bevoegdheid van de politie of onder het grondgebied van een andere gemeente, dan wordt het signaal niet in behandeling genomen en gerouteerd naar de bevoegde partij.

Wanneer is besloten dat er daadwerkelijk sprake is van ondermijning en dit onder het grondgebied en verantwoordelijkheid valt van de gemeente Den Haag, wordt het signaal in behandeling genomen. Het signaal wordt verrijkt met gegevens uit vier openbare bronnen: de Basisregistratie Personen (BRP), het Handelsregister, de Basisregistratie Kadaster (BRK) en het register van de Kamer van Koophandel (KvK).

¹ § 4.2.2 Handboek Privacy IKO Infodesk

Het raadplegen van bovengenoemde bronnen vindt plaats via een koppeling in PGA-x (HaalCentraal). Via deze koppeling kunnen de bronnen worden geraadpleegd. De raadpleging van de bronnen wordt daarnaast centraal gelogd door PGA-x.

Fase 2: het bepalen van de zwaarte & toewijzing van het signaal

Nadat het signaal is ontvangen en in PGA-x is gezet, gaat men over tot het bepalen van de zwaarte van het signaal. Hiervoor zijn geen vastgestelde procedures aanwezig, dit gebeurt aan de hand van de professionele inschatting en afweging van de betreffende medewerker.

Factoren waarnaar de medewerker kan kijken bij het beoordelen van de zwaarte van het signaal zijn bijvoorbeeld de beschrijving van het signaal (is het voldoende concreet?) of de leeftijd van het signaal (is het signaal van een recente datum?). Bijlage 1 van het Model privacy protocol bevat ook een checklist ten behoeve van de signaalanalyse.

Na het beoordelen van de zwaarte van het signaal zijn er een viertal opties:

1. Het signaal is gemeente overstijgend. In dat geval wordt het signaal gerouteerd naar een samenwerkingsverband zoals het RIEC of HEIT.
2. Het signaal is dermate zwaar dat strafrechtelijke vervolging is aangewezen, boven bestuursrechtelijke handhaving. Er vindt dan routing plaats naar een partij buiten de gemeente, zoals bijvoorbeeld de Politie of kinderscherming.
3. Een monodisciplinaire aanpak van het signaal volstaat. Het signaal wordt in dat geval aan een spoorhouder gekoppeld.
4. Er volgt een vervolganalyse, waarmee fase 3 ingaat.

Na bovenstaande classificering wordt het signaal gerouteerd (bij optie 1, 2 of 3), of het signaal blijft bij de IKO-medewerker (optie 4). De IKO medewerkers en de spoorhouders werken in PGA-x.

Fase 3: het verrijken van de melding via een bronnenonderzoek

In fase 3 bepaalt de privacy officer of en zo ja welke gemeentelijke bronnen naar aanleiding van het concrete signaal door de spoorhouders kunnen worden geraadpleegd. Dit betreft de 'privacy check 1'. Het raadplegen van de bronnen gebeurt door de spoorhouders middels een hit/no hit- vraag: wanneer voor het signaal relevante gegevens voorkomen in de bronnen, is er sprake van een 'hit' of meerdere 'hits'. De betrokken persoon is in dat geval bekend binnen het gemeentelijke domein. Wanneer dit niet het geval is, is er sprake van een 'no hit' en wordt het signaal niet in behandeling genomen. Het signaal wordt afgesloten en verdwijnt uit de werkvoorraad.

In theorie bepaalt de privacy officer vervolgens of de hits het signaal in voldoende mate bevestigen om door te gaan met het onderzoek en welke informatie afkomstig uit de hits relevant is voor het signaal. In de praktijk wordt dit gedaan door de IKO-medewerker. Hierna vindt er een beoordeling plaats van de informatie. Uit deze beoordeling kunnen een drietal opties volgen:

1. Er wordt overgegaan tot een mono- of multidisciplinaire aanpak door één gemeentelijk onderdeel of meerdere samenwerkende gemeentelijke onderdelen.
2. Het signaal wordt doorgeleid naar het RIEC-samenwerkingsverband.

3. Het signaal wordt doorgestuurd naar het gemeentelijk casusoverleg (signaaloverleg) met de gemeentelijke onderdelen waar sprake is van een relevante hit. Hier wordt vervolgens een plan van aanpak opgesteld (fase 4).

Voordat het gemeentelijke casusoverleg plaatsvindt bepaalt de privacy officer (in theorie) in 'privacy check 2A' welke verzamelde gegevens met de relevante, bij het signaal betrokken, gemeentelijke onderdelen mogen worden gedeeld ten behoeve van de vaststelling van de verdere aanpak en welke binnengemeentelijke gegevensuitwisseling nodig is voor het verwezenlijken van die aanpak. In de praktijk wordt deze beoordeling uitgevoerd door de IKO-medewerker.

Fase 4: Het opstellen van een plan van aanpak om het signaal te behandelen

Tijdens het gemeentelijk casusoverleg wordt een plan van aanpak opgesteld. Dit bestaat uit een plan van interventies en acties voor de spoorhouders. In het plan van aanpak is tevens het gewenste resultaat vastgesteld. De privacy officer wordt na het opstellen van het plan van aanpak geraadpleegd. De privacy officier dient dan vast te stellen welke gegevens de interventieplegers mogen gebruiken om de interventies te onderbouwen. Dit is de 'privacycheck 2B'. De privacy officer beoordeelt met andere woorden of de gegevensset rechtmatig gebruikt mag worden. In de praktijk wordt deze beoordeling uitgevoerd door de IKO-medewerker.

Na het casusoverleg en het beleggen van acties en interventies, kan er alsnog besloten worden om het signaal extern te routeren, of om er een externe partij bij te betrekken.

Systematische beschrijving van de verwerking

Onderstaand een schematische weergave van de persoonsgegevens. Wat ontvang je (wat krijg je), wat verwerk je (wat doe je ermee) en wat verstrek je (wat geef je door).

Wat krijg je	Van wie	Hoe
Signaal: • Vrije invulvelden • Algemene persoonsgegevens • Bijzondere persoonsgegevens	Burgers, organisaties en professionals	Meld een vermoeden applicatie, mailbox IKO, meld misdaad anoniem, spoorhouders, overige personen binnen de gemeente

Wat doe je ermee	Middelen	Wie
Verrijken van het signaal in open bronnen	HaalCentraal via API Gateway in PGA-x	IKO-medewerker
Verrijken van het signaal in gesloten bronnen	Bronstelsel/spoorhouder	IKO-medewerker

Wat geef je door	Aan wie	Hoe
Signaal	Spoorhouders	Via PGA-x

Signaal	Extern	E-mail, PGA-x
---------	--------	---------------

Persoonsgegevens

Wij hanteren de classificatie zoals weergegeven in onderstaande figuur om te bepalen welke persoonsgegevens worden verwerkt. Er wordt onderscheid gemaakt tussen weinig gevoelige gegevens (algemene persoonsgegevens), door de aard of context extra gevoelige gegevens (gevoelige persoonsgegevens) en zeer gevoelige gegevens die wettelijk extra beschermd zijn (bijzondere persoonsgegevens). Al naar gelang de situatie kunnen gegevens in verschillende categorie worden geplaatst.



Binnen de scope van deze DPIA worden de volgende categorieën van persoonsgegevens verwerkt:

	Algemeen	Gevoelig	Bijzonder
Vaste velden	• Geen	• Geen	• Geen
Open/ Ongestructu- reerde velden	<i>Subjectgegevens:</i> • <i>NAW gegevens</i> • <i>Geboortedatum</i> • <i>Onroerend goed</i> • <i>Telefoonnummer</i> <i>Gegevens over rechtspersoon:</i> • <i>KvK-nummer</i>	• Casusbeschrijving	• Foto's (mogelijk) • BSN

Ons kenmerk
BD/

	• <i>Adresgegevens</i> • <i>Handelsnaam</i> • <i>Rechtsvorm</i> • <i>DGA</i> • <i>Nevenvestigingen</i> <i>(en andere adresgegevens)</i> <i>Locaties (bijvoorbeeld gebouwen van subject)</i>		
--	---	--	--

4. Analyse privacy consequenties

Inleiding

Dit hoofdstuk beschrijft de resultaten uit de uitgevoerde DPIA per thema. Voor ieder thema geven we een korte toelichting en beschrijven wij de risico's, de impact van de risico's op de betrokkenen en de gemeente en de maatregelen die de gemeente kan treffen om de risico's tot een acceptabel niveau terug te brengen. Daarnaast worden ook de ethische aspecten die mogelijk spelen in dit hoofdstuk besproken.

4.1 Governance

Inleiding

Is helder wie de verantwoordelijke en de verwerker zijn en hoe wordt toegezien op een adequate bescherming van persoonsgegevens? Is er beleid gemaakt ten aanzien van privacy en wordt er intern gecontroleerd op naleving van dit beleid? Is duidelijk wie binnen de organisatie verantwoordelijk is voor privacy?

Feiten & analyse

De gemeente Den Haag wordt aangemerkt als verwerkingsverantwoordelijke voor de persoonsgegevens die zij verwerken in de uitoefening van hun publiekrechtelijke taken en bevoegdheden.

Het Model privacy protocol voor binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijning, zoals vastgesteld door de Tweede Kamer, heeft als basis gediend voor het gemeentesignalen proces, zoals dat door de gemeente Den Haag geïmplementeerd zal worden in het zaakstelsel PGA-x. Dit model is op enkele punten aangepast op basis van lokale omstandigheden zoals de lokale situatie, de concrete organisatorische structuur van de gemeente en aanvullend beleid.

Binnenkort wordt PGA-x in gebruik genomen. De leverancier van dit zaakstelsel is ^{5.1.2.f} treedt op als verwerker voor de directie Veiligheid van de gemeente Den Haag. Er is nog geen verwerkersovereenkomst gesloten waarin afspraken worden gemaakt met de directie Veiligheid over de kaders van de gegevensverwerking.

^{5.1.2.f} maakt gebruik van een subverwerker: ^{5.1.2.f} ^{5.1.2.f}

Er is een gemeentebreed privacybeleid aanwezig. De ontwikkeling van dit beleid is pril en staat nog in de kinderschoenen, volgens de privacy officer van BSD. Het beleid bevat voornamelijk algemene privacy-uitgangspunten. De rollen en verantwoordelijkheden zijn nog niet beschreven in het beleid. Het gemeentebreed privacy beleid is geen onderdeel van deze DPIA. Wij hebben daarom geen kennisgenomen van dit document. Het is belangrijk dat hier op centraler niveau binnen de gemeente aandacht aan wordt besteed.

Er is een gemeentebreed datalekprotocol aanwezig. Het proces gemeentesignalen betreft een nieuw proces, er is daarom nog geen ervaring met datalekken. De IKO-medewerkers hebben

geen training gehad over beveiligingsincidenten en datalekken. Tijdens de workshop werd aangegeven dat meer bewustwording over dit thema wenselijk is.

De gemeente houdt een register van verwerkingsactiviteiten bij in iNavigator. Het gemeentesignalen proces is niet hierin opgenomen.

Er is een privacy officer aangesteld binnen BSD. De privacy officer vervult een interimfunctie en heeft weinig beschikbare fte voor deze rol. Er is daardoor weinig gelegenheid voor IKO-medewerkers om vragen te stellen over privacy en gegevensbescherming. De gemeente heeft ook een FG aangesteld om toezicht te houden op de naleving van de AVG en gerelateerde wetgeving.

Risico's en maatregelen

Op basis van de analyse op het aspect *governance* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Er zijn geen goede inhoudelijke afspraken gemaakt over de passende omgang met (persoons-)gegevens met 5.1.2.f 5.1.2.f waardoor er onvoldoende waarborgen zijn dat zorgvuldig met gegevens wordt omgegaan

Er is momenteel nog geen verwerkersovereenkomst afgesloten met de leverancier van PGA-x, 5.1.2.f. Zowel de gemeente als de leverancier zijn echter verplicht om de (voorgenomen) verwerking te regelen in (bijvoorbeeld) een verwerkersovereenkomst. Contractuele afspraken omtrent de verwerking van persoonsgegevens ontbreken. De gemeente kan daardoor niet aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.

Maatregel

Er moet zo snel mogelijk en uiterlijk voor de ingebruikname van PGA-x een overeenkomst met 5.1.2.f worden gesloten. Lukt dit niet? Zorg dan dat alle onderstaande afspraken op een andere manier worden geborgd. In de verwerkersovereenkomst moet in ieder geval het volgende worden vastgelegd: algemene beschrijving, instructies, geheimhoudingsplicht, beveiliging, subverwerkers, privacy rechten, gegevens verwijderen en audits. Zorg er daarnaast voor dat er een mechanisme wordt gevonden waarbij structureel en periodiek wordt gestuurd op de nakoming en effectiviteit van deze maatregel.

Risico: Medewerkers herkennen datalekken niet

Medewerkers hebben geen training gehad waarin is stilgestaan bij beveiligingsincidenten en datalekken. Daardoor kunnen medewerkers datalekken niet direct herkennen. Indien datalekken niet worden herkend, kunnen ze ook niet worden opgelost en afgehandeld. Dit zorgt voor een blijvend risico op datalekken.

Maatregel

Organiseer een specifieke datalektraining voor iedere medewerker, inclusief spoorhouders, in dit proces (of directie breed). Zorg ervoor dat in deze training wordt stilgestaan bij het

herkennen en melden van beveiligingsincidenten en datalekken. Maak hierbij gebruik van het gemeentebrede datalekprotocol.

Risico: Te weinig capaciteit en competenties beschikbaar voor privacy ondersteuning waardoor aandachtspunten en issues niet tijdig worden opgepakt

In het proces gemeentesignalen is een belangrijke rol weggelegd voor de privacy officer. De privacy officer is, als hoeder van de persoonsgegevens, verantwoordelijk voor het ondersteunen van IKO-medewerkers bij het maken van belangrijke privacy afwegingen om te voorzien in een proportionele aanpak. Op dit moment is er een privacy officer aangesteld bij BSD. De privacy officer heeft echter onvoldoende fte beschikbaar om medewerkers in het proces gemeentesignalen te ondersteunen. Daarnaast is het onduidelijk of de privacy officer over de juiste kennis en ervaring beschikt om deze afwegingen te maken. Zonder structurele ondersteuning worden de juiste privacy-vragen niet gesteld, waardoor de rechtmatigheid van de verwerking niet geborgd is.

Voorgestelde maatregel

Draag zorg voor een vaste privacy officer, met voldoende kennis en ervaring van privacy- en gerelateerde wetgeving, die de medewerkers structurele ondersteuning kan bieden, privacy kaders kan stellen en toezicht kan houden op de gegevensverwerking. Afhankelijk van het takenpakket wordt geadviseerd om minimaal 0.6 fte beschikbaar te stellen voor de privacy officer van de directie Veiligheid. Het is belangrijk dat het verantwoordelijke managementniveau binnen de gemeente wordt geïnformeerd over deze noodzaak.

Risico: Verwerking niet opgenomen in het register van verwerkingsactiviteiten waardoor niet wordt voldaan aan verantwoordingsplicht

De verwerking is niet opgenomen in het gemeentebrede register van verwerkingsactiviteiten. De vastlegging en beschrijving van doel en grondslag voor de verwerkingsactiviteit ontbreekt daarom. De AVG verplicht de gemeente om een register van verwerkingsactiviteiten bij te houden. Dit is noodzakelijk om aantoonbaar te maken dat een verwerking aan de eisen uit de AVG voldoet. Het bijhouden van een register draagt daarom bij aan het waarborgen van de privacy van betrokkenen. Het is tevens noodzakelijk in het kader van de verantwoordingsplicht van de gemeente.

Maatregel

Voeg deze verwerking toe aan het register van verwerkingsactiviteiten in iNavigator. De privacy officer kan hierover adviseren. Het is bijvoorbeeld belangrijk dat er een duidelijke beschrijving van de grondslag en het doel van de verwerkingsactiviteit wordt vastgelegd (en goedgekeurd door het juiste managementniveau).

4.2 Grondslag & Doelbinding

Inleiding

Het moet helder zijn wat het doel van de gegevensverzameling is, op het moment dat de gemeente deze verzamelt. Het doel moet ook in overeenstemming zijn met de normale werkzaamheden van de gemeente en onderbouwd zijn door één of meer wettelijke grondslagen.²

Feiten & analyse

Het proces gemeentesignalen heeft als doel een bestuurlijke en geïntegreerde aanpak van ondermijning. Zoals eerder gedefinieerd in fase 1 van de systematische beschrijving van het proces is er sprake van ondermijning wanneer het signaal kwalificeert als georganiseerde of zware criminaliteit, waarbij misbruik wordt gemaakt van een overheidsinstantie (strafrechtelijke handhaving), of wanneer het signaal ziet op misbruik van gemeentelijke voorzieningen en faciliteiten (bestuursrechtelijke handhaving).

Georganiseerde ondermijnende criminaliteit start, wordt ondersteund en in stand gehouden met ondermijnende activiteiten. De gemeente heeft in de aanpak van ondermijning een belangrijke rol. Burgers en organisaties melden onrechtmatige zaken vaak bij de gemeente. De gemeente fungeert daarmee als een soort toegangspoort en heeft een signaalfunctie. Niet alle signalen die de gemeente ontvangt van ondermijnende criminaliteit passen echter binnen een georganiseerd criminaliteitsverband, zoals het RIEC. Desalniettemin kunnen deze signalen relevant zijn voor de gemeentelijke taakuitvoering. Door de verwevenheid van onder- en bovenwereld is het namelijk mogelijk dat de gemeente onbewust ondermijnende activiteiten faciliteert middels subsidies, vergunningen, uitkeringen etc. Dit tast de integriteit van de gemeente aan en creëert malafide economische machtsposities.

De gemeente heeft uiteenlopende publiekrechtelijke taken en bevoegdheden die van belang zijn om ondermijnende activiteiten in kaart te brengen en vroegtijdig te kunnen signaleren en interveniëren. De gemeente kan bijvoorbeeld verschillende bestuursrechtelijke instrumenten inzetten om barrières op te werpen tegen ondermijnende activiteiten om deze te voorkomen of verminderen.

De grondslag voor de verwerking van persoonsgegevens is artikel 6 lid 1 sub e AVG. 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 (de gemeente) is opgedragen. De rechtsgrondslag moet dan zijn vastgelegd in het Unierecht of nationaal recht. Artikel 172 Gemeentewet belast de burgemeester met de handhaving van de openbare orde onder gewone omstandigheden. Dit is van direct belang voor de aanpak van ondermijning, bijvoorbeeld doordat de burgemeester de bevoegdheid heeft om een pand te doen sluiten bij verstoring van de openbare orde of drugshandel. Daarnaast zijn er bevoegdheden in de handhaving van de openbare orde en

² De wettelijke grondslag is de rechtvaardiging om persoonsgegevens te mogen verwerken, zoals bedoeld in artikel 6 lid 1 e.v. van de Algemene Verordening Gegevensbescherming. De wettelijke grondslagen uit dit artikel zijn; toestemming, ter uitvoering van een overeenkomst, wettelijke plicht, vitale belang, taak van algemeen belang en het gerechtvaardigd belang.

veiligheid die niet specifiek aan de burgemeester, maar bij andere organen van de gemeente zijn belegd.

De wettelijke basis voor het handhavend optreden van de gemeente is verder uitgewerkt in specifieke wet- en regelgeving, zoals bijvoorbeeld de Gemeentewet en de Drank- en horecawet. Deze verschillende specifieke wettelijke grondslagen zijn nader uiteengezet in bijlage B, welke is bijgevoegd aan deze rapportage.³

De specifieke wet- en regelgeving bevat (in veel gevallen) ook specifieke artikelen over de te nemen bestuurlijke maatregelen (vergunningen intrekken, uitkeringen terugvorderen, panden sluiten, personen weren). De gemeentelijke bevoegdheden in specifieke wetgeving concretiseren daarom de meer algemene openbare orde bevoegdheid van de burgemeester in de Gemeentewet. Daarmee bieden zij ook een (mogelijke) grondslag voor de verwerking van persoonsgegevens ten behoeve van de aanpak van ondermijning.

De gemeente zal de grondslag ook (intern) moeten onderbouwen en vastleggen (zie risico onder Governance).

Persoonsgegevens die verzameld worden in dit proces worden ook voor andere (verenigbare) doeleinden gebruikt. Deze zijn:

- Het maken van rapportages in PGA-x. Er kunnen twee soorten rapportages beschikbaar worden gesteld.
 - Een fast-report tool op persoonsniveau of geaggregeerd niveau. Deze rapportages kunnen alleen bekeken worden door geautoriseerde gebruikers en kunnen geëxporteerd worden. De export functie wordt gelogd.
 - Er kunnen gegevens beschikbaar gesteld worden voor Index-rapportages aan de gemeente Den Haag. Voor deze functie heeft de gemeente Den Haag niet gekozen.
- Een gemeentesignaal kan als trigger dienen voor het Bibob en/of RIEC-liaison proces. Relevante informatie wordt gedeeld met de behandelaar. Het is onbekend of de overdracht via PGA-x kan plaatsvinden.

Rechtmatigheid van de verwerking

Op basis van de analyse valt te stellen dat de verwerking rechtmatig is, mits de beschikbare kaders worden nageleefd en juist geïnterpreteerd.

Risico's en maatregelen

Op basis van de analyse op het aspect *grondslag en doelbinding* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Aandachtspunten:

- Bij het verder verwerken van persoonsgegevens, verzameld in de uitoefening van bevoegdheden op grond van specifieke wet- en regelgeving, ter bestrijding van

³ Gebaseerd op het model privacy protocol binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijning

ondermijning, zal telkens beoordeeld moeten worden of aan het doelbindingsprincipe uit artikel 5 lid 1 sub b en 6 lid 4 AVG wordt voldaan. Dit zal bij de inzet van bevoegdheden in het kader van de betreffende wet- dan wel regelgeving bijvoorbeeld sneller aan de orde zijn dan bij de mogelijke inzet van andere bevoegdheden.

- Op sommige gegevens rust een (strikte) geheimhoudingsplicht. Er is dan mogelijk geen ruimte om gegevens verder te verwerken voor andere doeleinden. Dat betekent dat niet bij ieder signaal een hit/no hit-vraag kan worden gesteld. Dit is bijvoorbeeld aan de orde bij politiegegevens die aan de burgemeester zijn verstrekt op grond van artikel 16 lid 1 sub b onder 1 en 2 van de Wpg.
- Er is op dit moment geen jurist verbonden aan de directie Veiligheid die de bovengenoemde rechtmatigheidstoets kan uitvoeren. Rechtmatige binnengemeentelijke gegevensuitwisseling vereist relevante juridische kennis van de AVG en aanvullende wet- en regelgeving.
- De processen Bibob, RIEC-liaison en gemeentesignalen kennen overlap. Tevens kunnen persoonsgegevens voor het ene proces ook van belang zijn voor het andere proces. Schets kaders voor de uitwisseling van gegevens tussen deze processen. Leg vast op welke wijze PGA-x dit wel/niet kan faciliteren.
- De fast-report tool maakt rapportages op persoonsniveau mogelijk. Dit is niet wenselijk of noodzakelijk. Maak alleen rapportages op geaggregeerd niveau.

Risico: Spoorhouders weten niet altijd of ze gegevens mogen delen met de IKO-medewerker, hierdoor bestaat het risico dat er geen of meer gegevens gedeeld worden dan noodzakelijk.

Spoorhouders weten niet altijd of en wanneer ze gegevens mogen delen met de RIEC-liaison. De kaders hiervoor zijn beschreven in het Handboek Privacy IKO Infodesk en zijn verder uitgewerkt in het *“Werkproces integrale casusaanpak door het Regionaal Informatie en Expertise Centrum (RIEC)”*. Deze kaders zijn (nog) niet voldoende bekend (bij de spoorhouders). Daarnaast is er geen privacy officer die hierbij kan ondersteunen. Hierdoor kunnen er al snel geen of juist te veel gegevens beschikbaar worden gesteld aan de RIEC-liaison. Uit de workshop is gebleken dat dit vaak plaatsvindt.

Maatregel:

Zorg dat bovenstaande kaders voor de gegevensuitwisseling bekend zijn bij de spoorhouders (of ondersteunende privacy officers). Daarnaast moet de RIEC-liaison alle irrelevante gegevens afkomstig van spoorhouders verwijderen of anonimiseren, voordat de gegevens worden gedeeld met het RIEC.

5.1.2.f heeft tijdens de workshop aangegeven dat er een e-learning ontwikkeld kan worden voor gebruikers van PGA-x over privacy en gegevensbescherming in het kader van ondermijning. Geadviseerd wordt gebruik te maken van deze optie.

4.3 Juistheid

Inleiding

Is de kwaliteit van de gegevens gewaarborgd (actueel, juist en volledig)? Hoe worden gegevens over de personen verwerkt (handmatig of automatisch?) Vindt er controle op de datakwaliteit plaats en zo ja wanneer?

Feiten & Analyse

Een signaal is, in beginsel, afkomstig van burgers of organisaties die een melding willen doen van een ondermijnende activiteit. Een melding komt bij de IKO-Infodesk binnen via:

- ondermijning@denhaag.nl;
- Meld Misdad Anoniem (MMA);
- Meld een Vermoeden (MeV);
- via het Spoorhoudersnetwerk.

In principe is een signaal altijd onbetrouwbaar. Daarom moet worden onderbouwd of een signaal, na controle en verrijking, betrouwbaar genoeg wordt bevonden om interventies op te plegen. Het proces gemeentesignalen is feitelijk gericht op deze ‘waarheidsvinding’.

Een binnengekomen signaal wordt tijdens de kwalificatie daarvan geverifieerd in openbare bronnen, namelijk het Brp, KvK, BAG en Brk. PGA-x ontsluit deze bronnen via de centrale gemeentelijke API Gateway met HaalCentraal. De API gateway valt onder de generieke ICT infrastructuur van de gemeente en is geen onderdeel van deze DPIA. In deze DPIA wordt uitgegaan van de juistheid van de bronsystemen. Elk signaal leidt daardoor minimaal tot een subject, object of locatie op basis waarvan het signaal gerouteerd of (verder) verrijkt kan worden.

Als een signaal kwalificeert als ondermijning binnen het grondgebied van de gemeente Den Haag en de gemeente heeft interventiemogelijkheden, dan wordt de melding gerouteerd volgens de routeringsregels. Routing vindt plaats naar een afdeling van de gemeente in geval van een monodisciplinair aanpak, de Haagse Pand Brigade wanneer het gaat om malafide bedrijvigheid en/of prostitutie of het signaal wordt verder verrijkt door de IKO-medewerker.

Als de melding door het IKO wordt oppakt, wordt de zwaarte van het signaal bepaald door de IKO-medewerker op basis van zijn professionele afweging en de gemeentelijke prioritering. Bijlage 1 van het Model privacy protocol bevat echter ook een checklist ten behoeve van de signaalanalyse.

In deze DPIA wordt uitgegaan van de juistheid van de gegevens die de IKO-medewerker van Spoorhouders ontvangt uit hun bronsystemen.

Het signaal wordt steeds voorafgaande aan een interventie of het monitoren daarvan geverifieerd om te beoordelen of het nog actueel is.

Er worden geen signalen gemigreerd naar PGA-x. Hierin wordt begonnen met een schone lei. Er is daarom geen migratiestrategie nodig voor dit proces

Risico's en maatregelen

Er zijn ten aanzien van het beginsel *Juistheid* geen risico's geïdentificeerd.

4.4 Dataminimalisatie

Inleiding

Kan er met bijvoorbeeld minder persoonsgegevens, of op een andere manier worden gewerkt zonder de functionaliteit van het proces en systeem aan te tasten? Zijn er rapportages waarin tot individuen herleidbare informatie is opgenomen? Worden alleen die gegevens vastgelegd die absoluut noodzakelijk zijn voor het doel van de verwerking? Welke zijn dat niet?

Feiten & Analyse

Het proces gemeentesignalen bevat een aantal waarborgen om de proportionaliteit van de verwerking te waarborgen. Deze waarborgen worden ingevuld door een aantal procesmatige randvoorwaarden waarin gefaseerdheid een onderdeel is om bovenmatig gebruik van gegevens te voorkomen.

Een signaal bevat vaak veel wisselende persoonsgegevens vanwege het medium waarmee het wordt gemeld bij de gemeente. Dit is inherent aan dergelijke signalen.

De privacy officer bepaalt in 'privacy check 1' of en zo ja welke gemeentelijke bronnen naar aanleiding van het concrete signaal kunnen worden geraadpleegd via de spoorhouders en welke gegevens relevant zijn voor het signaal. In de praktijk wordt deze beoordeling uitgevoerd door een IKO-medewerker, omdat de rol van privacy officer niet voldoende is bekleed met de juiste kennis en beschikbare fte's.

Er is sprake van een hit als van een persoon bepaalde, voor het signaal relevante, gegevens in een bronbestand van een gemeentelijk onderdeel voorkomen. De betrokken persoon is in dat geval bekend binnen het betreffende gemeentelijke domein. Als er geen hit is, wordt het signaal niet in behandeling genomen.

Als er sprake is van een hit, dan worden de gegevens via de spoorhouder opgevraagd om te beoordelen of de gegevens het signaal in voldoende mate bevestigen om door te gaan met het onderzoek.

Indien het onderzoek daar aanleiding toe geeft, volgt een gemeentelijk casusoverleg met de gemeentelijke onderdelen waar sprake is van een relevante hit.

Voordat het gemeentelijke casusoverleg plaatsvindt bepaalt de privacy officer in 'privacy check 2' welke verzamelde gegevens met de relevante, bij het signaal betrokken,

gemeentelijke onderdelen mogen worden gedeeld ten behoeve van de vaststelling van de verdere aanpak en welke binnengemeentelijke gegevensuitwisseling nodig is voor het verwezenlijken van die aanpak en of dat toelaatbaar is. In de praktijk wordt deze check uitgevoerd door een IKO-medewerker.

Risico's en maatregelen

Ten aanzien van het beginsel *dataminimalisatie* zijn de volgende aandachtspunten geïdentificeerd. Deze worden hieronder beschreven.

Aandachtspunten:

- Bovenstaande waarborgen reflecteren een ideaalbeeld. De gemeente is op dit moment nog onvoldoende in staat om bovenstaande privacy checks uit te voeren. Er is namelijk geen capaciteit en competentie aanwezig binnen de directe Veiligheid om de rol van privacy officer te vervullen.
- Tijdens de workshop bleek het nog niet duidelijk is hoe dit proces in de praktijk uitgevoerd wordt. De IKO-medewerker dacht namelijk dat spoorhouders direct bevraagd konden worden (zonder 'privacy check' door een privacy officer). Dit proces vindt op deze manier nog niet plaats binnen de gemeente. Uit het bovenstaande blijkt echter dat er goede werkinstructies moeten komen over de invulling van de privacy checks in het proces (mogelijk concreter dan uitgewerkt in het Handboek).

4.5 Opslag

Inleiding

Welke bewaartermijnen zijn van toepassing? Hoe worden persoonsgegevens bewaard en worden persoonsgegevens die niet langer nodig zijn daadwerkelijk verwijderd? Worden op de middelen (desktop, pc, mobiele telefoon) zelf gegevens opgeslagen?

Feiten & Analyse

Gegevens worden opgeslagen in Outlook en PGA-x. Er wordt geen gebruik gemaakt van scanapparatuur.

De server van PGA-x staat in Rotterdam. De persoonsgegevens worden verwerkt binnen de EER.

Voor het binnengemeentelijk proces aanpak ondermijning zijn de bewaartermijnen niet vastgelegd in wetgeving. Het is aan de gemeente zelf om hier redelijke termijnen voor te bepalen. De gemeente volgt de bewaartermijnen uit het '*Modelprotocol binnengemeentelijke gegevensuitwisseling*'. Daarin wordt gesteld dat:

- Indien een signaal niet kwalificeert als ondermijning, wordt het signaal voor maximaal een jaar bewaard.
- Indien het signaal wel kwalificeert als ondermijning, wordt het maximaal vijf jaar bewaard.
- Gegevens in Outlook worden verwijderd direct nadat de gegevens zijn geüpload in PGA-x.

Deze bewaartermijnen zijn nog niet als instructie gegeven aan ^{5.1.2.f} voor implementatie van PGA-x.

De back-up worden volgens ^{5.1.2.f} bewaard conform de afspraken in de verwerkersovereenkomst. Zoals vastgesteld onder het thema 'Governance' moet de verwerkersovereenkomst nog worden gesloten. Er zijn dus nog geen afspraken over het back-up beleid bekend bij ^{5.1.2.f}

Nadat de bewaartermijn is verstreken wordt het dossier op een archiveringslijst (recordlijst) gezet. Deze recordlijst kan worden geëxporteerd naar het gemeentelijk archief, zodat te allen tijde duidelijk wordt wat er is vernietigd. Het is onduidelijk of deze verplichting in de archiefwet staat. De metadata van verwijderde dossiers is, na vernietiging, nog steeds beschikbaar in de vorm van rapportages.

Inactieve dossiers met daarin gegevens die niet langer worden gebruikt worden niet verwijderd uit de lijst met actieve dossiers. Deze dossiers blijven zichtbaar op het dashboard en zijn toegankelijk voor geautoriseerde personen.

Risico's en maatregelen

Ten aanzien van het beginsel *opslag* zijn de volgende aandachtspunten geïdentificeerd. Deze worden hieronder beschreven.

Aandachtspunten:

- De bewaartermijnen en het back-up beleid zijn nog gedeeld met 5.1.2.f De bewaartermijnen en het back-up beleid zijn bekend bij de gemeente. Leg deze zo snel mogelijk vast in de verwerkersovereenkomst.
- Er bestaat geen archiveringsplicht voor gegevens in dit proces. Het is onduidelijk waarom deze worden gedeeld met het gemeentelijk archief. Zet deze vraag uit bij DIV.

4.6 Bescherming

Inleiding

Persoonsgegevens moeten technisch en organisatorisch adequaat worden beschermd. Op welke wijze is de toegang tot gegevens afgeschermd? Is dit voldoende veilig in verhouding tot de gevoeligheid van de gegevens die verwerkt worden? Welke externe partijen hebben toegang tot de gegevens (leveranciers, samenwerkingspartners, dienstverleners) en hoe is de beveiliging daar geregeld?

Feiten & Analyse

5.1.2.f is ISO 27001 en NEN 7510 gecertificeerd. Er vindt jaarlijks een externe audit plaats. Daarnaast vinden maandelijks tot jaarlijks interne audits (afhankelijk van het onderwerp) plaats. Tweemaal per jaar vindt een code review plaats en wordt een pentest uitgevoerd. Er loopt een proces bij de gemeente, via de ISO, om de genomen effectiviteit van de genomen maatregelen te beoordelen.

5.1.2.f maakt gebruik van een subverwerker: 5.1.2.f g. 5.1.2.f is ISO 27001 en NEN 7510 gecertificeerd. Ze beschikken tevens over een ISAE 3402 type II verklaring en SOC2 Assurance rapport. Scope is onbekend.

De gemeente heeft nog geen autorisatiematrix of ander toegangsbeleid gedeeld met 5.1.2.f. Er zijn daarom nog geen rechten bekend. Toegang is gebaseerd op need-to-know. 5.1.2.f checkt eenmaal per drie maanden bij eigenaren van een dossier of de lijst met beheerders nog actueel is.

Alle handelingen in PGA-x worden gelogd in de audit log. 5.1.2.f voert geen monitoring uit. De logs kunnen in rapportages gedeeld worden met de gemeente.

Medewerkers kunnen inloggen in PGA-x via Single Sign On (SSO). Medewerkers loggen in op het netwerk via Mulfi Factor Authentication (MFA).

Er is nog geen key-user functioneel beheer aangesteld, maar dit wordt waarschijnlijk in samenwerking met het Zorg- en Veiligheidshuis geregeld.

Risico's en maatregelen

Ten aanzien van het beginsel *bescherming* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Aandachtspunten:

- De gemeente heeft nog geen autorisatiematrix opgesteld waarin het toegangsbeheer voor PGA-x wordt geregeld. Maak een autorisatiematrix gebaseerd op role based access. Laat deze autorisatiematrix toetsen door de Information Security Officer
- Het functioneel beheer van PGA-x is nog niet belegd. Zorg ervoor dat het functioneel beheer duidelijk belegd wordt. Mocht het functioneel beheer belegd worden bij 5.1.2.f zorg dan voor duidelijke afspraken over de omgang met

persoonsgegevens. De medewerker(s) die als functioneel beheerder te werk gaan zullen aan een geheimhoudingsverklaring gebonden moeten worden.

- Er vindt geen actieve monitoring plaats op de logging. Regel monitoring rules in die verdachte activiteiten signaleren. Denk hierbij aan het downloaden van bestanden op de persoonlijke schijf van de medewerker.
- Leg de informatiebeveiligingseisen vast in de verwerkersovereenkomst.

4.7 Transparantie

Inleiding

De gemeente is helder in de gegevens die zij verwerkt. De betrokkene moet goed kunnen begrijpen welke persoonsgegevens worden verwerkt (en waarom) en heeft het recht en de mogelijkheid om in te grijpen. De betrokkene heeft het recht op informatie, inzage, correctie en verwijdering.

Feiten & Analyse

De IKO-medewerker verzamelt gegevens uit openbare bronnen en uit gemeentelijke bronsystemen via spoorhouders van diensten binnen de gemeente over subject/object n.a.v. een ontvangen signaal. Het signaal, inclusief gegevens, wordt potentieel intern of extern gerouteerd.

De betrokkene wordt door de gemeente op geen enkele wijze geïnformeerd over de gegevensverwerking. Wel is er een pagina "Haags veiligheidsbeleid" waar de 3 sporen aanpak wordt beschreven⁴.

Er staat een privacyverklaring op de website van de gemeente Den Haag. Hierin wordt geen melding gedaan over de gegevensverwerking in het kader van de bestuurlijke en geïntegreerde aanpak ondermijning.

Betrokkenen worden (ter plaatse) geïnformeerd over het onderzoek als er een interventie plaatsvindt door een gemeentelijke dienst. De betrokkene wordt niet gewezen op zijn rechten op grond van de AVG.

Risico's en maatregelen

Ten aanzien van het beginsel *transparantie* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Betrokkenen worden onvoldoende geïnformeerd

Betrokkenen worden niet of nauwelijks geïnformeerd door de gemeente over de werkzaamheden en de mogelijke verwerking van hun persoonsgegevens door de IKO-infodesk. Als er al informatie wordt gegeven, dan is deze onvolledig. Zij weten dus niet dat de gemeente gegevens over hen verwerken in hun systemen en mogelijk delen met derden. Zij worden ook niet gewezen op hun rechten.

Voorgestelde maatregel

Informeer betrokkenen over de gegevensverwerking. Het uitgangspunt is dat betrokkenen zo snel en volledig mogelijk worden geïnformeerd. Dit is in het kader van het onderzoek niet altijd mogelijk. De algemene informatievoorziening aan de burger kan wel worden verbeterd, bijvoorbeeld bij het in eerste instantie verzamelen van gegevens bij de betrokkene. Tijdens interventies kan er een flyer worden uitgedeeld waarin betrokkene wordt geïnformeerd. Pas de privacyverklaring van de gemeente Den Haag aan. Neem een onderdeel op over de IKO-

⁴ <https://www.denhaag.nl/nl/in-de-stad/veiligheid/haags-veiligheidsbeleid.htm>

infodesk. Vul deze ook aan met andere verplichte informatie. De privacyverklaring moet minimaal de volgende gegevens bevatten:

- De identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van uw vertegenwoordiger in de EU;
- De contactgegevens van de FG als u die heeft.
- De doeleinden en rechtsgrond van de verwerking, en als u zich beroept op een gerechtvaardigd belang: op welk belang u zich beroept.
- De (categorieën van) ontvangers van de persoonsgegevens.
- Of u van plan bent de persoonsgegevens door te geven buiten de EU of een internationale organisatie en op welke juridische grond.
- De bewaartermijn van de gegevens.
- De rechten van de betrokkene, zoals het recht op inzage, correctie en verwijdering.
- Het recht van de betrokkene om de gegeven toestemming voor een bepaalde verwerking altijd in te kunnen trekken.
- Dat de betrokkene een klacht kan indienen bij de relevante privacytoezichthouder.
- Of en waarom de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn als de gegevens niet worden verstrekt.
- Of u gebruik maakt van geautomatiseerde besluitvorming, inclusief profilering, en hoe u besluiten neemt.
- Als de gegevens van een andere organisatie zijn verkregen: de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

4.8 Cultuur

Inleiding

Zijn medewerkers zich bewust van het belang van het beschermen van privacygevoelige gegevens? Gaat iedereen even zorgvuldig om met de gegevens, worden betrokkenen goed geïnformeerd over hoe men moet omgaan met die gegevens?

Feiten & analyse

Privacy wordt een steeds belangrijker thema binnen de directie Veiligheid.

Dit blijkt bijvoorbeeld uit het volgende. De afdeling Ondermijning heeft vorig jaar een het 'Handboek Privacy IKO-infodesk' laten opstellen door een extern adviesbureau. Dit handboek beschrijft de werkprocessen voor het Bibob, RIEC-liaison en gemeentesignalen proces vanuit privacy perspectief.

De afdeling Ondermijning heeft een externe privacy expert ingehuurd om te adviseren over de implementatie van de werkprocessen in PGA-x.

In dit proces wordt er met gevoelige gegevens gewerkt. Het is daarom van belang dat medewerkers goed op de hoogte zijn van de richtlijnen hoe om te gaan met deze gegevens.

Op dit moment wordt nog te weinig gedaan om de bewustwording van medewerkers op het gebied van privacy te vergroten. Zo is er al ruime tijd geen bewustwordingsactiviteit, zoals een training of e-learning, georganiseerd voor medewerkers. Tijdens de workshop is duidelijk aangegeven dat medewerkers hier behoefte aan hebben. Medewerkers zijn bereid zich te verdiepen in dit thema en erkennen de relevantie daarvan in het licht van de aard van de verwerkingsactiviteit.

Er is geen formeel clean-desk beleid aanwezig. In de workshop wordt aangegeven dat medewerkers hun laptop niet altijd vergrendelen. Tevens blijven veel documenten op bureaus liggen en worden de deuren niet altijd op slot gedaan.

PGA-x biedt een privacy module aan voor de gemeente Den Haag. Het is nog onbekend of deze door de gemeente Den Haag geïmplementeerd wordt.

Risico's en maatregelen

Op basis van de analyse op het aspect *governance* zijn de volgende risico's geïdentificeerd. Deze worden hieronder beschreven.

Risico: Er is te weinig aandacht voor privacy geweest waardoor medewerkers onvoldoende getraind zijn in het herkennen van privacy risico's in dit proces

Medewerkers zijn lange tijd niet meer getraind in privacy bewustwording. Hierdoor zijn zij onvoldoende getraind om privacy risico's en datalekken te herkennen en hoe ze hier mee om moeten gaan.

Voorgestelde maatregel

Train medewerkers in het herkennen van privacy risico's. Besteed meer aandacht aan de bewustwording van medewerkers op het gebied van privacy. Beoordeel en overweeg de privacy module in PGA-x te implementeren en zorg ervoor dat medewerkers deze uitvoeren voordat zij aan de slag gaan met het systeem.

5. Advies en accordering

In het risico overzicht dat als bijlage aan deze rapportage is toegevoegd wordt weergegeven welke privacy risico's de verwerking met zich meebrengt, welke beheersmaatregelen hiervoor nodig zijn en welke acties hieraan gekoppeld zijn. Dit overzicht wordt bewerkt zodra beheersmaatregelen worden uitgevoerd en risico's gemitigeerd, zo blijft de DPIA up to date ook na het uitvoeren van beheers acties.

Aanbevelingen voor vervolg

Wij adviseren om de hierboven genoemde risico's als volgt aan te pakken:

1. Benoem een business eigenaar van ieder risico in het risico overzicht en de bijbehorende maatregelen.
2. Geef de business eigenaar de opdracht de maatregelen in te voeren en daarmee het risico te mitigeren.
3. Geef elke 2 maanden een status update van de opvolging van deze aanbevelingen aan de FG en de Privacy Officer.

De huidige analyse is uitgevoerd voordat alle inhoudelijke gesprekken met de leverancier over implementatiekeuzes zijn gevoerd. Wij doen daarom een aanbeveling om een verdiepende analyse uit te voeren op de minimaal de volgende onderwerpen nadat alle implementatiekeuzes zijn gemaakt:

- Beveiliging en opslag

Advies FG

[GEBRUIK DEZE RUIMTE VOOR HET ADVIES VAN DE FG]

Naam: 5.1.2.e

Datum: [DATUM]

Accordering

Deze DPIA is opgeleverd aan:

Proceseigenaar	Functionaris Gegevensbescherming
Datum oplevering: 10-01-22	Datum oplevering: 10-01-22
Naam: 5.1.2.e	Naam: 5.1.2.e
Voor akkoord: [HANDTEKENING PROCESEIGENAAR]	Voor gezien: [HANDTEKENING FG]
Datum ondertekening: [DATUM]	Datum ondertekening: [DATUM]

Tekent voor gezien:

(Algemeen) Directeur [DIENST]
Datum oplevering: [DATUM]
Naam: 5.1.2.e
Tekent voor gezien: [HANDTEKENING DIRECTEUR]
Datum ondertekening: [DATUM]

Bijlage A

A1. Documentatie

De volgende documentatie is geraadpleegd.

Nr.	Documentnaam
1	Handboek Privacy IKO Infodesk
2	Model privacy protocol – handleiding binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijning
3	Informatiebeveiligingseisen externe dienstverlening PGA-x

A2. Geïnterviewden

De volgende personen hebben meegewerkt tijdens de DPIA sessie.

Datum	Geïnterviewden	Functie/Rol
22-07-2021	5.1.2.e	5.1.2.f
22-07-2021	5.1.2.e	5.1.2.e
22-07-2021	5.1.2.e S 5.1.2.e 5.1.2.e	5.1.2.e
22-07-2021	5.1.2.e	5.1.2.e 5.1.2.e
22-07-2021	5.1.2.e	Bestuursdienst DH, betrokken bij vormgeving privacy



HANDBOEK PRIVACY IKO INFODESK

Fout! Geen tekst met de opgegeven stijl in het document.

- Bibob proces
- RIEC Liaison proces
- Proces Binnengemeentelijke gegevensuitwisseling ondermijning

5.1.2.e

&

5.1.2.e

DATUM	22 april 2024
STATUS	Final
VERSIE	1.0
PROJECTNUMMER	20207940

Copyright © 2012 Verdonck, Klooster & Associates B.V.

Alle rechten voorbehouden. Niets van deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of enige andere manier, zonder voorafgaande schriftelijke toestemming van de auteursrechthebbende.



MANAGEMENTSAMENVATTING

De gemeente Den Haag heeft stappen gezet om de gemeentelijke informatiepositie voor de aanpak van ondermijning te versterken, om een betere partner in de integrale aanpak van ondermijnende georganiseerde criminaliteit te zijn. Binnen de gemeente is hiertoe het Informatieknooppunt Ondermijning (IKO) opgezet om data, informatie, kennis en expertise zo goed mogelijk te bundelen. Een belangrijk onderdeel van het IKO is de Infodesk: de backoffice van Team Ondermijning waar ondermijning gerelateerde signalen en casuïstiek worden opgepakt. De Infodesk maakt gebruik van het VIK, waarbinnen een bundeling van beschikbare gegevens/data plaatsvindt.

Voor de gemeentelijke aanpak ondermijningscasuïstiek (in RIEC verband) en voor de Bibob toetsing zijn door ^{5.1.2e} DPIA's uitgevoerd, die richting geven aan de te nemen maatregelen.

In vervolg hierop heeft de gemeente Den Haag ^{5.1.2e} gevraagd om voor het Bibob proces en het RIEC Liaison proces, alsook voor het nog te implementeren proces "behandelen van signalen ondermijning vanuit de gemeentelijke organisatie" aan de slag gaan met het verder uitwerken en concretiseren van deze processen.

Dit handboek biedt een nadere uitwerking van de processen vanuit privacy perspectief en vormt daarnaast (mede) input voor de aankomende implementatie van het zaakstelsel dat het VIK gaat ondersteunen.

INHOUDSOPGAVE

Managementsamenvatting	2
Inhoudsopgave	3
1 Inleiding	5
1.1 Introductie	5
1.2 Achtergrond	6
1.3 Leeswijzer	7
2 Het Bibob proces	8
2.1 Juridisch kader en ontwikkelingen	8
2.2 Het proces	10
2.3 Informatievoorziening burger	18
2.4 Verstrekkingen aan (keten)partners	19
3 Het RIEC Liaison proces	21
3.1 Juridisch kader & ontwikkeling	21
3.2 Het Proces	22
3.3 Informatievoorziening burger	29
3.4 Verstrekkingen aan (keten)partners	30
4 Binnengemeentelijke gegevensuitwisseling in het kader van aanpak criminele ondermijning	31
4.1 Juridisch kader en ontwikkelingen	31
4.2 Het proces	31
4.3 Informatievoorziening burger	40
4.4 Verstrekkingen aan (keten)partners	41
5 Rechten van betrokkene	42

5.1	Bibob proces	42
5.2	RIEC Liaison proces	42
5.3	Proces binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijning	43
6	Bewaartermijnen	44
A	Bijlage 1: Checklist ten behoeve van de signaalanalyse	46
B	Bijlage 2: analyses van de ruimte voor binnengemeentelijke gegevensuitwisseling in relevante wet- en regelgeving	60
C	Bijlage 3: Relevante links (extern)	61
D	Bijlage 4: Relevante links (intern)	62

1 INLEIDING

1.1 Introductie

In het kader van de bestrijding van ondermijnende criminaliteit, heeft de gemeente Den Haag binnen directie Veilig een Backoffice Ondermijning/Infodesk ingericht. In dit document worden Backoffice Ondermijning en Infodesk als synoniemen gebruikt. Hierbinnen wordt invulling gegeven aan een drietal processen; het gemeentelijk Bibob-proces, het werkproces van de RIEC- liaison en de binnengemeentelijke aanpak van ondermijnende criminaliteit.

De aanpak van ondermijning dient met inachtneming van wet- en regelgeving op het gebied van privacy plaats te vinden. Het verwerken van persoonsgegevens in het kader van de bestrijding van ondermijnende criminaliteit is geboden aan de eisen vanuit de AVG en UAVG en is daarnaast geboden aan verschillende sectorale wetten. Beginselen als doelbinding, transparantie en noodzakelijkheid van de gegevensverwerking vormen hierbij belangrijke, algemene uitgangspunten.

Zie voor uitgebreide toelichting op de samenhang tussen (U)AVG en sectorwetgeving en de consequenties daarvan voor de gegevensuitwisseling de “Voorlichting van de Afdeling advisering van de Raad van State van 20 maart 2020” met de titel “De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning”. Hierin wordt ook ingegaan op het RIEC-samenwerkingsverband en de wijze waarop daarbinnen met gegevensuitwisseling wordt omgegaan. En wordt geadviseerd om voor binnengemeentelijke gegevensuitwisseling de RIEC-werkwijze methodisch als inspiratie te laten dienen. De wijze waarop het werkproces van de RIEC-LIEC liaison en de binnengemeentelijke aanpak van ondermijnende criminaliteit in dit handboek worden beschreven vertoont dan ook veel overeenkomsten.

Doel van dit handboek is, duidelijkheid te verschaffen over de gegevensverwerking die plaatsvindt binnen de 3 genoemde Infodesk-processen en meer specifiek te maken:

- Welke gegevens je mag vragen en aan wie,
- Wat de bewaartermijnen zijn op dossier niveau,
- Welke gegevens je zelf mag verstrekken en aan wie,
- Welke informatie je moet verstrekken aan betrokkene(n)
- Hoe de betrokkene zijn rechten kan uitoefenen

Per proces zal ook worden ingegaan op zaken als:

- Welke contactpersonen en (keten-)partners er bij het proces betrokken zijn en welke afspraken daarmee zijn gemaakt
- De grondslagen voor de verwerkingen
- Kaders voor de verantwoording van de privacy afwegingen/keuzes die gemaakt worden
- Informatiedelingskader; wat mag aan wie verstrekt worden (intern en extern)
- Bevoegdheden die de medewerker nodig heeft (Bevoegdhedenmatrix)
- Rechten van betrokkenen
- Hoe aan transparantie invulling gegeven wordt

Dit handboek pretendeert niet volledig te zijn. Het is een levend document en dient periodiek herzien te worden. Op verschillende plekken in dit handboek zal verwezen worden naar kaders die vanuit landelijke gremia zijn opgesteld. Ook deze zijn aan verandering onderhevig.

Het verdient aanbeveling om specifiek op het onderwerp Ondernijning een privacy officer aan te stellen die naast kennis over privacy/AVG, goed onderlegd is in ondernijningswetgeving en wettelijke taken van de gemeente, om de afdeling ondersteuning te bieden bij het toepassen van wet- en regelgeving binnen specifieke casuïstiek.

1.2 Achtergrond

Met het gemeentelijk Bibob-proces is al jaren ervaring opgedaan en ten aanzien van hoe het proces uitgevoerd moet worden en welke gegevensuitwisselingen daarmee gepaard gaan, is al veel bepaald en vastgelegd in/door de Wet Bibob.

Voor de gemeentelijke bijdrage in het RIEC (vormgegeven in het RIEC-Liaison proces) en voor de binnengemeentelijke aanpak van ondernijning, is de huidige situatie minder helder voor wat betreft welke gegevensuitwisseling daarbij geoorloofd is binnen de kaders van de privacy wet- en regelgeving.

De mogelijkheden informatie te delen in het RIEC-liaison proces zijn met name afgeleid van het Landelijke RIECS/LIEC Convenant en bijbehorend Privacy protocol en de procesbeschrijving casusaanpak.

Voor de binnengemeentelijke (bestuurlijke) aanpak van ondernijning is in februari 2020 het "Model privacy protocol, Handleiding binnengemeentelijke gegevensuitwisseling ten behoeve van

de bestrijding van ondermijning”¹, door de Minister van Veiligheid en Justitie, aangeboden aan de Tweede Kamer, waarin de kaders voor gegevensdeling zijn gesteld.

Voor zowel de binnengemeentelijke (bestuurlijke) aanpak van ondermijning als voor de RIEC-Liaison werkwijze wordt het werkproces gekenmerkt door een gefaseerde aanpak, waarbij op verschillende momenten in het proces een privacy afweging gemaakt moet worden.

Telkens zal voor het concrete geval en voor de specifieke fase moeten worden afgewogen welke gegevens kunnen / mogen worden verwerkt, waarbij van belang is te bepalen hoe dicht de taak/bevoegdheid die men overweegt in te zetten ligt bij de taak/bevoegdheid waarvoor deze gegevens zijn verzameld.

Hoe deze gefaseerdheid werkt en welke afwegingen er gemaakt moeten worden (en hoe deze kunnen worden vastgelegd) zal per proces verder worden toegelicht in dit document.

1.3 Leeswijzer

Als eerste wordt ingezoomd op het Bibob-proces. Daarna wordt ingezoomd op het proces van de RIEC-Liaison. Tot slot wordt een toelichting gegeven op het algemene kader voor gegevensuitwisseling binnen de gemeente in het kader van de bestuurlijke aanpak van criminele ondermijning.

¹ Naar aanleiding van het advies van de Raad van State
Copyright © 2012 Verdonck, Klooster & Associates B.V.

2 HET BIBOB PROCES

2.1 Juridisch kader en ontwikkelingen

Wet Bibob

Op 1 juni 2003 is de Wet Bevordering integriteitsbeoordelingen door het openbaar bestuur (verder Wet Bibob genoemd) in werking getreden. De Wet Bibob verruimt de mogelijkheden van gemeenten en andere bestuursorganen om zich te beschermen tegen het risico dat ze criminele activiteiten faciliteren. Dit is nodig omdat criminele organisaties in sommige gevallen afhankelijk zijn van bestuurlijke beslissingen voor de continuering en afscherming van criminele activiteiten. De Wet Bibob is in het leven geroepen om dit incidentele misbruik van overheidsbeslissingen en de nadelige gevolgen hiervan voor bonafide ondernemers te voorkomen.

Op grond van de Wet Bibob is het mogelijk diepgaand onderzoek te doen naar de achtergrond van de persoon of onderneming middels de eigen bevoegdheden die een bestuursorgaan daar ingevolge de Wet Bibob toe heeft, of het vragen van een advies aan het Landelijk Bureau Bibob. Wanneer na onderzoek blijkt dat de vergunning mogelijk gebruikt gaat worden voor criminele activiteiten, kan het bevoegd bestuursorgaan de vergunning weigeren. Ook kan een reeds verstrekte vergunning om dezelfde reden tussentijds worden ingetrokken.

Blijkens de Memorie van Toelichting van de Wet Bibob zijn de beginselen van subsidiariteit en proportionaliteit belangrijke uitgangspunten van de wet. Het instrument Bibob dient dan ook een ultimum remedium te zijn.

Op 1 augustus 2020 is de vernieuwde Wet Bibob in werking getreden. Op dezelfde datum is ook een wijziging van het Besluit justitiële en strafvorderlijke gegevens in werking getreden. Deze wijzigingen hebben het toepassingsbereik van de Wet verruimd en maakt verder gaand onderzoek mogelijk. Momenteel wordt gewerkt aan een volgende wijziging van de Wet Bibob die uitwisseling van informatie verruimt tussen het Landelijk Bureau Bibob en bestuursorganen, en tussen bestuursorganen onderling.

Toepassingsbereik Wet BIBOB

De Wet Bibob is van toepassing op een groot aantal overheidsbeslissingen:

- Beschikkingen (waaronder vergunningen, ontheffingen, toekenningen, goedkeuringen, erkenningen, registraties en aanwijzingen);
- Subsidies;
- Overheidsopdrachten; en
- Vastgoedtransacties.

Het exacte bereik van de Wet Bibob volgt uit artikel 1 van de Wet Bibob in combinatie met een bijzondere wet (zoals de Drank- en Horecawet, Wet milieubeheer of Wet op de Kansspelen) waarin de Wet Bibob van toepassing is verklaard. In de bijzondere wet kan ook aangegeven zijn dat bij of krachtens Algemene Maatregel van Bestuur de Wet Bibob van toepassing is op de betreffende overheidsbeslissing.

Zie ook de “Beleidslijn voor de toepassing van de wet bevordering integriteitsbeoordelingen door het openbaar bestuur van de gemeente Den Haag”².

Weigeringsgronden

De Wet Bibob bevat de volgende vier gronden om een overheidsbeslissing in te trekken of te weigeren:

- De A-grond: het ernstige gevaar dat een overheidsbeslissing gebruikt zal worden om criminele voordelen te benutten (artikel 3, eerste lid, sub a, van de Wet Bibob);
- De B-grond: het ernstige gevaar dat een overheidsbeslissing gebruikt zal worden om strafbare feiten te plegen (artikel 3, eerste lid, sub b, van de Wet Bibob);
- Een strafbaar feit dat is gepleegd ter verkrijging of ter behoud van een overheidsbeslissing (artikel 3, zesde lid van de Wet Bibob); en
- De weigering van de houder van de beschikking om het bestuursorgaan, desgevraagd aanvullende gegevens te verstrekken, dan wel de weigering van de aanvrager of houder van de beschikking om het LBB desgevraagd aanvullende gegevens te verstrekken (artikel 4 van de Wet Bibob).

² <https://denhaag.raadsinformatie.nl/document/3368602/1/RIS280746%20Beleidslijn%20Bibob>

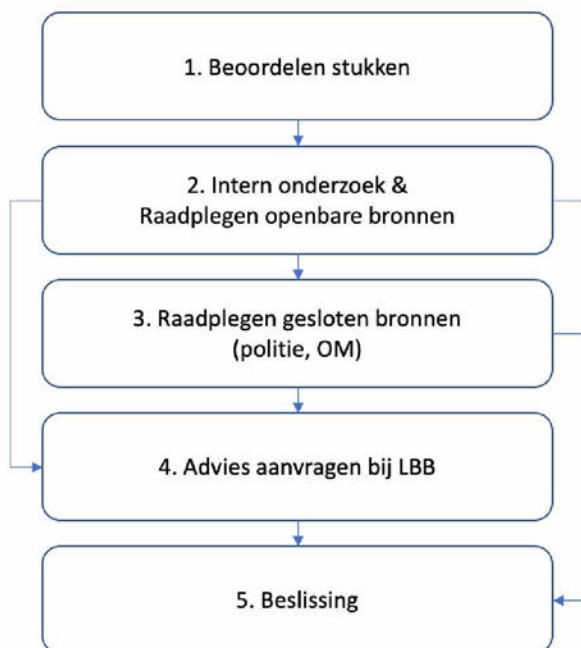
2.2 Het proces

Het Bibob-proces neemt start door een van de volgende gebeurtenissen, waarna het dossier aan een van de Bibob medewerkers wordt toegewezen.

- Bij overheidsbeslissingen (zie onder "Toepassingsbereik Wet Bibob" hierboven)
- Tip Officier van Justitie of LBB (artikel 11 respectievelijk artikel 26 Wet Bibob);
- Tip RIEC (artikel 7.2/7.3 Privacyprotocol RIECs/LIEC)

De aanleiding of trigger voor het starten van het Bibob proces moet worden vastgelegd in het dossier.

In de navolgende paragrafen wordt een omschrijving gegeven van de stappen in het proces Bibob. De stappen zijn beschreven in chronologische volgorde. De privacy van betrokkenen in dit proces wordt gewaarborgd door middel van een aantal privacy checks. Hierop zal gedetailleerd worden ingegaan.



2.2.1 Privacy afwegingskader Bibob proces;

Door de wijze waarop het Bibob-proces is opgezet, worden bijna automatisch afwegingen gemaakt of het noodzakelijk is een verdere inbreuk op de privacy van betrokkene te maken.

Zo zal het bij de overgang van stap 2 naar stap 3 van belang zijn dat de Infodesk-medewerker duidt en vastlegt waarom besloten wordt door te gaan naar stap 3. Dit gebeurt in de regel door middel van de toelichting bij het informatieverzoek dat aan de Politie, het OM, of de Belastingdienst wordt gestuurd. Hetzelfde geldt voor de overgang van stap 3 naar stap 4, waar besloten wordt advies te vragen aan het Landelijk Bureau Bibob. Ook daar dient de adviesaanvraag voor het LBB gemotiveerd te worden en wordt deze gaande het proces 'automatisch' vastgelegd. Deze motivering wordt schriftelijk vastgelegd in het dossier.

2.2.2 Het proces in stappen

1- BEOORDELEN STUKKEN

Doel van het deelproces: ophalen dossier uit de werkvoorraad en toewijzen aan een Bibob-medewerker. Deze stap start op het moment dat een Bibob-medewerker een willekeurig dossier ophaalt uit de werkvoorraad dan wel na intern overleg een dossier op naam zet, of door zelf een dossier in de werkvoorraad toe te voegen (bijvoorbeeld op grond van overige signalen, zoals een OM-tip). De Bibob-medewerker bestudeert het betreffende dossier en kan vervolgens een beslissing op het verzoek nemen of nader onderzoek naar de ondernemer en zijn zakenrelaties (laten) doen. Deze eerste toets vindt plaats op basis van het door de betrokkene aangeleverde dossier. De Bibob-medewerker kijkt of de informatie volledig is en klopt. Artikel 7a lid 2 Wet Bibob bepaalt dat de betrokkene in ieder geval de volgende gegevens aanlevert ten behoeve van het eigen onderzoek van het bestuursorgaan:

- a. de naam, het adres en de woonplaats of plaats van vestiging van de betrokkene;
- b. de naam, het adres en de woonplaats van de persoon door wie de betrokkene zich laat vertegenwoordigen;
- c. het burgerservicenummer, bedoeld in artikel 1, onder b, van de Wet algemene bepalingen burgerservicenummer, van de persoon, bedoeld in de onderdelen a en b;
- d. het nummer van inschrijving bij de Kamer van Koophandel;
- e. de rechtsvorm van de betrokkene;

- f. de handelsnaam of handelsnamen waarvan de betrokkene gebruikmaakt of heeft gemaakt;
- g. de naam, het adres en de woonplaats van de natuurlijke personen of rechtspersonen die, voor zover van toepassing:
 - 1. direct of indirect leiding geven of hebben gegeven aan betrokkene;
 - 2. direct of indirect zeggenschap hebben of hebben gehad over betrokkene;
 - 3. direct of indirect vermogen verschaffen of hebben verschaft aan betrokkene;
 - 4. onderaannemer van betrokkene zijn;
- h. de wijze van financiering.

Er vindt een nader onderzoek plaats indien de Bibob-medewerker een vermoeden heeft dat de informatie onvolledig of foutief is.

Doel	Toetsen stukken
Wie voert uit	Infodesk-medewerker die gemachtigd is voor het Bibob-proces
Welke info kan worden opgevraagd in deze stap	Nvt, het dossier / de stukken worden aangeleverd
Mogelijke uitkomsten	De eerste toets op basis van de stukken kan de volgende uitkomsten hebben: 1. Alles lijkt in orde, er blijkt geen gebleken risico (de rechtsrelatie kan worden aangegaan of gecontinueerd); → stap 5, Beslissen 2. Er zijn vermoedens van onvolledige of foutieve informatie, nader onderzoek is nodig → stap 2, Intern onderzoek
Privacy afweging	Naar stap 2 als er een vermoeden is van onvolledige of foutieve informatie

2- INTERN ONDERZOEK & RAADPLEGEN OPENBARE BRONNEN

Doel van het deelproces: het doen van een eigen onderzoek naar de ondernemer en zijn relaties door middel van het raadplegen van open bronnen. Dit onderzoek is erop gericht om vast te stellen in hoeverre het bestuursorgaan ernstige risico's, dan wel mindere mate van gevaar, loopt dat met het aangaan of continueren van een rechtsverhouding met een wederpartij, criminaliteit wordt gefaciliteerd. De bevoegdheid van het bestuursorgaan om eigen onderzoek te doen naar de

ondernemer en zijn zakelijke relaties volgt uit artikel 7a lid 1 Wet Bibob. De Bibob-medewerker kan de volgende bronnen raadplegen: BRP (via Haagse bron), Kadaster en het Handelsregister. De bevoegdheid van de Bibob-medewerker om gegevens uit openbare bronnen te verwerken volgt uit artikel 7b Wet Bibob. Daarnaast kan de Bibob-medewerker ook informatie opvragen bij de sector belastingzaken ter voorkoming van schijnconstructies. Dit volgt uit een daartoe gesloten convenant tussen bestuursdienst directie Veiligheid en dienst publiekzaken sector belastingzaken van de gemeente Den Haag. Dit convenant is tot stand gekomen ten behoeve van de samenwerking in het RIEC, maar uit artikel 2.4 van het convenant kan worden afgeleid dat het convenant overeenkomstig van toepassing is op de uitvoering van de Wet Bibob.

Doel	Verder onderzoek en analyseren door middel van open bronnen
Wie voert uit	Infodesk-medewerker (Bibob)
Welke info kan worden opgevraagd in deze stap	artikel 7a lid 1 Wet Bibob artikel 7b Wet Bibob
• BRP	Welke info: Familierelaties, burgerlijke staat, woonadres Hoe op te vragen; BRP via HaagseBron
• KvK	Welke info: bedrijfsinformatie per onderneming of bevraging natuurlijke persoon Hoe op te vragen: www.kvk.nl
• Kadaster	Welke info: bezit van panden en financiering daarvan Hoe op te vragen: mijnkadaster.nl
• Gemeentelijke belastingzaken	Welke info: gegevens omtrent wie de daadwerkelijke betaling van gemeentelijke belastingen verricht Hoe op te vragen: Gelet op Artikel 4 van het Convenant met Belastingzaken, dienen de werkafspraken schriftelijk vastgelegd te worden en worden daarmee onderdeel van het

	convenant. (tevens van belang voor RIEC Liaison proces)
Mogelijke uitkomsten	Het intern onderzoek kan de volgende uitkomsten hebben: 1. Er is geen of althans onvoldoende ernstig risico gebleken (de rechtsrelatie kan worden aangegaan of gecontinueerd); → stap 5 2. Verlenen onder voorwaarden (bij mindere mate van gevaar, gericht op wegnemen of beperken van gevaar). → stap 5 3. Ernstige risico's leiden in de regel tot een zelfstandige Bibob-toepassing (dat wil zeggen een negatieve beslissing, zonder inschakeling van LBB). → stap 5 4. Gerede twijfel maakt aanvraag van een advies bij het LBB noodzakelijk. → stap 4
Privacy afweging	Indien er gerede twijfels zijn ten aanzien van het te lopen risico, wordt het proces vervolgd met stap 3. De overweging die hieraan ten grondslag ligt wordt vastgelegd in het dossier en zal tevens dienen als motivering voor de informatieverzoek in de volgende stap. Er bestaat een indicatorenlijst uit 2013. Deze kan bij de beoordeling gebruikt worden, maar wordt in de praktijk aangevuld met (relevante) lokale en thema gebonden kennis van de Bibob-medewerker.

3- RIEC PARTNER BEVRAGING (P/OM/BD) - RAADPLEGEN GESLOTEN BRONNEN

Via een informatieverzoek aan het RIEC kan de Bibob-medewerker verzoeken om gegevens van politie, OM of de belastingdienst over de aanvrager (en diens bovengeschikten).

De grondslag voor het informatieverzoek kan worden gelezen in artikel 2 van het Convenant in samenhang met paragraaf 6 van het Privacyprotocol (bron: RIEC). Wanneer het informatieverzoek wordt gedaan via RIEC-IS bevat de aanvraag ten minste:

1. NAW-gegevens van de betrokkene(n);
2. Informatie eigen organisatie;
3. Omschrijving van de zaak;
4. Beschrijving wat het bestuursorgaan al heeft gedaan;
5. Beschrijving bestaande of gevraagde vergunning dan wel de transactie;
6. De zaak is duidelijk omschreven; indien gegevens ontbreken vraagt de behandelend RIEC-medewerker aanvullende gegevens op bij het bestuursorgaan;
7. Het is duidelijk welke informatie moet worden opgevraagd;
8. Het bestuursorgaan is bevoegd op grond van de wettelijke regels de informatie op te vragen;
9. De aanvraag is in overeenstemming met het Bibob-beleid van het bestuursorgaan
10. Het RIEC kan in de ondersteunende rol niet meer vragen dan het bestuursorgaan zelf zou kunnen vragen

De justitiële informatie kan behalve via RIEC-IS ook rechtstreeks door de bibob-medewerker worden opgevraagd via JustID. De route via RIEC-IS wordt voor justitiële gegevens zelden gebruikt. Dit is anders voor politiegegevens. Daar wordt vrijwel uitsluitend gebruik gemaakt van de route via RIEC-IS en zelden via de infodesk.

Doel	Verrijking van het Bibob-dossier met gegevens van RIEC Partners ter verdere onderbouwing van eventueel besluit
Wie voert uit	Infodesk-medewerker
Welke info kan worden opgevraagd in deze stap	Artikel 2 van het Convenant jo. paragraaf 6 van het Privacyprotocol
• Politie	Welke info: Art 8, Art 9 en Art 10 lid 1 en Art 13 Politiegegevens Hoe op te vragen: via informatieverzoek in RIEC-IS of via infodesk Politie (dit laatste wordt in de praktijk van gemeente Den Haag niet gedaan)
• OM	Welke info: justitiële gegevens Hoe op te vragen: via informatieverzoek RIEC-IS of via JustID (in de praktijk wordt JustID bevraagd)

• BD	Welke info: Grove schuld en opzet varianten genoemd onder 68,69, 69a AWR en onder 64, 65 Invorderingswet 1990 (<i>Zie voorbeeldvragen in “werkproces Bibob ondersteuning” van het Riec</i>) Hoe op te vragen: via informatieverzoek RIEC-IS
Mogelijke uitkomsten	Na verrijking van het dossier met informatie van de RIEC-partners kan de uitkomst zijn: 1. Er is geen of onvoldoende ernstig risico gebleken (de rechtsrelatie kan worden aangegaan of gecontinueerd); → stap5 2. Verlenen onder voorwaarden (bij mindere mate van gevaar, gericht op wegnemen of beperken van gevaar). → stap5 3. Ernstige risico's leiden in beginsel tot een zelfstandige Bibob-toepassing (dat wil zeggen een negatieve beslissing, zonder inschakeling van LBB). → stap5 4. Gerede twijfel maakt aanvraag van een advies bij het LBB noodzakelijk. → stap 4
Privacy afweging	Indien er voldoende aanwijzingen zijn dat er ernstig gevaar bestaat, wordt besloten om door te gaan met stap 4 en advies in te winnen bij het LBB. Motivatie wordt vastgelegd in dossier.

4- ADVIES VRAAG AAN LBB

Deze stap kan pas worden gezet nadat gebleken is dat er, gegeven de beschikbare informatie tot dan toe, geen mogelijkheden zijn tot bestuurlijk ingrijpen en er wel vermoedens zijn dat er sprake is van ondermijning.

Doel van dit deelproces is nader onderzoek in gesloten bronnen naar ondernemer en zakelijke relaties te doen via adviesvraag aan het LBB. Dit geschiedt op basis van artikel 7a lid 1 Wet Bibob. Het opvragen van een Bibob-advies is een zwaar middel dat forse inbreuk maakt op de privacy van de betrokkene en/of zijn zakelijke omgeving. Het is daarom een ultimatum remedium.

“Als het bestuursorgaan niet voldoende informatie over de wederpartij heeft maar bijvoorbeeld wel signalen heeft van het openbaar ministerie op grond van artikel 26 wet Bibob (OM-tip) dat, gelet op de zakelijke omgeving van betrokkene(n), risico’s bestaan op criminele facilitering, dan kan dat voor het bestuursorgaan aanleiding zijn om een advies te vragen aan het Landelijk Bureau Bibob.”

en

“De wetgever heeft er voor gekozen onderzoek in z.g. gesloten bronnen naar personen in de omgeving van de wederpartij te beleggen bij het Landelijk Bureau Bibob.”

(beide citaten uit: Procesbeschrijving RIEC ondersteuning Bibob)

Grondslag voor het verstrekken van gegevens aan en het inzetten van het LBB is gelegen in Artikel 27 jo Artikel 9 Wet Bibob

De adviesaanvraag wordt digitaal ingediend. Zodra de stukken geüpload zijn, ontvangt het LBB een melding. Zowel het Bibob-advies als andere documenten stuurt het LBB ook weer via Bestandenpostbus terug. Wanneer het LBB stukken heeft geüpload, wordt er een melding gestuurd via e-mail.

Doel	Advies aanvragen bij het LBB
Wie voert uit	Infodesk-medewerker Bibob
Welke info kan worden opgevraagd in deze stap	Art. 27 Wet Bibob
LBB	Welke info: Advies LBB Hoe op te vragen: Aanvraag via Bestandenpostbus inclusief volledig dossier uploaden Aanvullende afspraken: advies komt ook retour via Bestandenpostbus
Mogelijke uitkomsten	Door naar volgende stap (stap 5, beslissing)
Privacy afweging	N.v.t.

5- BESLISSING

In deze processtap wordt de beslissing vastgelegd en gemotiveerd.

Afhankelijk van de bevindingen uit het eigen onderzoek eventueel aangevuld met het advies van het LBB, wordt de beslissing bepaald. Deze kan zijn:

- Verlenen
- Verlenen onder voorwaarden
- Afwijzen o.b.v. Bibob grond
- Afwijzen o.b.v. strafbaar feit ter verkrijging vergunning
- Buiten behandeling laten o.b.v. AWB

Doel	Beslissen zodat beschikking kan worden opgemaakt
Wie voert uit	Infodesk-medewerker Bibob
Welke info kan worden opgevraagd in deze stap	-
Mogelijke uitkomsten	Beslissing
Privacy afweging	Nvt

2.3 Informatievoorziening burger

2.3.1 Generieke informatie verstrekking

Het Gemeentelijk Bureau Bibob (GBB) en de samenwerking met het Landelijk Bureau Bibob (LBB) wordt toegelicht op de website van gemeente Den Haag, in de stad, ondernemen, gemeentelijk bureau Bibob³.

De werking van de Wet Bibob wordt verder uitgebreid toegelicht op de website van gemeente Den Haag, in de stad, ondernemen, Wet Bibob⁴. Hier wordt de burger ook verwezen naar de informatie over het LBB op de site van Justis.nl

Hiermee wordt invulling gegeven aan de transparantie verplichting uit de AVG.

³ <https://www.denhaag.nl/nl/in-de-stad/ondernemen/gemeentelijk-bureau-bibob.htm>

⁴ <https://www.denhaag.nl/nl/in-de-stad/ondernemen/wet-bibob.htm>

2.3.2 Specifieke informatieverstrekking

Tijdens de aanvraag van een overheidsbeslissing (in het kader van een beschikking, subsidie, overheidsopdracht of vastgoedtransactie) wordt de aanvrager gewezen op de Bibob-toets die zal plaatsvinden. Betrokkene wordt middels een notificatiebrief vanuit de burgemeester wederom geïnformeerd indien er advies wordt gevraagd aan het LBB. Ook als een onderzoek plaatsvindt naar aanleiding van een signaal, bijvoorbeeld naar aanleiding van een tip van het OM, wordt betrokkene op overeenkomstige wijze geïnformeerd.

2.4 Verstrekkingen aan (keten)partners

Binnen het Bibob-proces is sprake van twee type verstrekkingen naar (keten)partners buiten het gemeentelijke domein;

VERSTREKKING AAN EEN ANDERE DEELNEMER VAN HET RIEC

In de wet Bibob is in artikel 7 lid 6 jo 28 lid 2 onder d van de Wet Bibob bepaald dat het bestuursorgaan bevoegd is om de gegevens die het in het kader van het eigen Bibob-onderzoek over betrokkene(n) heeft verzameld, dan wel het advies dat het Landelijk Bureau Bibob over betrokkene(n) en derden heeft uitgebracht, door te verstrekken aan een andere deelnemer van een regionaal samenwerkingsverband voor de aanpak van georganiseerde criminaliteit, voor zover deze gegevens noodzakelijk zijn voor het ondersteunen van het bestuursorgaan bij het toepassen van deze wet. (zie procesbeschrijving Bibob ondersteuning door bestuursorgaan van het RIEC⁵) Deze verstrekingsgrondslag is ook van belang bij de stap in het Bibob-proces waar de gemeentelijk Bibob medewerker informatie opvraagt bij de politie, het OM, of de Belastingdienst (zie uitwerking hieronder). En meer in het algemeen wanneer het bestuursorgaan de ondersteuning van het RIEC inroept bij de uitvoering van het gemeentelijke deel van het Bibob proces.

⁵ <https://www.riec.nl/maatregelen-en-documenten/documenten/publicaties/2019/08/15/procesbeschrijving-bibob-ondersteuning-door-bestuursorgaan>

VERPLICHTE VERSTREKKING AAN HET LANDELIJK BUREAU BIBOB (LBB) OP VERZOEK

De verstrekking van informatie aan het LBB heeft een expliciete grondslag in artikel 27 van de Wet Bibob. Daar is bepaald dat verschillende bestuursorganen verplicht zijn om desgevraagd gegevens aan het LBB te verstrekken. (Gezien deze wettelijke verplichting is sprake van rechtmatige verstrekking in de zin van artikel 6, eerste lid, onder c, van de Algemene verordening gegevensbescherming (AVG)) De gegevens moeten noodzakelijk zijn voor de totstandkoming van de adviezen van het LBB. Inhoudelijk is de informatie die verstrekt moet worden niet beperkt. (zie Factsheet Gegevensverstrekking en Wet-Bibob (bestuursorganen) ⁶)

6

[https://www.iustis.nl/binaries/Factsheet%20Gegevensverstrekking%20en%20de%20Wet%20Bibob%20\(bestuursorganen\)%20%20aug_tcm34-342088.pdf](https://www.iustis.nl/binaries/Factsheet%20Gegevensverstrekking%20en%20de%20Wet%20Bibob%20(bestuursorganen)%20%20aug_tcm34-342088.pdf)

3 HET RIEC LIAISON PROCES

3.1 Juridisch kader & ontwikkeling

Voor achtergrond en informatie over de Regionale Informatie- en Expertise Centra (RIEC's) en het Landelijk Informatie- en Expertise Centrum (LIEC); zie www.RIEC.nl.

Binnen het RIEC, is de gemeente een van de samenwerkingspartners. De gemeente wordt binnen het RIEC vertegenwoordigd door de RIEC Liaison. De RIEC Liaison (werkzaam binnen de infodesk) vertegenwoordigt de gemeente in het RIEC.

Binnen het samenwerkingsverband RIEC wordt samengewerkt op basis van het Convenant ten behoeve van Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingssknelpunten en Bevordering Integriteitsbeoordelingen. RIECs hebben formeel geen wettelijke grondslag op basis waarvan zij gegevens kunnen uitwisselen. De wettelijke grondslag voor verwerking binnen het RIEC wordt in de toekomst gecreëerd in Wet Gegevensuitwisseling Samenwerkingsverbanden (WGS). WGS is nog niet door consultatie heen. Tot die tijd wordt het RIEC convenant en bijbehorende privacy protocol als uitgangspunt gehanteerd.

Convenant ten behoeve van de Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit

In dit Convenant wordt invulling gegeven aan artikel 26 AVG. Hierin is bepaald dat de verwerkingsverantwoordelijken, zijnde de convenantpartners, verplicht worden op transparante wijze hun verantwoordelijkheden voor de nakoming van de Verordening vast te stellen, met name met betrekking tot de uitoefening van de rechten van betrokkenen.

Privacyprotocol RIEC's-LIEC

Het Privacyprotocol RIEC's-LIEC is onderdeel van het convenant. Het Privacyprotocol:

- bevordert de zorgvuldige verwerking van persoonsgegevens;
- is een verdere uitwerking van het Convenant;
- beschrijft de manier waarop de convenantpartners in het samenwerkingsverband persoonsgegevens delen;
- is integraal van toepassing op alle RIEC's en beschrijft eenduidig de werkwijze van alle RIEC's.

Uitwerking hieronder van het RIEC Liaison proces gaat in op het intern gemeentelijke deel van het RIEC proces, binnen gemeente Den Haag.

3.2 Het Proces

Het “Werkproces integrale casusaanpak door het Regionaal Informatie en Expertise Centrum (RIEC)”⁷, zoals dat in 2019 is gepubliceerd, vormt de basis voor de verdere beschrijving van het RIEC Liaison proces.

Essentiële zaken die daarin beschreven staan, zijn:

- De beschrijving van de fasering in de informatievergaring, waarbij de eerste stap de vergaring van informatie vanuit de gemeente is.
- De juridische toets die daarin is opgenomen ten aanzien van òf gegevens uit verschillende bronbestanden verstrekt mogen worden in het kader van de RIEC aanpak (de verenigbaarheidstoets conform Art 6 lid 4 AVG) die daarin is uitgevoerd
- De daarin opgenomen analyse van de 8 bronbestanden waarvan gebruik gemaakt kan worden, afgeleid van de paragraaf 6.1 van het Privacyprotocol RIEC’s-LIEC, dd. april 2020⁸

In het hiervoor genoemde “Werkproces integrale casusaanpak” wordt gesproken over de informatievergaring bij de gemeente als fase 1 van het proces, waarin de verschillende open en gesloten gemeentelijke bronnen worden geraadpleegd.

Binnen RIEC Haaglanden is ervoor gekozen om deze eerste fase van het werkproces op te delen in twee fasen; een QuickScanfase en een Informatieverzoek fase.

Hierbij komt de Informatieverzoekfase overeen met wat in het algemeen aangeduid wordt als fase 1 van het RIEC werkproces casusaanpak.

De Quickscanfase is een verkorte uitvraag die voorafgaat aan de werkelijke informatieverzoek fase, met als doel vast te stellen òf het relevant is de gemeente te betrekken bij de casusaanpak.

⁷ <https://www.riec.nl/documenten/publicaties/2019/08/15/procesbeschrijving-integrale-casusaanpak>

⁸ <https://www.riec.nl/documenten/richtlijnen/2020/04/17/privacyprotocol-april-2020>

De Quickscanfase wordt doorgaans binnen 1 week doorlopen en geeft daarmee snel uitsluitsel over òf deelname vanuit de gemeente noodzakelijk is.

De beantwoording van een informatie verzoek kost doorgaans afhankelijk van de casus/het signaal (veel) meer tijd.

Naast dat het splitsen in twee fasen bijdraagt aan de proportionaliteit, zorgt het eveneens voor een efficiëntere werkbelasting, doordat alleen voor casuïstiek waarbij de gemeente ook werkelijk een bijdrage gaat leveren, de gegevens worden verzameld, geduid en verstrekt aan het RIEC.

Spoorhouders

Binnen de gemeente Den Haag is ervoor gekozen om gebruik te maken van spoorhouders, die op verzoek van de RIEC liaison, de achterliggende bronsystemen kunnen raadplegen. Deze systemen hebben betrekking op de verschillende (wettelijke) bronbestanden. Hiervoor is gekozen enerzijds om ervoor te zorgen dat de RIEC liaison geen toegang voor al deze systemen benodigd heeft. Anderzijds zijn de spoorhouders beter in staat om voor hun eigen domein informatie te duiden ten behoeve van ondermijning. Per domein is derhalve een spoorhouder aangewezen die in de praktijk de RIEC liaison ondersteunt in het (RIEC) proces.

Quickscanfase

In de Quickscanfase wordt nog niet alle gemeentelijke informatie uit de 8 informatiebronnen bijeengebracht, maar staan de volgende 3 vragen centraal:

- is er informatie aanwezig binnen de gemeente betreffende het signaal
- is er belang bij de gemeente om deel te nemen aan het casusoverleg
- zijn er voor de gemeente interventiemogelijkheden inzake het signaal

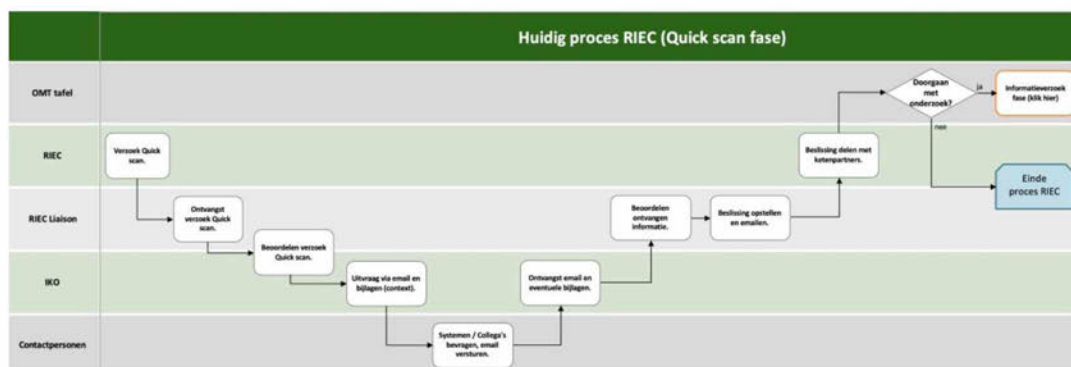
De RIEC Liaison ontvangt een QuickScan verzoek via RIEC-IS en krijgt daarvan een notificatie per email. De RIEC Liaison⁹ vraagt daarop de spoorhouders om de verschillende onder hun verantwoordelijkheid vallende bronbestanden/systemen te raadplegen. In dit stadium worden echter nog geen gegevens verstrekt door de spoorhouders. Zij beantwoorden de vragen van de RIEC Liaison (is er informatie, is er belang en is er interventie mogelijkheid) alleen met ja of nee. De RIEC Liaison inventariseert de antwoorden van de verschillende spoorhouders en besluit op basis

⁹ De RIEC liaison wordt in de praktijk ondersteund door de informatieondersteuner. Deze werkt onder de verantwoordelijkheid van de RIEC liaison.

daarvan of het voor de gemeente relevant is om aan te sluiten bij de eventuele casusaanpak vanuit het RIEC. Met deze informatie wordt vervolgens binnen het RIEC aan de ondermijningstafel in overleg met de overige partners besloten of het signaal tot een casus leidt, welke partijen daaraan gaan deelnemen en wie de regie op de aanpak neemt.

Indien besloten wordt tot een casusaanpak vanuit het RIEC, wordt overgegaan tot de volgende fase en wordt een informatieverzoekfase gestart.

Omdat de ondermijningstafel slechts periodiek plaatsvindt, kan het in de praktijk voorkomen dat de accountmanager RIEC, op basis van reeds ontvangen reacties op de QuickScan, vooruitlopend op de ondermijningstafel beslist om een informatieverzoek uit te zetten bij de partners.

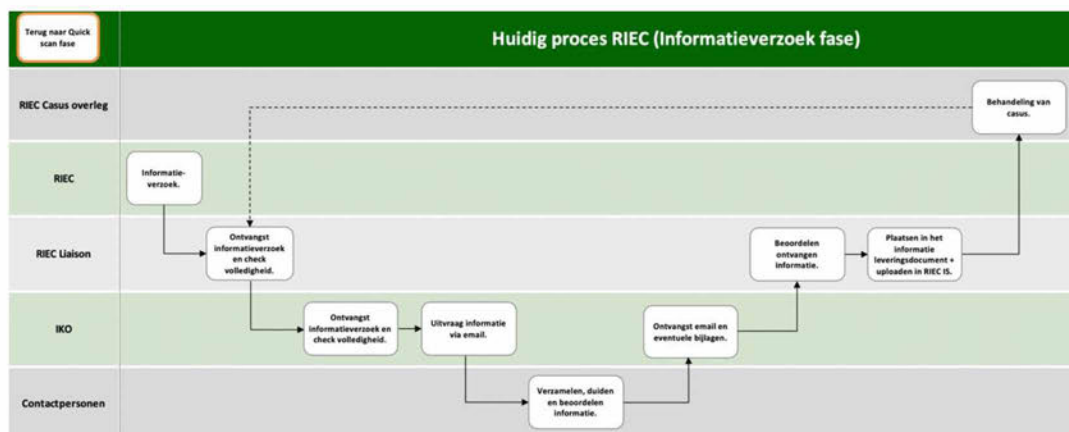


Informatieverzoekfase

Nadat aan de Ondermijningstafel is besloten dat een casusaanpak vanuit het RIEC noodzakelijk is, ontvangt de RIEC Liaison via RIEC-IS een Informatieverzoek. Daarop zal de RIEC Liaison de spoorhouders verzoeken om de onderliggende informatie te verstrekken ten behoeve van de casusaanpak. Hierbij worden in principe alleen die spoorhouders gevraagd die tijdens de quickscan fase hebben aangegeven over informatie te beschikken.

Nadat alle informatie van de spoorhouders is ontvangen wordt deze in RIEC-IS verzameld/samengebracht door de RIEC Liaison.

Deze informatie wordt via RIEC-IS alleen verstrekt aan (raadpleegbaar gemaakt voor) bij de casus betrokken RIEC partners.



3.2.1 Privacy afwegingskader RIEC Liaison proces

Door een Quickscan uit te voeren voorafgaand aan het informatieverzoek, wordt invulling gegeven aan de vereisten van proportionaliteit en subsidiariteit.

Op basis van de resultaten van de Quickscan kan aan de ondermijningstafel van het RIEC beter afgewogen worden of het voor de gemeente noodzakelijk is om deel te nemen aan de casusaanpak. Pas wanneer daartoe besloten is, wordt overgegaan tot het daadwerkelijk opvragen van de informatie middels een informatieverzoek.

De spoorhouder ontvangt een beperkte set aan informatie ter toelichting op het signaal: subjecten (personen en/of bedrijven), objecten (panden en adressen), korte beschrijving verdenking en eventueel informatie uit open bronnen zoals verstrekt door het RIEC. Voordat een signaal wordt gedeeld met de gemeente, voert het RIEC een intake uit. Uit deze intake kan meer informatie blijken dan gedeeld wordt bij het uitzetten van het QuickScan verzoek. In sommige gevallen kan de RIEC liaison besluiten deze aanvullende informatie te delen met de spoorhouder(s). In dat geval zal altijd, ter verantwoording voor het delen van deze informatie, door de RIEC liaison een (korte) motivering moeten worden genoteerd (in het dossier).

3.2.2 Het proces in stappen

1- STAP 1: QUICKSAN VERZOEK

Doel	Vaststellen deelname gemeente bij casusaanpak
Wie voert uit	RIEC Liaison ism Spoorhouders

Welke info kan worden opgevraagd in deze stap	Of er binnen de gemeente, voor het signaal relevante, informatie aanwezig is en of er belang is deel te nemen aan een casusaanpak.
• Spoorhouders: <i>Voor overzicht welke spoorhouders geraadpleegd worden en welke bronnen geraadpleegd worden, zie paragraaf 3.2.3 "Overzicht bronsystemen – Wetgeving - Spoorhouders – Bronsystemen"</i>	Welke info; <i>Aanwezigheid, belang, interventie mogelijkheid: ja/nee</i> Hoe op te vragen; <i>RIEC Liaison stuurt verzoek (huidig via email) naar de Spoorhouders, die vervolgens de achterliggende bronsystemen bevragen</i> Aanvullende afspraken (Nog te implementeren); • De subject/object/signaal informatie die de spoorhouders ontvangen, waarover de QS vragen gesteld worden, zijn vertrouwelijk. In afspraken met de spoorhouders moet hier invulling aan gegeven worden. Bijvoorbeeld door overeen te komen dat deze informatie na beantwoorden van de vragen verwijderd wordt / niet bewaard wordt door de spoorhouders. • Er moeten nadere afspraken worden gemaakt over gebruik veilige email, of gedeeld zaaksysteem
Mogelijke uitkomsten	Op basis van de informatie die de RIEC Liaison ontvangt van de verschillende spoorhouders, besluit de RIEC Liaison gemeente-breed terug te koppelen aan het RIEC: • Wel/geen informatie. • Bij wel informatie; wel/geen belang bij casus betrokken te worden • Bij wel informatie en wel belang; wel/geen interventiemogelijkheden.

2- STAP 2: INFORMATIE VERZOEK

Doel	Voldoen aan informatieverzoek. Verzamelen, duiden en verstrekken van voor de casusaanpak noodzakelijke gegevens
Wie voert uit	RIEC Liaison ism Spoorhouders
Welke info kan worden opgevraagd in deze stap	Voor het signaal relevante informatie vanuit de verschillende bronbestanden wordt verzameld en geduid.
• Spoorhouders: Voor overzicht welke spoorhouders geraadpleegd worden en welke bronnen geraadpleegd worden, zie paragraaf 3.2.3 “Overzicht bronsystemen – Wetgeving - Spoorhouders – Bronsystemen”	Welke info; Gegevens uit de betreffende bronsystemen voor zover deze relevant/noodzakelijk zijn voor de casusaanpak naar aanleiding van het signaal. Hoe op te vragen; RIEC Liaison stuurt informatieverzoek (huidig via email) naar de Spoorhouders (die in de QS fase hebben aangegeven over relevante informatie te beschikken), die vervolgens de achterliggende bronsystemen raadplegen om de gegevens te verzamelen en nader te duiden. Aanvullende afspraken (Nog te implementeren); • De subject/object/signaal informatie die de spoorhouders ontvangen, waarover de QS vragen gesteld worden, zijn vertrouwelijk. In afspraken met de spoorhouders moet hier invulling aan gegeven worden. Bijvoorbeeld door overeen te komen dat deze informatie na beantwoorden van de vragen verwijderd wordt / niet bewaard wordt door de spoorhouders. (en afspraken over gebruik veilige email, of gedeeld zaaksysteem?)

Mogelijke uitkomsten	RIEC Liaison consolideert de van de spoorhouders ontvangen informatie en registreert deze in RIEC-IS
Privacy afweging	Toets op relevantie van de informatie in het kader van het signaal door de RIEC Liaison

3.2.3 Overzicht bronsystemen – Wetgeving - Spoorhouders – Bronsystemen

Welke bronbestanden door de Spoorhouders geraadpleegd mogen worden is overgenomen uit het “Werkproces integrale casusaanpak door het Regionaal Informatie en Expertise Centrum (RIEC)”. Hierin is een uitvoerige analyse opgenomen ten aanzien van welke gegevens uit welke bronbestanden kunnen worden verstrekt aan de RIEC samenwerkingspartners in het kader van de integrale casusaanpak door het RIEC.

#	Bronbestanden	Dienst	Wetgeving	Spoorhouder	Bronstelsysteem
1	BRP-gegevens	DPZ/KCC	-Wet basisregistratie personen -Besluit basisregistratie personen	5.1.2.e 5.1.2.e 5.1.2.e 5.1.2.e	BRP Akten Burgerlijke Stand
2	Gegevens betreffende vergunningen	BSD	-Verschillende wetten waaronder: Drank- en Horecawet, Wet op de kansspelen en de Algemene Plaatselijke Verordening (let daar op artikel 437 lid 2 Wetboek van Strafrecht) -Artikel 28 lid 2 onder d jo. Artikel 30 lid 6 Wet Bibob	5.1.2.e 5.1.2.e	De info is afkomstig uit Digi-As en een afgeschermd map op de G-schijf (alleen de mensen van team Bibob mogen bij deze informatie).
3	Gegevens betreffende subsidieaanvragen en verstrekkingen				
4	Gemeentelijke belastinggegevens	DPZ Belasting-zaken	convenant		IBS

5	Gegevens bestuurlijke handhaving		-Artikel 13b Opiumwet -Artikel 3, 38 en 41 Drank- en horecawet -Artikel 34 Wet op de kansspelen -Artikel 437 lid 2 Wetboek van Strafrecht -Artikel 172 en 172a Gemeentewet -Artikel 149 jo 151a Gemeentewet -Artikel 17 Woningwet -Artikel 2 jo. Artikel 8 jo. Artikel 9 jo. Artikel 10 Huisvestingswet	X HHO HHO X X X X X	CityControl
6	Gegevens omtrent bezwaarschriften			.	
7	Gegevens betreffende klachten/meldingen openbare orde en veiligheid		Artikel 172 Gemeentewet	.	
8	Gegevens ruimtelijke ontwikkeling vastgoed		Artikel 92 Woningwet 2015 jo. Artikel 1.1. lid 1 Wet algemene bepalingen omgevingsrecht		

3.3 Informatievoorziening burger

3.3.1 Generieke informatie verstrekking

Momenteel wordt de burger, op de website van de gemeente Den Haag, niet geïnformeerd over het RIEC proces of de deelname van de gemeente Den Haag daaraan. Wel is er een pagina "Haags veiligheidsbeleid" waar de 3 sporen aanpak wordt beschreven.

In het kader van transparantie naar betrokkenen zou dit een logisch plek zijn om bijvoorbeeld onder punt 3 "integrale aanpak van ondermijning", toe te voegen:

"De gemeente werkt samen met andere partijen in het RIEC. Voor meer informatie zie www.riec.nl."

In aanvulling hierop wordt in artikel 15 lid 2 van het Privacy Protocol het volgende gelezen over de algemene informatievoorziening aan betrokkene(n).

‘In het belang van de algemene transparantie over de geïntegreerde aanpak van de georganiseerde criminaliteit worden het Convenant, Privacyprotocol en de werkprocessen van de RIECs gepubliceerd op de websites van alle RIECs en alle convenantpartijen’.

3.3.2 Specifieke informatieverstrekking

Regie op het proces ligt bij het RIEC. Daar wordt ook besloten of/wanneer betrokkene wordt geïnformeerd over een onderzoek. Dit valt buiten de verantwoordelijkheid van de gemeente Den Haag als deelnemer aan het RIEC proces. In artikel 15 lid 1 jo. 11.3 van het Privacy Protocol is besloten dat het subject (de betrokkene) in principe geïnformeerd wordt op het moment dat er interventie wordt uitgevoerd. Indien interventie achterwege blijft, dient het subject binnen een termijn van een maand geïnformeerd te worden over het onderzoek. Dit kan in bepaalde gevallen tijdelijk achterwege worden gelaten op grond van artikel 41 UAVG (in het belang van het o.a. onderzoek).

3.4 Verstrekkingen aan (keten)partners

Anders dan aan het samenwerkingsverband RIEC (en daarmee dus aan de deelnemers aan het RIEC), vinden er geen verstrekkingen plaats.

4 BINNENGEMEENTELIJKE GEGEVENSUITWISSELING IN HET KADER VAN AANPAK CRIMINELE ONDERMIJNING

4.1 Juridisch kader en ontwikkelingen

Februari 2020 is het Model privacy protocol binnengemeentelijke gegevensdeling aangeboden aan de Tweede Kamer, door de Minister van Veiligheid en Justitie.

Het protocol is opgesteld in opdracht van het Strategisch Beraad Ondermijning (SBO) en besproken in een klankbordgroep waarin gemeenten, de Vereniging Nederlandse Gemeenten (VNG) en de Autoriteit Persoonsgegevens (AP) hebben deelgenomen. Zowel de VNG als de AP hebben aangegeven waardering te hebben voor het modelinformatieprotocol en zien dit als belangrijke stap die meer duidelijkheid schept op het gebied van informatiedeling.

Dit modelprotocol (dat op zichzelf is afgeleid van het RIEC's/LIEC protocol) vormt de basis voor de hierop volgende uitwerking van het binnengemeentelijke proces aanpak criminele ondermijning Den Haag

Implementatie van het Proces Overig binnen gemeente Den Haag

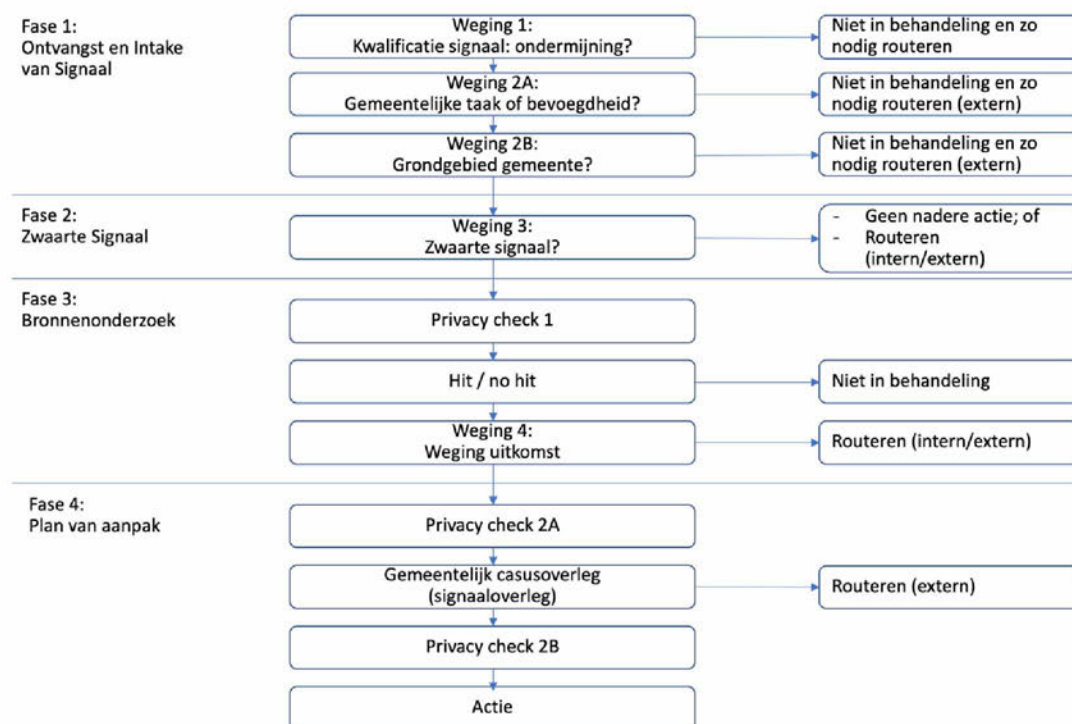
Gemeente Den Haag heeft eind 2020 nog geen gestructureerde werkwijze ten aanzien van het omgaan met interne signalen die (kunnen) duiden op criminele ondermijning. Het oppakken van deze signalen binnen de Infodesk gaat lopen via het "Overige werkproces". Hierin worden gemeentelijke signalen, meldingen en informatieverzoeken opgepakt die binnenkomen via de MeV-App, MMA-meldingen en ^{5.1.2.e} @denhaag.nl.

Ambitie is het proces hiervoor begin 2021 te implementeren op basis van het Modelprotocol. Onderstaande uitwerking van het proces is – met kleine aanpassingen - overgenomen uit het modelprotocol. *Verdere uitwerking hiervan is in afwachting van de implementatie binnen gemeente Den Haag.*

4.2 Het proces

Het proces start naar aanleiding van een signaal of een vermoeden, ontvangen van een burger of een professional. De scope is daarbij heel breed.

Het proces wordt gekenmerkt door een combinatie van een 'gefaseerde, stapsgewijze aanpak' en verschillende rechtmatigheidswaarborgen. Door de gefaseerde aanpak wordt bovenmatige gegevensverwerking voorkomen (alleen verwerken wat noodzakelijk is). De rechtmatigheidswaarborgen (de Privacy checks) zijn ingebouwd in het proces om te borgen dat gehandeld wordt op een wijze die in lijn is met de AVG en UAVG en met de sectorale wetgeving waaruit de te gebruiken gegevens veelal afkomstig zijn.



4.2.1 Privacy afwegingskader Binnengemeentelijk bestuurlijk proces;

Gedurende het proces, wordt in de verschillende stappen telkens besloten of het noodzakelijk is om het signaal/vermoeden verder te onderzoeken, niet verder te behandelen, of te routeren naar een andere partij binnen of buiten de gemeente.

De privacy afwegingen zullen telkens per stap in het proces toegelicht worden.

Het (zaak- of dossier-)systeem zal ondersteuning moeten bieden voor het gaandeweg vastleggen van de afweging die geleid heeft tot een bepaald procesverloop. Daar waar besloten wordt

gegevens op te vragen, kan dan onderbouwd worden waarom deze gegevens voor het onderzoek noodzakelijk zijn. Dit ter verantwoording van de gemaakte keuzes achteraf.

4.2.2 Het proces in stappen

WEGING 1: KWALIFICATIE SIGNAAL: ONDERMIJNING?

Het signaal wordt na ontvangst beoordeeld door de regisseur ondermijning. Voor de beoordeling van een signaal is van belang wat het signaal inhoudt en of het betrekking heeft op ondermijning. Dat betreft de **eerste weging**. Een signaal wordt bij intake beoordeeld op grond van een aantal kenmerken en indicatoren.

Deze signaalanalyse is nader uitgewerkt in bijlage 1 (van het model protocol): de 'Checklist ten behoeve van de signaalanalyse'. De beoordeling van een signaal vindt plaats binnen het kader 'ondermijnende criminaliteit'. In aanvulling hierop is tenminste sprake van één van de indicatoren 'situationele en lokale verankering'. Daarna wordt gekeken naar de indicatoren 'signalering', die nader uitgewerkt zijn in een lijst met 'red flags'.

Zodra aan de hand van bijlage 1 (van het model protocol) – die geen limitatief overzicht bevat en die ook kan worden aangepast al naar gelang de eigen gemeentelijke praktijk en ervaringen – is vastgesteld dat sprake is van een ondermijningssignaal, vindt de **tweede weging** plaats.

De tweede weging valt uiteen in twee delen: weging 2A en weging 2B.

WEGING 2A: GEMEENTELIJKE TAAK OF BEVOEGDHEID?

Weging 2A betreft de vraag of het binnengekomen signaal betrekking heeft op een taak of bevoegdheid van de gemeente, en niet op een taak of bevoegdheid van een andere instantie (bijvoorbeeld van de politie, kinderbescherming, etc.). Het is hierbij dus van belang na te gaan of het signaal in beginsel tot gemeentelijk optreden kan leiden. Een dergelijke gemeentelijke taak is bijvoorbeeld een van de openbare orde- bevoegdheden van de burgemeester.

Vervolgens zijn er twee opties:

- Het signaal kan mogelijk aanleiding vormen voor inzet van een gemeentelijke taak of bevoegdheid. In dat geval wordt overgegaan naar weging 2B;

- Het signaal kan geen aanleiding vormen voor inzet van een gemeentelijke taak of bevoegdheid. Het signaal wordt niet in behandeling genomen door de gemeente en zo nodig doorverwezen naar de bevoegde instantie.

WEGING 2B: GRONDGEBIED GEMEENTE?

Weging 2B betreft de vraag of het signaal betrekking heeft op het grondgebied van de gemeente. Het gaat, met andere woorden, om de vraag of het subject of object waar het signaal betrekking op heeft binnen de gemeente woont respectievelijk is gevestigd. De volgende vragen moeten daarbij achtereenvolgend worden beantwoord:

1. Gaat het om een object of een subject?
2. In het geval van een object: is het object binnen de gemeentegrenzen gelegen (dan wel is er anderszins een link met de gemeente)?
3. In het geval van een subject: is het subject woonachtig binnen de gemeentegrenzen (dan wel is er anderszins een link met de gemeente)?

Deze vragen worden beantwoord aan de hand van informatie uit openbare bronnen zoals de basisregistraties. Daarbij zullen in ieder geval het handelsregister van de Kamer van Koophandel, het Kadaster, de Basisregistratie personen (BRP) en de Basisregistratie adressen en gebouwen (BAG) vaak van belang zijn.

Ook nu zijn er weer twee opties:

- Het signaal heeft betrekking op het grondgebied van de gemeente. In dat geval gaat men door naar fase 2;
- Het signaal valt buiten het grondgebied van de gemeente. Het signaal wordt niet in behandeling genomen door de gemeente en zo nodig doorverwezen naar een andere gemeente of instantie.

WEGING 3: ZWAARTE SIGNAAL?

In **fase 2** vindt de beoordeling van signalen van burgers en professionals plaats. Hier vindt dan ook de **derde weging** plaats. De gemeente weegt de zwaarte van het signaal en beoordeelt waar het signaal het beste kan worden afgehandeld.

De gemeente zou ten aanzien van de 'zwaarte-weging' kunnen vastleggen, bijvoorbeeld in gemeentelijk beleid, hoe een dergelijke weging, aansluitend bij lokale omstandigheden, wordt

uitgevoerd en welke factoren daarbij relevant zijn, zoals 'is het signaal voldoende concreet?' 'is het signaal van recente datum?', 'heeft het signaal betrekking op een onderwerp ter zake waarvan een trend- en fenomeenanalyse is uitgevoerd waaruit blijkt dat er bijzondere aandacht voor een bepaald fenomeen vereist is?', etc. Ook kan in dit beleid worden opgenomen onder welke omstandigheden in aanvullende openbare bronnen, waaronder op internet, onderzoek kan worden gedaan naar het signaal. Het zal in beide gevallen steeds moeten gaan om objectieve criteria.

Na deze tweede weging volgt een beslismoment bij het ondermijningsteam:

- er gebeurt niets met het signaal. Het signaal wordt niet in behandeling genomen (waarbij het signaal gedurende een jaar versleuteld bewaard wordt en daarna vernietigd wordt); of
- een signaal wordt naar een gemeentelijk onderdeel gestuurd dat de regie vervolgens voert; of
- een signaal wordt naar het RIEC gestuurd dat de regie vervolgens voert; of
- er volgt een vervolganalyse, waarmee fase 3 ingaat.

PRIVACY CHECK 1

In **fase 3** van het protocol bepaalt de privacy officer in het kader van **Privacy check 1** (zie daarover 4.2.3) of en zo ja welke gemeentelijke bronnen naar aanleiding van het concrete signaal kunnen worden geraadpleegd en...

HIT / NO HIT

...na raadpleging van de betrokken gemeentelijke bronnen door middel van een hit/no hit- vraag, welke gegevens relevant zijn voor het signaal. Soms zal aan de hand van 'dat'- informatie kunnen worden geconstateerd dat verdere 'wat-informatie' niet nodig is, bijvoorbeeld als uit de 'dat-informatie' blijkt dat het om (te) oude informatie gaat. In dat geval zal geen 'wat-informatie' mogen worden opgevraagd. Onderdeel van de hit/no hit-check is de beoordeling of het om voor het signaal relevante informatie gaat.

- Als van een persoon bepaalde, voor het signaal relevante, gegevens in een bronbestand van een gemeentelijk onderdeel voorkomen, is sprake van een 'hit': de betrokken persoon/bepaalde info is bekend binnen het betreffende gemeentelijke domein. Zie hierna voor de vervolgstappen.
- Als er geen hit is dan wordt verder geen actie ondernomen: het signaal wordt niet in behandeling genomen.

WEGING 4: WEGING UITKOMST

Bij een hit volgt de **vierde weging**, waarbij de uitkomsten van de hit(s) worden gewogen. Concreet gaat het om de vraag of de hit(s) een signaal in voldoende mate bevestigen om door te gaan met het onderzoek naar het signaal. De analyse leidt tot:

1. een mono- of multidisciplinaire aanpak door één gemeentelijk onderdeel of meerdere samenwerkende gemeentelijke onderdelen: er hoeft geen ondermijnende activiteit te zijn, de regie en uitvoering liggen bij desbetreffend gemeentelijke onderdeel/onderdelen op grond van de daarvoor bedoelde wettelijke bevoegdheid(heden). Hierbij is een regierol vanuit het ondermijningsteam niet benodigd;
2. het gemeentelijk casusoverleg met betrokken afgevaardigden van de desbetreffende gemeentelijke onderdelen waar sprake is van een relevante hit en waarbij de regie bij het ondermijningsteam ligt. Dit is dan op grond van het gegeven dat het signaal en de informatie uit de fases 1, 2 en 3 op ondermijning duiden. Het vormt de start van fase 4;
3. doorgeleiding naar het RIEC-samenwerkingsverband, omdat er sprake is van georganiseerde criminaliteitsverband waarvoor de partners in het RIEC benodigd zijn.

PRIVACY CHECK 2A

Fase 4 van het protocol gaat over het ontwikkelen van een plan van aanpak en het voeren van regie op het plan en het afsluiten van de casus. Voorafgaand aan het gemeentelijk casusoverleg (signaaloverleg) voert de privacy officer **Privacy check 2A** uit (zie daarover 4.2.3): er wordt vastgesteld of en zo ja, welke van de in de fases 1 t/m 3 verzamelde gegevens mogen worden gedeeld met het/de relevante, bij het signaal betrokken, gemeentelijke onderdeel/onderdelen ten behoeve van de verdere aanpak. De privacy officer kan daarbij ook beoordelen of eventuele onderliggende gegevens uit een concreet dossier voor de verdere aanpak van de casus binnengemeentelijk mogen worden gedeeld en zo ja, met welk gemeentelijk onderdeel/welke gemeentelijke onderdelen.

GEMEENTELIJK CASUSOVERLEG (SIGNAALOVERLEG)

Terzijde: tijdens het signaaloverleg kan alsnog blijken dat er geen binnengemeentelijke actie vereist is, maar dat het signaal bij het RIEC moet worden ingebracht.

PRIVACY CHECK 2B

Als de (gezamenlijke of volgordelijke) aanpak op basis van het signaaloverleg is bepaald en duidelijk is welke concrete aanpak en bevoegdheden de gemeente wil inzetten en welke binnengemeentelijke gegevensuitwisseling daarvoor nodig is, controleert de privacy officer tot slot of de verzamelde gegevens mogen worden gedeeld met het relevante gemeentelijke onderdeel/de relevante gemeentelijke onderdelen ten behoeve van de verdere aanpak en beoogde inzet van bevoegdheden door die gemeentelijke onderdelen. Deze beoordeling vindt opnieuw plaats aan de hand van de bij de privacy checks te stellen vragen. Dit betreft **weging 5**.

ACTIE

4.2.3 Toelichting op de privacy checks in het proces

Uitwerking van de twee privacy checks in fase 3 en 4

In **fase 3** van het protocol bepaalt de privacy officer in het kader van **Privacy check 1** of en zo ja welke gemeentelijke bronnen naar aanleiding van het concrete signaal kunnen worden geraadpleegd. In **fase 4** stelt de privacy officer in het kader van **Privacy check 2** vast:

- i) welke in de fases 1 t/m 3 verzamelde gegevens met de relevante, bij het signaal betrokken, gemeentelijke onderdelen mogen worden gedeeld ten behoeve van de vaststelling van de verdere aanpak; en
- ii) welke binnengemeentelijke gegevensuitwisseling nodig is voor het verwezenlijken van die aanpak en of dat toelaatbaar is.

De vraag welke binnengemeentelijke gegevensdeling is toegestaan moet steeds worden beantwoord aan de hand van de specifieke wettelijke regeling die op de betreffende gemeentelijke informatie van toepassing is.

Dat is nog niet zo eenvoudig: niet alleen zijn op de verschillende soorten gemeentelijke bronnen verschillende wettelijke regelingen van toepassing, ook is iedere casus anders en zal daarom steeds een op het geval toegespitste afweging moeten worden gemaakt. Er is dan ook niet één simpel antwoord te geven op de vraag wie, wanneer, welke informatie binnen de gemeente mag delen ter bestrijding van ondermijning.

Privacy check 1 (start van fase 3)

Privacy check 1 vormt de belangrijkste privacybeoordeling en vindt plaats in het kader van de hit/no hit-analyse (start van fase 3). Per geval moeten steeds de volgende privacyvragen worden beantwoord.

A. Wat is de wettelijke basis voor het primaire gebruik?

Allereerst wordt bepaald welke gegevens nodig zijn voor het onderzoek naar een signaal. Op basis daarvan wordt vastgesteld op basis van welke gemeentelijke taak deze gegevens aanvankelijk zijn verkregen (ook wel: het primaire gebruik van de gegevens). Deze taak zal steeds een wettelijke basis hebben, bijvoorbeeld in de Gemeentewet of een andere sectorale wet.

De wettelijke regeling op basis waarvan gegevens aanvankelijk zijn verkregen, is in sterke mate bepalend voor de vraag of gegevens (ook) kunnen worden gebruikt voor de bestrijding van ondermijning. Zo kan die wettelijke regeling een geheimhoudingsbepaling bevatten die het (verdere) gebruik van gegevens beperkt of anderszins regelen of en zo ja, in hoeverre de gegevens voor bepaalde doeleinden of taken mogen worden gebruikt.

B. Is bestrijding van ondermijning verenigbaar met het oorspronkelijk doel waarvoor de gegevens zijn verzameld?

In aanvulling daarop geldt dat het gebruik van gegevens ter bestrijding van ondermijning een toelaatbare verdere verwerking moet zijn. Van een toelaatbare verdere verwerking is sprake als het gebruik van de gegevens verenigbaar is met het doel waarvoor de gegevens aanvankelijk zijn verkregen. Daarbij moeten de volgende vragen worden beantwoord:

1. Wat is het doel van de wet en/of de wettelijke bepaling op basis waarvan de gegevens aanvankelijk zijn verkregen?
2. Is het bestrijden van ondermijning verenigbaar met dat primaire doel?
3. Wat is het kader waarin de persoonsgegevens zijn verzameld?
4. Wat is de aard van de verwerkte persoonsgegevens?
5. Wat zijn de mogelijke gevolgen voor de betrokkene?
6. Worden er passende waarborgen getroffen?

Van verenigbaarheid in de zin van de vragen 1 en 2 zal sneller sprake zijn als de wettelijke basis voor het primaire gebruik gerelateerd is aan het bestrijden van ondermijning, bijvoorbeeld een openbare orde bevoegdheid van de burgemeester. Dat wordt lastiger als de wettelijke basis betrekking heeft op een geheel ander domein, zoals het sociaal domein.

“Het bestrijden van ondermijning” als doel voor een verdere verwerking is breed. In het concrete geval wordt dit doel daarom gepreciseerd door het te vertalen naar de gemeentelijke wettelijke bevoegdheden die de gemeente ten behoeve van de aanpak van het signaal zou willen inzetten.

Het zal hierbij veelal gaan om wettelijke taken en gemeentelijke bevoegdheden die zien op openbare orde bevoegdheden en bevordering van de leefbaarheid. Van belang hierbij is dat aan het voorzienbaarheids criterium wordt voldaan: een betrokkene moet kunnen voorzien dat de bedoelde gegevensverstrekking zou kunnen plaatsvinden.

Indien de privacy officer concludeert dat sprake is van onverenigbaarheid, kan het gebruik van de gegevens ter bestrijding van ondermijning toch toelaatbaar zijn als er een expliciete wettelijke grondslag voor dat gebruik is (zie onder het kopje: *Wat is de wettelijke basis voor het primaire gebruik?*).

Bijlage 2 (van het model privacy protocol) bevat voorbeelden van bovenstaande analyse met betrekking tot wetten op basis waarvan gegevens kunnen worden verkregen die vaak relevant zullen zijn voor het tegengaan van ondermijning door gemeenten (als gezegd zal het hierbij veelal gaan om wettelijke taken en bevoegdheden die zien op openbare orde bevoegdheden en bevordering van de leefbaarheid).

Voor de verwerking van bijzondere en strafrechtelijke persoonsgegevens geldt een bijzonder regime: die gegevens mogen in beginsel alléén worden verwerkt als uit de wet op basis waarvan die gegevens zijn verkregen blijkt dat dat – voor de in die wet genoemde doelen – mag. Voor strafrechtelijke gegevens geldt nog een andere relevante uitzonderingsgrond: een gemeente zal die gegevens mogen verwerken als zij krachtens de Wet politiegegevens of Wet justitiële en strafvorderlijke gegevens zijn verkregen (zie voor een uitwerking van verstrekking op grond van de Wet politiegegevens bijlage 2 (van het model privacy protocol)).

C. Is het gebruik van de gegevens noodzakelijk en proportioneel en wordt aan het subsidiariteitsvereiste voldaan?

Gegevens mogen alleen worden gebruikt voor de bestrijding van ondermijning als dat gebruik noodzakelijk en proportioneel is en er geen minder ingrijpende middelen voorhanden zijn. Bij de vraag of een verstrekking noodzakelijk en proportioneel is, spelen onder meer de volgende omstandigheden een rol:

- de aard en ernst van een binnengekregen signaal. Bij aanwijzingen dat er ernstige feiten spelen, zal informatie eerder mogen worden gedeeld;
- de ernst van de inbreuk die op de persoonlijke levenssfeer van de betrokkene wordt gemaakt. Daarbij kan onder meer acht worden geslagen op:
 - de voorzienbaarheid van de (cumulerende) inbreuk die op de persoonlijke levenssfeer wordt gemaakt;
 - de vraag in hoeverre een compleet beeld van de betrokkene ontstaat; -in hoeverre een betrokkene negatieve gevolgen zal ondervinden van de gemaakte inbreuk;

- de aard van de gegevens (hoe gevoeliger, hoe terughoudender ermee moet worden omgegaan);
- of een betrokkene zich effectief kan verweren tegen gemaakte inbreuken (bijv. rechtsbescherming).

In het kader van de vraag naar subsidiariteit moet bijvoorbeeld, als is vastgesteld dat sprake is van een verenigbare verdere verwerking of een expliciete wettelijke grondslag voor het gebruik, eerst een 'hit/no hit'-check worden gedaan (met andere woorden: eerst nagaan dat er bepaalde informatie bij de gemeente berust), alvorens de informatie zelf kan worden geraadpleegd (wat is de informatie waarover de gemeente beschikt). In sommige gevallen kan de eerste vorm van informatie volstaan (subsidiariteit).

Aanvullende waarborg: privacy check 2A en 2B

Als aanvullende waarborg is in dit protocol een tweede privacy beoordelingsmoment opgenomen: privacy check 2A en 2B.

Deze wordt door de privacy officer uitgevoerd voorafgaand aan het signaaloverleg (start fase 4). De privacy officer stelt bij iedere casus vast of en zo ja welke verzamelde gegevens daadwerkelijk mogen worden gedeeld met de/het relevante, bij het signaal betrokken, gemeentelijke onderdeel/de relevante gemeentelijke onderdelen ten behoeve van de verdere aanpak. De privacy officer kan daarbij ook beoordelen of eventuele onderliggende gegevens uit een concreet dossier voor de verdere aanpak van de casus binnengemeentelijk mogen worden gedeeld en zo ja, met welk gemeentelijk onderdeel / gemeentelijke onderdelen. Met name de beoordeling van de *noodzaak* om informatie te delen, zal daarbij centraal staan. Het gaat dan niet alleen om de hoeveelheid gegevens, maar ook om de vraag of alle deelnemers de betreffende informatie nodig hebben. Denkbaar is bijvoorbeeld dat een signaal op maar 3 domeinen ziet en de informatie ten aanzien van dat signaal dus ook alleen aan de deelnemers vanuit die domeinen mag worden verstrekt (in plaats van aan alle domeinen die aan tafel zitten).

Zoals aangegeven in paragraaf 3.2 kan ook in fase 4 – bij het bepalen van het plan van aanpak voor een casus – een privacy check nodig zijn, te weten om te bepalen of de verzamelde gegevens daadwerkelijk mogen worden gedeeld met het relevante gemeentelijke onderdeel/de relevante gemeentelijke onderdelen ten behoeve van de verdere aanpak en beoogde inzet van bevoegdheden. Daartoe zullen dezelfde vragen moeten worden gesteld als hierboven omschreven.

4.3 Informatievoorziening burger

De wijze en het moment waarop betrokkene geïnformeerd wordt over een eventueel onderzoek, moet nader bepaald worden in de latere uitwerking van het proces.

Bron Model Privacy Protocol:

“Daarnaast legt de gemeente, bijvoorbeeld in beleid, vast wanneer de betrokken persoon of het betrokken bedrijf wordt geïnformeerd over een onderzoek. Vanuit transparantie-oogpunt is het uitgangspunt dat betrokkenen zo snel en volledig mogelijk worden geïnformeerd over onderzoek dat naar hen wordt gedaan. Dat is evenwel niet altijd mogelijk, omdat het informeren van betrokkenen het onderzoek kan schaden. Dat doet niet af aan de mogelijkheid om meer in algemene zin te informeren over de mogelijkheid dat gegevens verder worden verwerkt ter bestrijding van ondermijning, bijvoorbeeld in het algemene privacybeleid van de gemeente of, beter nog, bij het in eerste instantie verzamelen van de gegevens bij de betrokkene. In beleid over het informeren van betrokkenen kan worden aangesloten bij de informatieplicht van de artikelen 13 en 14 AVG en de uitzonderingen daarop zoals opgenomen in artikel 23 AVG en artikel 41 UAVG. Bij verwerkingen van persoonsgegevens die onder het toepassingsbereik van de AVG vallen, is het vanzelfsprekend verplicht te voldoen aan deze bepalingen inzake de informatieplicht.”

4.4 Verstrekkingen aan (keten)partners

Er vinden in principe geen verstrekkingen plaats aan ketenpartner/partijen buiten de gemeente. Wel kan het voorkomen dat een signaal, na weging, blijkt bij een ketenpartner te moeten worden opgepakt, bijvoorbeeld omdat het niet onder de taak/bevoegdheid van de gemeente valt, of omdat een aanpak samen met andere (RIEC-) partners meer aangewezen blijkt.

5 RECHTEN VAN BETROKKENE

Betrokkenen kunnen op grond van de AVG vragen om inzage in de persoonsgegevens die verwerkt worden door de gemeente Den Haag. Deze verzoeken kunnen centraal binnenkomen bij de gemeente of rechtstreeks gericht zijn aan een van de (proces-)verantwoordelijken.

5.1 Bibob proces

Betrokkenen nemen kennis van het Bibob advies omdat het onderdeel vormt van de beschikking (als motivering daarvan). Eventueel kan afschrift van het advies worden opgevraagd, na ondertekening van geheimhoudingsverklaring. Daarna staat bezwaar en beroep open voor betrokkene conform Awb.

5.2 RIEC Liaison proces

Het RIEC Liaison proces wordt uitgevoerd als onderdeel van de RIEC samenwerking. Betrokkenen zullen zich (naar verwachting) nooit specifiek richten tot de gemeente / de RIEC Liaison met een verzoek om inzage in de persoonsgegevens die over hem/haar verwerkt worden. Wel kan een betrokkene een eerste verzoek om inzage bij de gemeente neerleggen, maar het is aan het hoofd RIEC om de beantwoording van verzoeken te coördineren.

Zie Artikel 15.3 jo. 11.3 Privacyprotocol RIECs-LIECs.

Betrokkenen kunnen bij de convenantpartners (*waaronder dus de gemeente*) een verzoek indienen om met betrekking tot verwerkingsactiviteiten in het kader van de RIEC-samenwerking: inzage te verkrijgen, rectificatie of wissing te verzoeken, of bezwaar te maken tegen die verwerking.

Het proces van beantwoording van verzoeken wordt gecoördineerd door het hoofd RIEC conform een daarvoor vastgestelde procedure.

Op grond hiervan kan de gemeentelijke RIEC Liaison gevraagd worden om hieraan bijdrage te leveren.

Het RIEC Den Haag is voor betrokkenen te benaderen via Postadres: Postbus 16471, 2500 BL, Den Haag T: 5.1.2.e E: 5.1.2.e @denhaag.nl

5.3 Proces binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijning

Nader uit te werken in latere fase / tijdens implementatie van dit proces binnen gemeente Den Haag.

Bron Model Privacy Protocol:

“Verder hebben betrokkenen, in ieder geval als het gaat om de verwerking van persoonsgegevens, het recht te verzoeken om inzage in de persoonsgegevens die ten aanzien van hen worden verwerkt (artikel 15 AVG). Desgewenst kunnen zij verzoeken om rectificatie, wissing of beperking van die verwerking (artikel 16, 17 en 18 AVG). Ook hierbij kunnen de uitzonderingen van artikel 23 AVG en artikel 41 UAVG aan inwilliging van de verzoeken in de weg staan.”

6 BEWAARTERMIJNEN

Algemeen:

Voor de drie in dit handboek beschreven processen geldt dat binnen de uitvoering van het proces hoofdzakelijk gegevens bijeengebracht worden vanuit verschillende gemeentelijke bronnen. De gegevens die in/tijdens het proces worden vastgelegd in het dossier hebben hun 'oorsprong' dus in de meeste gevallen in andere bronsystemen en zijn voor andere (gemeentelijke) doeleinden verzameld. Ieder van die bronsystemen kent een eigen bewaartermijnenbeleid.

Waar hieronder gesproken wordt over bewaartermijnen, gaat het dus om de bewaring van de gegevens in het dossier binnen het infodesk proces / (te implementeren) zaaksysteem (en niet over de gegevens in het originele bronsysteem).

Bibob proces

Voor een bibob dossier is de bewaartermijn (sinds de wijziging van Wet Bibob dd augustus 2020) gesteld op 5 jaar. Daarna dient het dossier verwijderd en eventueel gearhiveerd te worden.

RIEC Liaison proces

Voor het RIEC geldt voor de persoonsgegevens die in het kader van het samenwerkingsverband worden vastgelegd in (o.a.) RIEC-IS, een bewaartermijn van 5 jaar. Zie voor de toelichting hierop Art 17 van Privacyprotocol RIECs-LIEC.

Voor de gegevens die in het kader van het RIEC Liaison proces verzameld worden, dient de maximale bewaartermijn nog vastgesteld te worden.

Gegevens worden opgeslagen in RIEC -IS en zijn opnieuw te herleiden uit de verschillende bronbestanden.

Daardoor bestaat feitelijk geen noodzaak om de gegevens, na registratie in RIEC-IS, voor langere tijd te bewaren. En zouden de gegevens bijvoorbeeld kort na het afsluiten van de casus verwijderd kunnen worden uit het Zaaksysteem (en huidig: verwijderd worden uit in- en uitgaande emailboxen en persoonlijke / gedeelde opslaglocaties). Echter is het met de huidige inrichting van het RIEC IS zo dat: 1) toegang tot casusinformatie op medewerker-persoonsniveau wordt toegekend (het geen vervanging door een directe collega in dezelfde functie in de weg staat) en 2) er geen zoekfunctie wordt ondersteund in RIEC IS. Om die 2 redenen is het toch van belang om de gemeentelijke voorbereiding op en input voor het RIEC proces (en de daarmee gepaard gaande

dossier registratie intern de gemeente) voor een langere periode te bewaren. Echter nooit langer dan de maximale bewaartermijn die binnen RIEC IS is toegestaan.

Bewaartermijn implementatie moet meegenomen worden bij de implementatie van het zaakstelsel.

Proces binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijning

Voor het binnengemeentelijk proces aanpak ondermijning zijn de bewaartermijnen niet vastgesteld in wetgeving. Het is aan de gemeente om hier zelf redelijke termijnen voor te bepalen. Dit moet in het implementatietraject voor dit proces nog worden geconcretiseerd.

Enige "guidance" hiervoor kan gevonden worden in het Modelprotocol binnengemeentelijke gegevensuitwisseling. Daarin wordt gesteld dat signalen die niet verder in behandeling worden genomen, bijvoorbeeld nog een jaar versleuteld bewaard worden. Voor een casus die wel tot een aanpak heeft geleid, wordt voorgesteld de gegevens – na afsluiting van de casus en de daarop volgende monitoring fase - nog gedurende een jaar te bewaren.

A Bijlage 1: Checklist ten behoeve van de signaalanalyse

Bron: Model Privacy Protocol, pagina 20-30

Zie: <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/02/20/tk-bijlage-model-privacy-protocol-binnengemeentelijke-gegevensdeling/tk-bijlage-model-privacy-protocol-binnengemeentelijke-gegevensdeling.pdf>

Aan de hand van onderstaande checklist wordt stapsgewijs beoordeeld of het signaal betrekking heeft op ondermijning. De checklist is afhankelijk van maatschappelijke ontwikkelingen en kan reeds daarom niet als limitatief worden beschouwd. Vanzelfsprekend kan de checklist worden aangepast al naar gelang de eigen gemeentelijke praktijk en ervaringen.

De ontvangst van een signaal door de regisseur ondermijning vormt het startpunt voor het protocol. Er wordt tot uitgangspunt genomen dat het delen van signalen met de regisseur ondermijning op rechtmatige wijze geschiedt. Vanzelfsprekend zal een verstrekker van een signaal wel steeds moeten vaststellen of die verstrekking in lijn is met de privacyregelgeving.

Stap 1:

Het signaal heeft betrekking op een dan wel meer van de volgende categorieën personen.

Openbare inrichtingen

- a. pandeigenaar
- b. verhuurder
- c. huurder/pachter
- d. exploitant
- e. beheerder/Leidinggevende
- f. tussenpersoon
- g. geldschietters

Georganiseerde hennepcultuur/drugs(-handel)

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder

- d. Tussenpersoon (verhuurmakelaar, evt. andere vormen?)

Mensenhandel, -smokkel en uitbuiting (o.a. illegale prostitutie)

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. eigenaar (illegale) seksinrichting
- e. eigenaar (illegale) massagesalon
- f. exploitant van een vergunde seksinrichting
- g. beheerder van een vergunde seksinrichting
- h. illegaal werkende prostituee (dwz zonder vergunning)

Fraude in de vastgoedsector

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Tussenpersoon (verhuurmakelaar, andere vormen?)
- e. stichting, vereniging of andere ondernemingsvorm (of bestuurders hiervan)

Misbruik in de vastgoedsector

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Tussenpersoon (verhuurmakelaar, andere vormen?)
- e. stichtingvereniging of andere ondernemingsvorm (of bestuurders hiervan)

Fraude en/of witwassen en daaraan gerelateerde vormen of andere vormen van financieel-economische criminaliteit

(o.a. ook illegaal gokken/heling/underground banking)

- a. ontvanger/begunstigde uitkering vanuit de gemeente
- b. ontvanger/begunstigde subsidie vanuit de gemeente
- c. andersoortige begunstigende beschikking vanuit de gemeente
- d. een tussenpersoon/gemachtigde met betrekking tot zorg
- e. pandeigenaar

Overig

- a. overige faciliteerders die ondermijnende of criminele activiteiten mogelijk maken en/of (on)bewust in stand houden;

- b. en/of personen die een rol spelen bij een regionaal thema of een handavingsknelpunt zoals:
- Outlaw Motorcycle Gangs (OMG's): leden van OMG's;
 - Woonwagencentra: eigenaren woonwagens, huurders, bewoners;
 - Windhappers (personen met veel geld en geen inkomen dan wel personen van wie de levensstijl niet past bij het bekende inkomen);
 - Harddrugs.

Stap 2:

Het signaal kan een van onderstaande kenmerken omvatten:

Kader/begripsbepaling 'ondermijnende criminaliteit'
Aantasting van instituten die zich richten op legale perspectieven en de werking van het samenlevingssysteem borgen en sturen
Aantasting van de gezagspositie van bestuur, politie en/of andere overheidsorganen
Aantasting of latente c.q. mogelijke aantasting van de openbare orde en veiligheid
Ontwrichting of latente c.q. mogelijke ontwrichting van de maatschappelijke, politieke en/of economische structuren
Onrechtmatigheden, maatschappelijke bedreigingen en/of georganiseerde criminaliteit

In aanvulling is tenminste sprake van één van onderstaan- de locatie-, persoons- en/of bedrijfsgebonden indicatoren binnen het grondgebied van gemeente.

Indicator 'situatieve en lokale verankering'
Gelegenheidsstructuren (of criminaliteit bevorderende condities) in de bestuurlijke omgeving (wet en regelgeving; toezicht en handhaving)
Gelegenheidsstructuren (of criminaliteit bevorderende condities) in de (sociaal-) maatschappelijke omgeving (fysieke omgevingskenmerken, maatschappelijke ontwikkelingen, sociale relaties of netwerken, informele controle)
Gelegenheidsstructuren (of criminaliteit bevorderende condities) in de zakelijke / economische omgeving (beroepen, branches, marktpartijen).
Processen, procedures, instructies en/of structuren binnen (een) (publieke) organisatie(s) die het mogelijk maakt (on-)bewust te faciliteren
Bij de gelegenheidsstructuren is een locatie (zoals een pand of bedrijf/onderneming), een persoon, een groep, een familie en/of netwerk (meerdere personen die samenwerken) betrokken

Stap 3

En kan tenminste sprake zijn van één van onderstaande indicatoren, hetgeen nader uitgewerkt is in de bijbehorende lijst met 'red flags'.

Indicator 'signalering'
Incongruenties (omstandigheden en gedragingen); feit dat indicaties niet goed bij elkaar passen, niet goed overeenstemmen in aard, omvang en intensiteit
Malafide en/of criminele activiteiten, hinder en/of overlast
Veelal systematisch en structureel gepleegd
Latent aanwezig
Complex

Lijst met 'red flags'

Algemeen
• Salaris uitbetalen per week en/of per kas. • Financiële man/financieel 'directeur' kan factuur niet plaatsen en moet navraag doen/flat vragen bij de baas. • Sterke waardeestijging van moeilijk waardeerbare aandelen. • Grootaandeelhouder heeft geen weet van wat überhaupt in de onderneming gaande is. • De officiële eigendomsverhoudingen in rechtspersoon zijn niet in verhouding met de daadwerkelijke gezagsverhoudingen. • Huurders/gebruikers/kopers die ook op een andere wijze een functie bij koper of verkoper van een onroerende zaak vervullen • Onmogelijkheid om gezien inkomen en/of vermogen onroerende zaken te kopen en/of financiering te krijgen. • Waarde van afzonderlijke appartementsrechten na splitsing (in het bijzonder indien een deel in de privé- en een deel de zakelijke sfeer terecht komen. • Leningen met aflossingen/geldstromen vanuit het buitenland. • Plotselinge stijgingen in vermogensopstellingen box 3 inkomstenbelasting. • Niet gebruikelijke juridische vastgoedconstructies, mede in combinatie met verzoek om vrijstelling ex art. 15 lid 1 letter h WBR. • Vastgoedondernemingen die volgens het handelsregister geen werkzame personen hebben. • Aangifte door huurder van bedreiging/ intimidatie omdat hij het idee heeft dat de verhuurder hem uit de woning wil hebben. (Een dergelijke aangifte kan duiden op een criminele verhuurder.) • Meerdere provisies naar verschillende personen. Personen die voor elkaar betalen. • Onlogische geldstromen en/of facturen. • Vaste 'functionele' relatie tussen bankmedewerker en specifieke personen van overige zakelijke dienstverleners. • Onvoldoende waarborgen binnen de financiële onderneming voor de bescherming van de integriteit van medewerkers door functiescheiding.

- Exclusieve relatie tussen medewerker van hypotheekbank, notaris en belastingadviseur.
- Geconstateerd is dat grote bedragen niet opvallen en vertrouwen wekken. Juist bij grote bedragen dient de financiële onderneming echter alert te zijn omdat daarin schijn en wezen kunnen verschillen
- Het gebruik van waardeverklaringen in plaats van officiële taxatierapporten.
- Afwijkend tarief voor (ogenschijnlijke) standaardopdracht.
- Waardebepaling van panden met krakers en panden met mogelijke bestemmingswijziging.
- Het gebruik van oude beschikbare bronnen (bijvoorbeeld oud kadastraal uittreksel of bewijs van eigendom).
- Meerdere sterk wisselende taxaties voor eenzelfde vastgoed in een relatief korte periode.
- Exclusieve relatie (volume- en/of prijsafspraken) tussen de makelaar/taxateur en de intermediair/financiële onderneming voor taxaties ten behoeve van de financiering.
- Eigen belang bij de uitkomst van de taxatie of de hoogte van het taxatiebedrag.
- Retourprovisie of commerciële afspraken met intermediairs en financiële onderneming.
- Ontbreken van vaste onderdelen in het onderzoek ten behoeve van de waardebepaling door de makelaar/taxateur (informatie over vergelijkbare panden, WOZ-waarden, gebruik van het puntensysteem voor het vaststellen van de waarde of de hoogte van de huren, sloop-/handhaven- afweging).
- Ontbreken standaarddossieropbouw met onderliggende documentatie en uitzonderingsrapportages
- Onvoldoende waarborgen bij de makelaar/taxateur voor de bescherming van de integriteit van medewerkers door functiescheiding (afhankelijk van omvang kantoor; bijvoorbeeld scheiding tussen de intake en de uitvoering van opdrachten en review van uit te brengen taxatierapporten en waardeverklaringen).
- Exclusieve relatie tussen notaris, belastingadviseur en medewerker van hypotheekbank.
- Aparte belastingadviseur voor offshore structuur.
- Hoge vergoeding voor belastingadviseur (vast maandbedrag en uurtarief).
- De koper verricht betalingen aan de (fiscaal) adviseur van de verkoper.
- Exclusieve relatie tussen belastingadviseur, notaris en medewerker van hypotheekbank.
- Bedrijfskosten van de onderneming zijn zeer laag.
- Een combinatie van een beperkt inkomen en een grote investering in vastgoed.
- Personen die bij volmacht handelen (dit kan wijzen op het buiten beeld houden van de 'ultimate beneficial owner').
- Doorverwijzen van Nederlandse klanten door trustkantoren naar buitenlandse banken, waar men coderekeningen kan aanhouden.
- Trustkantoor geeft opdracht terug en/of beeindigt de relatie.

- Aanpassen jaarstukken door accountant t.b.v. het verkrijgen van hypothecaire lening.
- Investeerder is een wereldburger die nergens of ieder geval niet in Nederland belastingplichtig is.
- Een combinatie van een beperkt inkomen en een grote investering in vastgoed.
- Grote afhankelijkheid overige zakelijke dienstverlener van één klant.
- Iemand met een minderheidsbelang heeft feitelijke leiding over de onderneming, terwijl de overige partijen met een belang opvallend passief zijn en blijven.
- Makelaar/verhuurmakelaar/tussenpersoon die bij meerdere panden betrokken is geweest waar overtredingen zijn geconstateerd.

Loverboys: minderjarigen (< 18 jaar)

- Spijbelen
- Haalt ('ineens') slechte cijfers
- Lijkt ineens veel geld te hebben (dure kleding, telefoon etc.)
- Keert zich af van ouders/vrienden
- Grensoverschrijdend gedrag
- Komt alleen nog thuis om te slapen
- Heeft onverklaarbare schulden
- Loopt regelmatig weg, is veel weekenden en nachten weg

Financiering

T.a.v. partijen

- Gebruik vennootschappen in een land waar niet wordt geregistreerd wie de aandeelhouder is.
- Combinatie van een offshore vennootschap en een geldstroom die uit een land met een bankgeheim komt.
- Complexe vennootschappelijke constructies.

T.a.v. kredietdossiers

- Onvoldoende CDD.
- Onvolledig kredietdossier en (te) oude stukken (bijvoorbeeld niet aantreffen van originele door de makelaar/taxateur gewaarmerkte taxatierapporten).

- Financiële onderneming gaat akkoord met passeren akte, terwijl het dossier nog incompleet is.
- Kredietdossier is in één keer compleet/ spoed.
- Kredietbeoordelaar controleert niet de door kredietaanvrager opgegeven vermogensbestanddelen, inkomen en/of winst.
- Bij financiering wordt verkoopwaarde van een pand meegenomen, terwijl persoon pand niet op naam heeft staan.
- ABC-constructie (specifiek igv financiële problemengeld- lener: risico dat A voor te lage waarde uit boedel wordt getild, B-C transactie wel tegen normale waarde)
- Hypotheken worden verstrekt aan personen met (financiële) antecedenten (bijvoorbeeld persoon staat opgenomen in BKR als wanbetaler van geldleningen).
- Meerdere malen BKR getoetst in korte tijd.
- BKR-registratie recent beëindigd (check BKR historie)
- Op de loonstrook die wordt overgelegd aan de hypotheekverstrekker staat aangegeven dat het salaris per kas wordt uitbetaald.
- Vormfouten in aangeleverde documenten, zoals loonstrook, werkgeversverklaringen, taxatierapporten en depotnota's.
- Recente datum indiensttreding.
- Afwijkende adressen op verschillende documenten.
- Aanvragers hebben meerdere onderpanden.
- Gefingeerd samenwonen (personen 'bij elkaar geplakt').
- Taxatierapporten zijn niet in fysieke originele vorm opgenomen in het kredietdossier.
- Het aantreffen van meerdere – kort na elkaar – vervaardigde / gedateerde taxatierapporten (kan wijzen op een situationeel gebruik hiervan).
- Aanvraag financiering voor verbouwing terwijl verbouwing al (nagenoeg) gereed is.
- Makelaar/taxateur/notaris/bouwkundig deskundige betrokken bij transactie die niet afkomstig is uit 'de streek'.

T.a.v. de taxatie

- Huren die gezien de locatie / pand opvallend hoog zijn (hiermee kan een te hoge taxatie worden bewerkstelligd en kan worden witgewassen).
- Aanwezigheid van risicovolle ondernemingen en/of bedrijfsomschrijvingen volgens gegevens van de KvK op het adres van het te financieren vastgoed.
- Taxaties voor financieringsaanvraag die de waarde na verbouwing vermelden, zonder dat de financiële onderneming een goede controle laat plaatsvinden op de relatie waardevermeerdering vs. verbouwing en op de nota's.
- Exclusieve relatie tussen de financiële onderneming en de makelaar/taxateur die taxaties verricht ten behoeve van de financiering.
- Opdrachtgever taxatie is (onbekende) derde.

- Het als financiële onderneming slechts gebruik maken van één vaste makelaar/taxateur voor taxaties, zonder dat er een controle plaatsvindt indien de gevraagde kredietfaciliteit onder een bepaald bedrag blijft.

T.a.v. verstrekking hypotheek en bouwdepot

- De bewuste bankmedewerker (accountmanager) is de medewerker met hoogste provisie.
- Het verstrekte bedrag van de hypotheek staat niet in verhouding tot de (legale) inkomsten (salaris, huur of uit onderneming)/ verhouding leeftijd vs. inkomen vs. Beroep
- Meerdere hypotheeken gevestigd op één pand in combinatie met herhaaldelijk oversluiten.
- Hypotheken worden in korte tijd meerdere keren substantieel verhoogd.
- Onttrekkingen aan bouwdepots zonder facturen.

Financiering

- (Ver)bouw nota's worden onwaarschijnlijk snel achter elkaar ter uitbetaling ingezonden.
- Offertes ingediend als factuur.
- Werkzaamheden op factuur zijn niet gespecificeerd (indicator valse factuur)/ hoogte van het uit te betalen bedrag staat in geen verhouding tot de uitgevoerde werkzaamheden/geleverde goederen.
- Op factuur wordt niet verwezen naar de termijn van de aannemingsovereenkomst (indicator valse factuur).
- Het onttrekken van gelden inclusief omzetbelasting aan bouwdepots van zakelijke entiteiten.
- Nationale Hypotheek Garantie (NHG) meerdere keren verstrekt tbv dezelfde partij.
- Adres volgens Basisregistratie Personen (BRP) wijkt af van adres volgens NHG.

T.a.v. transport hypotheekakte

- Discrepancie aan begin of eind van transactie tussen degene die het geld forneert en degene die eigenaar wordt.
- Op het moment van transport wordt de hypotheek doorgehaald. Het lijkt alsof (een deel van) de verkoopopbrengst voor verrekening wordt gebruikt. Dit is echter niet het geval. Op de afrekening van de notaris staat ("aflossing hoofdsom X: nihil").

- Waarborg wordt niet ingeroepen dan wel niet opgeëist (wijst op gelieerde partijen).

T.a.v. gebruik rekeningen

- Omschrijving 'one of our clients' op bankafschriften.
- Contante stortingen middels sealbags op rekeningen waarvoor geen dergelijke overeenkomst is afgesloten met de bank.
- Sealbagstortingen op derdengeldenrekeningen (of andere rekeningen) van advocatenkantoren of notariskantoren (verschoningsgerechtigden).
- Kosten voor contante geldtransporten in opdracht van de bank die worden doorbelast aan de client.
- Grote aflossing hypotheek zonder dat dat onderbouwd kan worden door verkoop vorige woning of andere bronnen.
- Ontvangen aflossingen vanaf derdengeldenrekeningen van advocaten, terwijl geen sprake is van een boedel- scheiding of een faillissement.
- Taxaties voor financieringsaanvraag die de waarde na verbouwing vermelden.

T.a.v. financierende partijen

- Financierende partij is een buitenlandse niet-financiële instelling.
- Financierende partij is een (constructie met) offshore vennootschap(pen) en/of komt uit land met een bankgeheim en/of kort na het ontstaan van een dergelijke constructie wordt vastgoed aangeschaft.
- Financierende partij is een vennootschap waarvan de aandelen aan toonder zijn
- Financiering door verkoper.
- De waarborgsom wordt bijeengebracht door anderen dan de juridische eigenaar of diens hypotheeknemer.
- Financierende partij is een niet-zakelijke partij.
- Financierende partij is onbekend.
- Financierende partij is een vennootschap waarvan de aandelen aan toonder zijn.

T.a.v. financiering zelf

- Hypotheek is niet beschikbaar op datum van levering.
- Financiering, waarbij geen hypotheek wordt gesteld.
- Grote aankoop vindt plaats zonder financiering.
- Koper blijft bedrag schuldig aan verkoper.
- Financiering door verkoper, waarbij ten gunste van verkoper een hypotheek wordt gevestigd.
- Financiering vindt plaats door verkoper tegen een hoge rente.

- Niet betaalde interest, waar geen (juridisch) gevolg aan wordt gegeven (Dit kan duiden op een feitelijke macht en/of eigendomsverhouding die niet strookt met de geregistreerde juridische overeenkomsten).
- Herfinanciering gaat niet naar de verkoper, de verkoper wordt uit andere bron betaald.
- Financiering, waarbij geen hypotheek wordt gesteld.

T.a.v. geldstroom

- Geldstroom komt van een niet-financiële instelling in het buitenland.
- Geldstroom komt vanuit (constructie met) offshore structuur en/of komt uit een land met een bankgeheim.
- Geldstroom komt van een vennootschap waarvan de aandelen aan toonder zijn.
- Geldstroom is afkomstig van buitenlandse coderekening.
- Uitbetaling aan derde partij die niet betrokken is bij de akte.
- Aflossing niet aan degene die oorspronkelijk heeft gefinancierd.

Financiering
T.a.v. ongebruikelijke geldstroom

- Geldstroom komt van een niet zakelijke partij.
- Geldstroom komt van een vennootschap waarvan de aandelen aan toonder zijn.
- Geldstroom afkomstig van de derdengeldenrekeningen van verschoningsgerechtigden in Nederland.
- Betalingen provisies, commissies, advieskosten.

Koop/verkoop
T.a.v. partijen

- De koper heeft geen kennis van het te kopen object / de te kopen objecten.
- Kopende partij 'houdt' voor een ander.
- Levering aan verschillende rechtspersonen die door dezelfde persoon worden vertegenwoordigd.
- Gebrek aan transparantie m.b.t. uiteindelijke koper ('nader te noemen meester').

- Transacties tussen gelieerde partijen(privé/B.V., familieleden)
- De personen in de koopovereenkomst komen niet allen terug in de akte van levering.
- Koper in koopakte en in uiteindelijke leveringsakte verschillen, er is een partij bijgekomen (mutaties in partijen gedurende traject).
- Huurder koopt een woning van een verhuurder die een buitenlandse rechtspersoon is.
- Betrokkenheid bij transport van een persoon die niet aanwijsbaar bij de transactie is betrokken.

T.a.v. transport vastgoed

- ABC-transactie met opvallende waardeinstijgingen.
- Groot aantal transporten bij de notaris in een zeer kort tijdsbestek.
- Naadloze aansluiting tussen taxatiewaarde en koopsom.

T.a.v. financiële afwikkeling

- Bij verkoop stort de notaris het aankoopbedrag op een door de verkoper opgegeven rekening, niet zijnde zijn eigen rekening of die van de kredietverstrekker (hypotheeknemer).
- Notaris stort aanbetaling van cliënt terug op andere rekening(en).
- Bij het niet doorgaan van de transactie omdat de koper niet afneemt, betaalt de verkoper een afkoopsom aan de partij die zou kopen.

Algemeen

- Een combinatie van een beperkt inkomen en een grote investering in vastgoed.
- Verhouding koopsom t.o.v. huur is heel hoog.
- Verlies op vastgoedtransactie na recente verkrijging.
- Overdracht economisch eigendom.
- Constructie die bestaat uit een combinatie van nieuwe rechtspersonen in het buitenland en overgenomen vennootschappen in Nederland die handelt en beheert.
- Bij ABC-transactie: Verkoop B-C vindt plaats vóór A-B transactie (wijst op orkestreren, gelieerde partijen).
- In het jaar voorafgaand aan de koop/verkoop door de institutionele belegger heeft een ABC-transactie plaats- gevonden waarbij sprake is van onverklaarbare waar- de-stijgingen en/of dubieuze partijen.
- In het jaar na de koop/verkoop door de institutionele belegger heeft een ABC-transactie plaatsgevonden waarbij sprake is van onverklaarbare waardeinstijgingen en/of dubieuze partijen.

- 'Handelingsvrijheid' vermogensbeheerder.
- In het jaar voorafgaand aan de koop/verkoop door het pensioenfonds heeft een ABC-transactie plaatsgevonden waarbij sprake is van onverklaarbare waardeinstijgingen en/of dubieuze partijen.
- In het jaar na de koop/verkoop door het pensioenfonds heeft een ABC- transactie plaatsgevonden waarbij sprake is van onverklaarbare waardeinstijgingen en/of dubieuze partijen.
- Commissiebetalingen/winstdelingen/aanbrengprovisies.
- Provisiebetalingen zonder zichtbare tegenprestatie.
- De verkoper factureert ten tijde van de verkoop aan koper voor advieskosten.
- Bevoordeling sociaal netwerk (familielid/relatie). Betrokken partijen melden een verschillende koopsom. (Sommige partijen hebben het over de officiële koopsom, andere partijen bedoelen vermoedelijk de totale koopsom inclusief betalingen buiten de akte om.)

Koop/verkoop

- Transactie wordt met terugwerkende kracht ongedaan gemaakt.
- Grote afwaardering in het jaar van aankoop ten laste van de (fiscale) winst.
- Zeer snel groeiende vastgoedportefeuille.
- Onverklaarbare waardesprongen (in verhouding tot verstreken tijdspanne).
- 'Handelingsvrijheid' vermogensbeheerder.
- De naadloze aansluiting van de taxatiewaarde bij de koopsom op het moment van verkoop.

Gebruik/exploitatie van een pand

Algemeen

- Wijziging van vastgoed of andere adviseur kan duiden op wijziging van de ubo.
- De als stroman naar voren geschoven koper, bestuurder en/of aandeelhouder heeft geen daadwerkelijke bemoeienis met exploitatie, maar komen alleen met een volmacht naar voren bij de notaris. beheerder
- Voorts heeft bijv. een belasting- adviseur of advocaat een relatief grote rol.
- Criminelen zijn direct (loondienst) of indirect (verrichten van diensten, inzet sociaal netwerk) betrokken bij exploitatie in risicovolle sectoren.

- Commissies voor het aanbrengen van werkzaamheden aan een partij buiten de directe keten.
- Huurder wordt geïnformeerd over het vestigen van een hypotheek op het gehuurde.
- Niet betaalde huren, waar geen (juridisch) gevolg aan wordt gegeven. (Dit kan duiden op een feitelijke macht en/of eigendomsverhouding die niet strookt met de geregistreerde juridische overeenkomsten.)
- Verzekeringsclaims voor brand- en/of opstalverzekeringen, net voordat een grote verbouwing gaat plaatsvinden.
- Contante huurontvangsten (op rekening van persoon die het betreffende pand niet in bezit heeft).
- Grote contante opnamen.
- Betalingen protectiegelden.
- Een vreemde verhouding tussen ontvangen huren en getaxeerde waarde.
- Huren die gezien de locatie / pand opvallend hoog zijn (hiermee kan een te hoge taxatie worden bewerkstelligd en kan worden witgewassen).
- De als stroman naar voren geschoven koper, bestuurder en/ of aandeelhouder heeft geen daadwerkelijke bemoeienis met exploitatie, maar komen alleen met een volmacht naar voren bij de notaris. Voorts heeft bijv. een belastingadviseur of advocaat een relatief grote rol.
- Criminelen zijn direct (loondienst) of indirect (verrichten van diensten, inzet sociaal netwerk) betrokken bij exploitatie in risicovolle sectoren.
- Commissies voor het aanbrengen van werkzaamheden aan een partij buiten de directe keten.
- Huurder wordt geïnformeerd over het vestigen van een hypotheek op het gehuurde.

T.a.v. gebruik pand voor mensenhandel

- Er is geen arbeidsovereenkomst, de arbeidsvoorwaarden zijn slecht gedefinieerd of de arbeidsovereenkomst is opgesteld in een taal die de betreffende persoon niet machtig is.
- Lijkt bang te zijn voor de man/vrouw die hem/haar begeleidt
- De personen beschikken niet zelf over eigen identiteitspapieren
- Slechte huisvesting
- Er is sprake van hoge huren
- Huur wordt inhoudend op salaris
- Ontbreken van huurcontracten
- Vertoont tekenen van angst of lijkt zich ongemakkelijk te voelen, vooral in de aanwezigheid van de supervisor,
- Tijdens gesprek vertelt hij/zij tegenstrijdigheden
- De persoon/personen lijken niet goed te weten waar men is/verblijft

- Iemand anders voert steeds het woord, er lijkt sprake te zijn van controle/gezagsverhouding
- De betalingen vinden onregelmatig en/of vaak te laat plaats.
- Weet niet hoeveel hij/zij verdient.
- Niet vrijelijk kunnen beschikken over (een deel) van de eigen verdiensten, geen eigen bankrekening/ bankpas in bezit)
- Inhouden boetes, (onduidelijke) kosten werkgever en/of borg
- Verplicht om transport, levensmiddelen en/of andere diensten bij één aanbieder (werkgever) af te nemen
- Illegaal verblijf.
- Moet een buitensporige vergoeding terugbetalen voor werving, vervoer, huisvesting, eten, gereedschap of veiligheidsuitrusting en die vergoeding wordt rechtstreeks ingehouden op zijn/haar loon.
- De terugbetalingsregeling voor voorschotten op het loon is onduidelijk of gemanipuleerd.

Gebruik/exploitatie van een pand

- Personen verklaren lange werkdagen te moeten maken
- Bevindt zich in een situatie waarin hij/zij op meerdere manieren van anderen afhankelijk is (hij/zij is bijvoorbeeld afhankelijk van de werkgever voor onderdak, eten, banen voor familieleden of voor andere behoeften).
- Men beschikt niet over eigen inkomsten
- Schaars gekleed en weinig bezit
- Er zijn diverse telefoons en/of laptops in de woning
- Wonen en slapen op de werkplek
- Er lijkt een vorm van toezicht te zijn (een persoon in de woning aanwezig, of de telefoon gaat zeer regelmatig over tijdens pandcontrole)
- Vertoont tekenen van angst of lijkt zich ongemakkelijk te voelen, vooral in de aanwezigheid van de supervisor,
- Weet niet wat zijn/haar verblijfplaats of adres is.
- Heeft regelmatig klanten, maar geen geld om bijv. huur te betalen
- Wordt bij ziekte of zwangerschap gedwongen te werken
- Huren de woning niet zelf
- Alle vragen worden door de begeleidende persoon beantwoordt in plaats van door het potentiële slachtoffer.
- De opmerkingen van het potentiële slachtoffer vertonen geen samenhang of komen ingestudeerd over, door middel van indoctrinatie.

B Bijlage 2: analyses van de ruimte voor binnengemeentelijke gegevensuitwisseling in relevante wet- en regelgeving

Bron: Model Privacy Protocol, pagina 32 ev

Zie: <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2020/02/20/tk-bijlage-model-privacy-protocol-binnengemeentelijke-gegevensdeling/tk-bijlage-model-privacy-protocol-binnengemeentelijke-gegevensdeling.pdf>



analyses van ruimte
voor

C Bijlage 3: Relevante links (extern)

Bibob

<https://www.justis.nl/producten/bibob/>

<https://www.justis.nl/producten/bibob/wet-bibob/index.aspx>

<https://www.justis.nl/producten/bibob/documenten/index.aspx>

RIEC

<https://www.riec.nl>

<https://www.riec.nl/maatregelen-en-documenten/convenant>

<https://www.riec.nl/documenten/richtlijnen/2020/04/17/privacyprotocol-april-2020>

<https://www.riec.nl/maatregelen-en-documenten/documenten/publicaties/2019/08/15/procesbeschrijving-integrale-casusaanpak>

Binnengemeentelijke uitwisseling

<https://www.rijksoverheid.nl/documenten/rapporten/2020/02/20/tk-bijlage-model-privacy-protocol-binnengemeentelijke-gegevensdeling>

D Bijlage 4: Relevante links (intern)

Gemeentelijk proces datalekken

<https://denhaag.sharepoint.com/sites/werknet/portalen/ictdiv/Paginas/Gegevensbescherming-en-incidenten.aspx>

Privacy en security organisatie gemeente Den Haag

<https://denhaag.sharepoint.com/sites/werknet/gegevensbescherming>

(Hier staan alle contactpersonen in het privacy en informatieveiligheid werkveld)

Haags Veiligheidsbeleid

<https://www.denhaag.nl/nl/in-de-stad/veiligheid/haags-veiligheidsbeleid.htm>

Bibob

<https://www.denhaag.nl/nl/in-de-stad/ondernemen/gemeentelijk-bureau-bibob.htm>

<https://www.denhaag.nl/nl/in-de-stad/ondernemen/wet-bibob.htm>

Model privacy protocol

Handleiding binnengemeentelijke gegevensuitwisseling
ten behoeve van de bestrijding van ondermijning

Inhoudsopgave

1	LEESWIJZER	4
1.1	<i>Algemeen</i>	4
1.2	<i>Evaluatie</i>	5
2	(DE AANPAK VAN) ONDERMIJNING	6
2.1	<i>Problematiek en noodzaak van de aanpak van ondermijning</i>	6
2.2	<i>Doel (bestuurlijke en geïntegreerde) aanpak "ondermijning"</i>	7
2.3	<i>Doel van dit protocol</i>	8
3	HET PROTOCOL: EEN OVERZICHT	9
3.1	<i>Schematische weergave</i>	9
3.2	<i>Toelichting op de 4 fases van het protocol</i>	10
3.3	<i>Waarborgen in de verschillende fases</i>	15
4	UITWERKING VAN DE TWEE PRIVACY CHECKS IN FASE 3 EN 4	17
	BIJLAGE 1: CHECKLIST TEN BEHOEVE VAN DE SIGNAALANALYSE (NIET LIMITATIEF)	21
	BIJLAGE 2: ANALYSES VAN DE RUIMTE VOOR BINNENGEMEENTELIJKE GEGEVENSUITWISSELING IN RELEVANTE WET- EN REGELGEVING	32
	<i>A. APV/Openbare orde-bevoegdheden</i>	32
	<i>B. Wet politiegegevens</i>	35
	<i>C. Drank- en Horecawet</i>	39
	<i>D. Huisvestingswet</i>	43
	<i>E. Wet bijzondere maatregelen grootstedelijke problematiek</i>	46
	<i>F. Woningwet</i>	52
	<i>G. Wet bevordering integriteitsbeoordelingen door het openbaar bestuur</i>	55
	<i>H. Algemene wet inzake rijksbelastingen</i>	58
	<i>I. Invorderingswet 1990</i>	62
	<i>J. Wet basisregistratie personen</i>	64
	<i>K. Wet algemene bepalingen omgevingsrecht</i>	66
	<i>L. Participatiewet</i>	71
	<i>M. Wet maatschappelijke ondersteuning 2015</i>	76
	<i>N. Jeugdwet</i>	80
	<i>O. Wet structuur uitvoeringsorganisatie werk en inkomen</i>	85

1 Leeswijzer

1.1 Algemeen

Dit model privacy protocol kan voor gemeenten een handleiding en basis voor een eigen privacy protocol vormen voor de binnengemeentelijke gegevensuitwisseling ten behoeve van de bestrijding van ondermijning.

Het gaat om een *model* voor een mogelijk privacy protocol. Op bepaalde punten moet het model worden aangevuld aan de hand van de concrete lokale omstandigheden. In dit model is aangegeven op welke punten een gemeente dat kan doen, bijvoorbeeld door het model op dat punt aan te vullen met een analyse van de lokale situatie, of aan de hand van de concrete organisatorische structuur van de gemeente, of door aanvullend beleid te formuleren.

In dit model zijn verschillende stappen geformuleerd. Door die stappen langs te lopen, komt de gemeente tot een aanpak van ondermijning die voldoet aan de eisen van de privacywetgeving. Op deze manier kan elke gemeente dit model gebruiken en desgewenst aanpassen aan de eigen organisatie.

Dit model is niet bedoeld als enige mogelijkheid om de aanpak van ondermijning in te richten. Veel gemeenten hebben al een aanpak ontworpen, waarbij op andere wijze aan de privacyregelgeving zal zijn voldaan.

De aanleiding voor dit model protocol is de voorlichting van de Afdeling advisering van de Raad van State van 20 maart 2019 over *De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning*. De Afdeling adviseerde onder meer om te voorzien in een gemeentelijk model privacy protocol voor binnengemeentelijke gegevensuitwisseling rond ondermijnende criminaliteit.

Het doel van het protocol is om gemeenten, die binnengemeentelijk gegevens willen uitwisselen ten behoeve van de aanpak van de bestuurlijke en bestuursrechtelijke aanpak van ondermijning door gemeenten en zich afvragen of en wat mag, langs de vragen te leiden die zij dan moeten beantwoorden. Daarbij staat steeds voorop dat er een gemeentelijke taak of bevoegdheid moet zijn waarvoor de gegevensuitwisseling wordt overwogen.

Het model kent twee soorten waarborgen. In de eerste plaats gaat het om procesmatige waarborgen. Doel van deze waarborgen is onder andere om te voorzien in een proportionele aanpak. In de tweede plaats gaat het om rechtmatigheidswaarborgen. Het gaat dan om de privacy-vragen die de gemeente in ieder geval moet beantwoorden. Van belang daarbij is om steeds aan te knopen bij bestaande gemeentelijke wettelijke taken en bevoegdheden. Het zal daarbij veelal

gaan om wettelijke taken en bevoegdheden die zien op openbare orde bevoegdheden en bevordering van de leefbaarheid.

In hoofdstuk 2 wordt de aard van de ondermijnende criminaliteit en de noodzaak van de aanpak ondermijning uiteengezet. In hoofdstuk 3 volgt een schematische weergave van de werking van dit protocol en een toelichting op de vier fases die daarin worden onderscheiden. Daarin komen de procesmatige en de rechtmatigheidswaarborgen terug.

Aan de basis van dit model privacy protocol staat het privacy protocol dat de gemeente Rotterdam heeft vastgesteld¹. De belangrijkste toevoegingen aan het Rotterdams privacy protocol worden gevormd door twee "privacy checks" in fase 3 en 4 van het protocol en een analyse van de belangrijkste wetten die in de gemeentelijke praktijk het meest relevant zijn voor het verkrijgen van gegevens ter bestrijding van ondermijning. Daarbij zijn de gemeentelijke wettelijke taken en bevoegdheden steeds leidend. De analyses zijn als bijlage 2 bij dit model protocol gevoegd. In die analyses is per wet aangegeven of, en zo ja, in hoeverre, er ruimte bestaat om binnen een gemeente persoonsgegevens te delen met als oogmerk de bestrijding van ondermijning. De aanpak die in de analyses is gevolgd, kan ook als voorbeeld dienen voor nog verder te analyseren andere relevante wet- en regelgeving die (onder meer) taken en bevoegdheden van gemeenten regelen. De analyses van de verschillende wetten vormen het kader voor de privacy checks in fase 3 en 4 van het protocol. Met de privacy checks zal de inhoudelijke beoordeling van de vraag of, en zo ja, in hoeverre gegevens binnengemeentelijk kunnen worden gedeeld, kunnen worden vormgegeven en wordt invulling gegeven aan de rechtmatigheidswaarborgen.

1.2 Evaluatie

Na vaststelling zal de gemeente periodiek evalueren of in de praktijk ook conform het privacy protocol wordt gehandeld en daarnaast beoordelen of het privacy protocol of de bijlagen daarbij aanpassing behoeven, bijvoorbeeld indien wet- en regelgeving wordt aangepast en/of als sprake is van nieuwe verschijningsvormen van ondermijning. Dergelijke veranderingen kunnen immers van invloed zijn op de rechtmatigheid van de verwerkingen van persoonsgegevens en dit kan leiden tot aanpassing van het protocol.

¹ De Afdeling advisering van de Raad van State heeft in haar advies *De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning* van 20 maart 2019 naar de aanpak van Rotterdam verwezen (p. 52 van het advies).

2 (De aanpak van) ondermijning

2.1 Problematiek en noodzaak van de aanpak van ondermijning

Georganiseerde ondermijnende criminaliteit start, wordt ondersteund en in stand gehouden met ondermijnende activiteiten. De negatieve gevolgen hiervan blijken omvangrijker te zijn en dieper in de samenleving geworteld te zijn dan eerder werd gedacht. De Afdeling advisering van de Raad van State wijst in haar voorlichting van 20 maart 2019 over *De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning* op het inzicht dat ondermijnende criminaliteit niet alleen langs strafrechtelijke weg kan worden bestreden. Gemeenten hebben in de aanpak van ondermijning een belangrijke rol. Een optreden als één overheid en één gemeente waarbij alle partijen hun eigen rol en bevoegdheden uitoefenen is noodzakelijk. De sluimerende aanwezigheid van georganiseerde criminaliteit en bijbehorende ondermijnende activiteiten leiden tot aantasting van de leefbaarheid in de wijken en hebben ernstige gevolgen voor de samenleving op het gebied van veiligheid en maatschappelijke integriteit. Door de verwevenheid van onder- en bovenwereld, hetgeen kenmerkend is voor ondermijnende activiteiten, is het ook mogelijk dat de overheid deze onbewust faciliteert middels subsidies, vergunningen, uitkeringen etc. Dit leidt tot aantasting van de integriteit van de overheid. Hierdoor ontstaan malafide economische machtsposities binnen de samenleving die zijn opgebouwd met op ondermijnende wijze vergaard kapitaal.

Gemeenten ontvangen soms signalen van ondermijnende activiteiten die niet of niet direct passen binnen een georganiseerd criminaliteitsverband en daardoor niet direct onder de criteria van het RIEC-samenwerkingsverband vallen, maar wel relevant zijn voor de gemeentelijke taakuitvoering. De gemeente is veelal een toegangspoort voor burgers en organisaties om meldingen te doen van onrechtmatige zaken. De gemeente heeft hierdoor een belangrijke signaalfunctie. Via haar organisatiestructuur heeft de gemeente veelal ook goed zicht op de lokale (sociale) structuren. Op basis van haar wettelijke taken en bevoegdheden beschikt de gemeente over informatie waarmee ondermijnende activiteiten in kaart kunnen worden gebracht. De gemeente heeft ook verschillende bestuursrechtelijke instrumenten die haar in staat stellen om, in samenhang met de kennis van de fysieke en sociale omgeving van de wijken, barrières op te werpen tegen ondermijnende activiteiten en deze te voorkomen of te verminderen.

Voor een effectieve aanpak van deze ondermijnende activiteiten (en mogelijk georganiseerde criminaliteit) is een geïntegreerde bestuurlijke aanpak binnen de gemeente een noodzakelijk vereiste. De signalen, afkomstig van burgers en

organisaties, dienen als input voor het signaleren en aanpakken van ondermijnende en mogelijk georganiseerde criminaliteit.

In dit rapport wordt voor definiëring van ondermijnende criminaliteit aangesloten bij de kenmerken die de Afdeling advisering van de Raad van State in haar advies noemt:²

- het gaat om georganiseerde criminaliteit (zij het vooral georganiseerd in flexibele netwerken en niet zozeer in hiërarchieën),
- waarmee meestal grote hoeveelheden geld worden verdiend,
- waarbij de criminele activiteiten en de gehanteerde methodes kunnen wisselen. Zij worden bepaald door winstgevendheid en de kans om onopgemerkt te blijven,
- waarbij de grote winsten worden gebruikt om de bovenwereld te ondermijnen (witwaspraktijken, normvervaging binnen gemeenschappen en wijken, inschakeling van advocaten, accountants en notarissen),
- en waarbij de ondermijning ook dreigt door te werken naar de overheid (corruptie, aantasting van integriteit).

2.2 Doel (bestuurlijke en geïntegreerde) aanpak “ondermijning”

Het doel van deze aanpak³ is om door middel van binnengemeentelijke samenwerking:

- ondermijnende activiteiten te signaleren en te analyseren;
- te voorkomen dat de gemeente ondermijnende activiteiten (onbewust) faciliteert;
- vroegtijdig te kunnen signaleren en interveniëren middels een bestuurlijke aanpak;
- onrechtmatigheden en maatschappelijke bedreigingen veroorzaakt door criminele activiteiten te voorkomen, en daarmee bedreigingen voor de leefbaarheid en openbare orde in de gemeente te voorkomen.

Het gaat bij deze aanpak om (rechts)personen/netwerken die binnen de gemeente actief zijn in illegale en of onrechtmatige (criminele) activiteiten:

- a. waarbij de gemeente mogelijkheden heeft om de rechtmatige situatie te herstellen, bedreigingen voor de leefbaarheid of openbare orde tegen te gaan, of onrust weg te nemen en/of;
- b. die de gemeente (onbewust) mogelijk faciliteert.

² Zie het rapport van de Raad van State, ‘De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning’, Voorlichting van de Afdeling advisering van de Raad van State van 20 maart 2019, p. 17.

³ Let op: voor de vraag of gegevens binnengemeentelijk mogen worden verstrekt zal, zoals hierna nog verder zal worden toegelicht, steeds moeten worden aangeknoopt bij bestaande gemeentelijke wettelijke taken en bevoegdheden.

Tevens draagt een goede informatiepositie van gemeenten bij aan de voorfase van de RIEC-samenwerking, althans voor zover gemeenten informatie in RIEC-verband kunnen verstrekken.⁴

2.3 Doel van dit protocol

Dit protocol bevat de benodigde randvoorwaarden om te realiseren dat de gemeentelijke aanpak van ondermijning in lijn met privacywet- en regelgeving plaatsvindt. Deze waarborgen vallen in twee delen uiteen:

- Allereerst gaat het om meer **procesmatige randvoorwaarden**. Hierbij vormen gefaseerdheid (voorkomen van bovenmatig gebruik van gegevens), transparantie (vaststellen van een protocol waarbij zichtbaar en inzichtelijk wordt met welk doel en op welke wijze de gemeente persoonsgegevens verwerkt) en noodzaak (zicht krijgen op waar ondermijning binnen de grenzen van de gemeente aanwezig is) de basisuitgangspunten. Hierdoor worden alleen de gegevens gebruikt die ten behoeve van de analyse en het plan van aanpak relevant zijn.⁵

De procesmatige waarborgen worden gevormd door de opzet van het modelprotocol, zoals opgenomen en toegelicht in hoofdstuk 3.

- Daarnaast gaat het om **rechtmatigheidswaarborgen**. Toepassing van het protocol moet steeds in lijn met privacy wet- en regelgeving zijn. Zowel de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) als sectorale wetten stellen beperkingen aan het uitwisselen en combineren van persoonsgegevens. Het gaat daarbij veelal om abstracte normen, die in iedere specifieke casus moeten worden geïnterpreteerd en toegepast. Dit protocol biedt handvatten voor de analyse die steeds moet worden gemaakt.

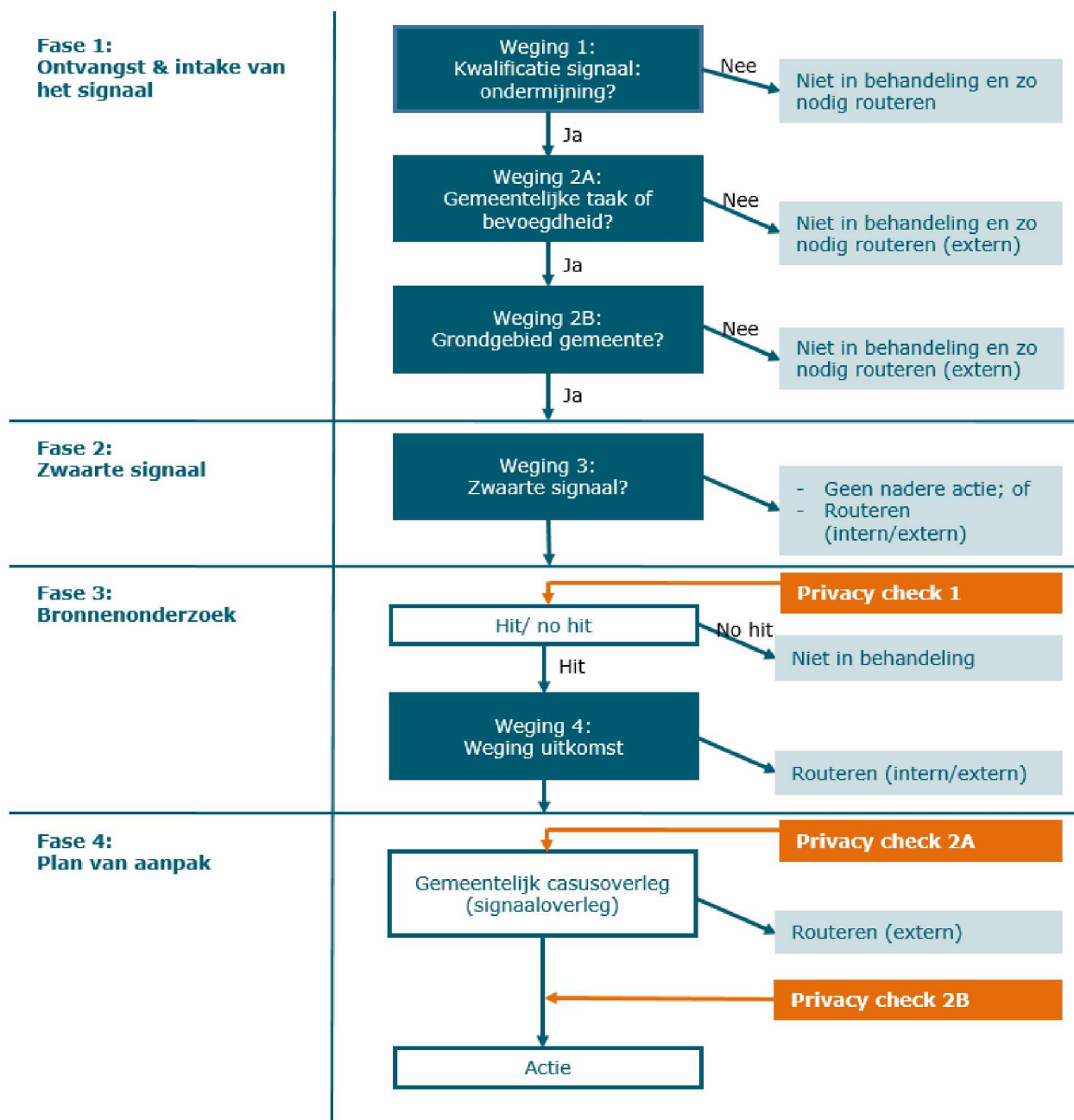
De rechtmatigheidswaarborgen komen in hoofdstuk 4 aan bod in de vorm van een uitwerking van de privacy checks die gedurende het proces moeten worden verricht.

⁴ Onderhavig document heeft geen betrekking op de vraag of en zo ja, in hoeverre gegevens met het RIEC kunnen worden gedeeld.

⁵ De procesmatige randvoorwaarden vormen in zekere zin ook rechtmatigheidswaarborgen.

3 Het protocol: een overzicht

3.1 Schematische weergave



3.2 Toelichting op de 4 fases van het protocol

Het proces van het signaleren en aanpakken van signalen van ondermijnende activiteiten verloopt met het oog op proportionaliteit en subsidiariteit in vier fases, en met de inzet in die fases van een daartoe aangewezen functionaris (hierna: de regisseur ondermijning) die waarborgt dat de verschillende fases ook op juiste wijze worden gevolgd. Hieronder worden de verschillende fases toegelicht. Daarbij geldt dat de beoordeling van een binnengekomen signaal het startpunt van het protocol vormt. Er wordt in dit protocol dan ook tot uitgangspunt genomen dat het delen van signalen met de regisseur ondermijning op rechtmatige wijze geschiedt. Vanzelfsprekend zal een verstrekker van een signaal wel steeds moeten vaststellen of die verstrekking in lijn is met de privacyregelgeving.

Fase 1 heeft betrekking op de ontvangst en de intake van een signaal. Een signaal kan op verschillende manieren binnenkomen, zoals via een telefonische, schriftelijke (vaak digitale) melding van een burger of professional of een melding via Meld Misdaad Anoniem.

Het signaal wordt na ontvangst beoordeeld door de regisseur ondermijning. Voor de beoordeling van een signaal is van belang wat het signaal inhoudt en of het betrekking heeft op ondermijning. Dat betreft de **eerste weging**. Een signaal wordt bij intake beoordeeld op grond van een aantal kenmerken en indicatoren.

Deze signaalanalyse is nader uitgewerkt in bijlage 1 van dit model protocol: de 'Checklist ten behoeve van beoordelingskader Ondermijning'. De beoordeling van een signaal vindt plaats binnen het kader 'ondermijnende criminaliteit'. In aanvulling hierop is tenminste sprake van één van de indicatoren 'situationele en lokale verankering'. Daarna wordt gekeken naar de indicatoren 'signalering', die nader uitgewerkt zijn in een lijst met 'red flags'.

Zodra aan de hand van bijlage 1 – die geen limitatief overzicht bevat en die ook kan worden aangepast al naar gelang de eigen gemeentelijke praktijk en ervaringen⁶ – is vastgesteld dat sprake is van een ondermijningssignaal, vindt de **tweede weging** plaats.

De eerste weging valt uiteen in twee delen: weging 2A en weging 2B.

Weging 2A betreft de vraag of het binnengekomen signaal betrekking heeft op een taak of bevoegdheid van de gemeente, en niet op een taak of bevoegdheid van een andere instantie (bijvoorbeeld van de politie, kinderbescherming, etc.). Het is hierbij

⁶ De checklist is overgenomen uit het eerder genoemde privacyprotocol van de gemeente Rotterdam.

dus van belang na te gaan of het signaal in beginsel tot gemeentelijk optreden kan leiden. Een dergelijke gemeentelijke taak is bijvoorbeeld een van de openbare orde-bevoegdheden van de burgemeester.⁷

Vervolgens zijn er twee opties:

- ➔ Het signaal kan mogelijk aanleiding vormen voor inzet van een gemeentelijke taak of bevoegdheid. In dat geval wordt overgegaan naar weging 2B;
- ➔ Het signaal kan geen aanleiding vormen voor inzet van een gemeentelijke taak of bevoegdheid. Het signaal wordt niet in behandeling genomen door de gemeente en zo nodig doorverwezen naar de bevoegde instantie.⁸

Weging 2B betreft de vraag of het signaal betrekking heeft op het grondgebied van de gemeente. Het gaat, met andere woorden, om de vraag of het subject of object waar het signaal betrekking op heeft binnen de gemeente woont respectievelijk is gevestigd. De volgende vragen moeten daarbij achtereenvolgend worden beantwoord:

1. Gaat het om een object of een subject?
2. In het geval van een object: is het object binnen de gemeentegrenzen gelegen (dan wel is er anderszins een link met de gemeente)?
3. In het geval van een subject: is het subject woonachtig binnen de gemeentegrenzen (dan wel is er anderszins een link met de gemeente)?

Deze vragen worden beantwoord aan de hand van informatie uit openbare bronnen zoals de basisregistraties. Daarbij zullen in ieder geval het handelsregister van de Kamer van Koophandel, het Kadaster, de Basisregistratie personen (BRP) en de Basisregistratie adressen en gebouwen (BAG) vaak van belang zijn.⁹

Ook nu zijn er weer twee opties:

- ➔ Het signaal heeft betrekking op het grondgebied van de gemeente. In dat geval gaat men door naar fase 2;
- ➔ Het signaal valt buiten het grondgebied van de gemeente. Het signaal wordt niet in behandeling genomen door de gemeente en zo nodig doorverwezen naar een andere gemeente of instantie.¹⁰

⁷ Zie voor een uitwerking van de verschillende openbare orde-bevoegdheden van de burgemeester het rapport van de Raad van State, 'De rol van gemeenten in de bestuurlijke en integrale aanpak van ondermijning', Voorlichting van de Afdeling advisering van de Raad van State van 20 maart 2019, hoofdstuk 3.

⁸ Onderhavig document heeft geen betrekking op de vraag of en zo ja, in hoeverre gegevens met andere (wel bevoegde) instanties kunnen worden gedeeld.

⁹ Zie www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/basisregistraties-en-afsprakenstelsels/inhoud-basisregistraties/stelselplaat/ voor een overzicht van basisregistraties. Bijlage 2 onder I bevat een uitwerking van de Wet basisregistratie personen.

¹⁰ Onderhavig document heeft geen betrekking op de vraag of en zo ja, in hoeverre gegevens met een andere gemeente of instantie kan worden gedeeld.

*Aan het einde van **fase 1** is vastgesteld of het signaal:*

- betrekking heeft op ondermijning (zie daarvoor bijlage 1);*
- mogelijk aanleiding kan vormen voor inzet van een gemeentelijke taak of bevoegdheid (het zal hierbij veelal gaan om wettelijke taken en bevoegdheden die zien op openbare orde bevoegdheden en bevordering van de leefbaarheid); én*
- betrekking heeft op een subject of object dat binnen de gemeente woont resp. is gevestigd.*

Alleen als dat zo is, komt fase 2 in beeld.

In **fase 2** vindt de beoordeling van signalen van burgers en professionals plaats. Hier vindt dan ook de **derde weging** plaats. De gemeente weegt de zwaarte van het signaal en beoordeelt waar het signaal het beste kan worden afgehandeld.

De gemeente zou ten aanzien van de 'zwaarte-weging' kunnen vastleggen, bijvoorbeeld in gemeentelijk beleid, hoe een dergelijke weging, aansluitend bij lokale omstandigheden, wordt uitgevoerd en welke factoren daarbij relevant zijn, zoals 'is het signaal voldoende concreet?' 'is het signaal van recente datum?', 'heeft het signaal betrekking op een onderwerp ter zake waarvan een trend- en fenomeenanalyse is uitgevoerd waaruit blijkt dat er bijzondere aandacht voor een bepaald fenomeen vereist is?', etc. Ook kan in dit beleid worden opgenomen onder welke omstandigheden in aanvullende openbare bronnen, waaronder op internet, onderzoek kan worden gedaan naar het signaal.¹¹ Het zal in beide gevallen steeds moeten gaan om objectieve criteria.

Na deze tweede weging volgt een beslismoment bij het ondermijningsteam:

- ➔ er gebeurt niets met het signaal. Het signaal wordt niet in behandeling genomen (waarbij het signaal gedurende een jaar versleuteld bewaard wordt en daarna vernietigd wordt); of
- ➔ een signaal wordt naar een gemeentelijk onderdeel gestuurd dat de regie vervolgens voert; of
- ➔ een signaal wordt naar het RIEC gestuurd dat de regie vervolgens voert¹²; of
- ➔ er volgt een vervolganalyse, waarmee fase 3 ingaat.¹³

*Aan het einde van **fase 2** is vastgesteld of het signaal zwaar genoeg is om daar een nadere analyse op te verrichten. Alleen in dat geval komt fase 3 in beeld. Of een signaal zwaar genoeg is, kan worden bepaald aan de hand van daartoe te definiëren gemeentelijke criteria.*

¹¹ Hierbij zou aansluiting gezocht kunnen worden bij het Protocol internetonderzoek door gemeenten. Zie <https://autoriteitpersoonsgegevens.nl/nl/nieuws/besluit-internetonderzoek-door-gemeenten>.

¹² Zie in dit verband voetnoot 4.

¹³ In dit protocol wordt tot uitgangspunt genomen dat het delen van signalen met (de regisseur ondermijning van) het ondermijningsteam en het verder verwerken van die signalen op rechtmatige wijze geschiedt.

In **fase 3** van het protocol bepaalt de privacy officer¹⁴ in het kader van **Privacy check 1** (zie daarover hoofdstuk 4 hierna) of en zo ja welke gemeentelijke bronnen naar aanleiding van het concrete signaal kunnen worden geraadpleegd, en, na raadpleging van de betrokken gemeentelijke bronnen door middel van een hit/no hit-vraag, welke gegevens relevant zijn voor het signaal. Soms zal aan de hand van 'dat'-informatie kunnen worden geconstateerd dat verdere 'wat-informatie' niet nodig is, bijvoorbeeld als uit de 'dat-informatie' blijkt dat het om (te) oude informatie gaat. In dat geval zal geen 'wat-informatie' mogen worden opgevraagd. Onderdeel van de hit/no hit-check is de beoordeling of het om voor het signaal relevante informatie gaat.

- ➔ Als van een persoon bepaalde, voor het signaal relevante, gegevens in een bronbestand van een gemeentelijk onderdeel voorkomen, is sprake van een 'hit': de betrokken persoon/bepaalde info is bekend binnen het betreffende gemeentelijke domein. Zie hierna voor de vervolgstappen.
- ➔ Als er geen hit is dan wordt verder geen actie ondernomen: het signaal wordt niet in behandeling genomen.

Bij een hit volgt de **vierde weging**, waarbij de uitkomsten van de hit(s) worden gewogen. Concreet gaat het om de vraag of de hit(s) een signaal in voldoende mate bevestigen om door te gaan met het onderzoek naar het signaal. De analyse leidt tot:

- a. een mono- of multidisciplinaire aanpak door één gemeentelijk onderdeel of meerdere samenwerkende gemeentelijke onderdelen: er hoeft geen ondermijnende activiteit te zijn, de regie en uitvoering liggen bij desbetreffend gemeentelijke onderdeel/onderdelen op grond van de daarvoor bedoelde wettelijke bevoegdheid(heden). Hierbij is een regierol vanuit het ondermijningsteam niet benodigd;
- b. het gemeentelijk casusoverleg met betrokken afgevaardigden van de desbetreffende gemeentelijke onderdelen waar sprake is van een relevante hit en waarbij de regie bij het ondermijningsteam ligt. Dit is dan op grond van het gegeven dat het signaal en de informatie uit de fases 1, 2 en 3 op ondermijning duiden. Het vormt de start van fase 4;
- c. doorgeleiding naar het RIEC-samenwerkingsverband, omdat er sprake is van georganiseerde criminaliteitsverband waarvoor de partners in het RIEC benodigd zijn.¹⁵

¹⁴ Of een andere daartoe aangewezen deskundig persoon. Hierna wordt het begrip privacy officer gebruikt.

¹⁵ Zie in dit kader voetnoot 4.

*Aan het einde van **fase 3** is door de privacy officer in het kader van **Privacy check 1** vastgesteld welke gemeentelijke bronnen naar aanleiding van het concrete signaal kunnen worden geraadpleegd, en, na raadpleging van de betrokken gemeentelijke bronnen door middel van een hit/no hit-vraag, vastgesteld welke gegevens relevant zijn voor het signaal. Op basis daarvan wordt beoordeeld of het signaal (verder) in behandeling wordt genomen en zo ja of sprake is van situatie a, b of c hierboven. Alleen in geval van situatie b, treedt fase 4 in werking.*

Fase 4 van het protocol gaat over het ontwikkelen van een plan van aanpak en het voeren van regie op het plan en het afsluiten van de casus. Voorafgaand aan het gemeentelijk casusoverleg (signaaloverleg) voert de privacy officer **Privacy check 2** uit (zie daarover hoofdstuk 4 hierna): er wordt vastgesteld of en zo ja, welke van de in de fases 1 t/m 3 verzamelde gegevens mogen worden gedeeld met het/de relevante, bij het signaal betrokken, gemeentelijke onderdeel/onderdelen ten behoeve van de verdere aanpak. De privacy officer kan daarbij ook beoordelen of eventuele onderliggende gegevens uit een concreet dossier voor de verdere aanpak van de casus binnengemeentelijk mogen worden gedeeld en zo ja, met welk gemeentelijk onderdeel/welke gemeentelijke onderdelen.

Als de (gezamenlijke of volgordelijke) aanpak op basis van het signaaloverleg is bepaald en duidelijk is welke concrete aanpak en bevoegdheden de gemeente wil inzetten en welke binnengemeentelijke gegevensuitwisseling daarvoor nodig is, controleert de privacy officer tot slot of de verzamelde gegevens mogen worden gedeeld met het relevante gemeentelijke onderdeel/de relevante gemeentelijke onderdelen ten behoeve van de verdere aanpak en beoogde inzet van bevoegdheden door die gemeentelijke onderdelen. Deze beoordeling vindt opnieuw plaats aan de hand van de bij de privacy checks te stellen vragen. Dit betreft **weging 5**.

Terzijde: tijdens het signaaloverleg kan alsnog blijken dat er geen binnengemeentelijke actie vereist is, maar dat het signaal bij het RIEC moet worden ingebracht.¹⁶

*Aan het einde van **fase 4** is door de privacy officer in het kader van **Privacy check 2** vastgesteld:*

- i) welke in de fases 1 t/m 3 verzamelde gegevens met de relevante, bij het signaal betrokken, gemeentelijke onderdelen mogen worden gedeeld ten behoeve van de vaststelling van de verdere aanpak (**privacy check 2A**); en*
- ii) welke binnengemeentelijke gegevensuitwisseling nodig is voor het verwezenlijken van die aanpak en of dat toelaatbaar is (**privacy check 2B**).*

Tot slot

¹⁶ Zie in dit kader voetnoot 4.

De gemeente bepaalt hoe lang na afsluiting van een casus monitoring volgt (in een actieve omgeving), en hoe lang de informatie over de casus daarna nog bewaard moet worden (in een niet actieve omgeving).

3.3 Waarborgen in de verschillende fases

Het gebruik van de checklist

In de eerste fase wordt aan de hand van de checklist op grond van een aantal kenmerken en indicatoren beoordeeld of daadwerkelijk sprake is van een ondermijnings signaal. Daarmee kan de checklist worden aangemerkt als een verzameling van een of meer kenmerken die mogelijk samenhangen met een hoger (overtredings)risico, namelijk dat sprake is van ondermijning. Op basis daarvan wordt bepaald welke bevoegdheden de gemeente kan en wil inzetten. De kenmerken en indicatoren in de checklist kunnen daarmee worden aangemerkt als selectiecriteria zoals bedoeld in het Mensenrechtelijk Toetsingskader (hierna toetsingskader) van het College voor de Rechten van de Mens. Het toetsingskader helpt overheidsfunctionarissen te bepalen wanneer selectiecriteria leiden tot discriminatie op grond van ras of nationaliteit. Omdat de checklist geen limitatief overzicht bevat en kan worden aangepast al naar gelang de eigen gemeentelijke praktijk en ervaringen, kan het toetsingskader helpen bepalen wanneer selectiecriteria leiden tot discriminatie op grond van ras of nationaliteit. Het presenteert de (denk)stappen die doorlopen moeten worden om te toetsen of een risicoprofiel binnen de grenzen van het discriminatieverbod blijft. Het is aan gemeenten zelf om hun voorgenomen aanvullingen en/of aanpassingen te toetsen aan de hand van het toetsingskader.

[Discriminatie door risicoprofielen - Mensenrechtelijk toetsingskader | Rapport | Rijksoverheid.nl](#)

Het bewaren van signalen en nadien verkregen informatie

Uit de hierboven opgenomen toelichting op de vier fases volgt dat in iedere fase de conclusie kan zijn dat een signaal niet (verder) wordt behandeld. De gemeente bepaalt of en zo ja, hoe lang dergelijke signalen (versleuteld) worden bewaard (en wanneer er aanleiding is om een signaal te ontsleutelen). Datzelfde geldt voor informatie betreffende een afgesloten casus. Hoofregel is dat niet-relevante signalen moeten worden verwijderd.

Het informeren van betrokkenen

Daarnaast legt de gemeente, bijvoorbeeld in beleid, vast wanneer de betrokken persoon of het betrokken bedrijf wordt geïnformeerd over een onderzoek. Vanuit

transparantie-oogpunt is het uitgangspunt dat betrokkenen zo snel en volledig mogelijk worden geïnformeerd over onderzoek dat naar hen wordt gedaan. Dat is evenwel niet altijd mogelijk, omdat het informeren van betrokkenen het onderzoek kan schaden. Dat doet niet af aan de mogelijkheid om meer in algemene zin te informeren over de mogelijkheid dat gegevens verder worden verwerkt ter bestrijding van ondermijning, bijvoorbeeld in het algemene privacybeleid van de gemeente of, beter nog, bij het in eerste instantie verzamelen van de gegevens bij de betrokkene. In beleid over het informeren van betrokkenen kan worden aangesloten bij de informatieplicht van de artikelen 13 en 14 AVG en de uitzonderingen daarop zoals opgenomen in artikel 23 AVG en artikel 41 UAVG. Bij verwerkingen van persoonsgegevens die onder het toepassingsbereik van de AVG vallen, is het vanzelfsprekend verplicht te voldoen aan deze bepalingen inzake de informatieplicht.

Rechten van de betrokkenen

Verder hebben betrokkenen, in ieder geval als het gaat om de verwerking van persoonsgegevens, het recht te verzoeken om inzage in de persoonsgegevens die ten aanzien van hen worden verwerkt (artikel 15 AVG). Desgewenst kunnen zij verzoeken om rectificatie, wissing of beperking van die verwerking (artikel 16, 17 en 18 AVG). Ook hierbij kunnen de uitzonderingen van artikel 23 AVG en artikel 41 UAVG aan inwilliging van de verzoeken in de weg staan.

4 **Uitwerking van de twee privacy checks in fase 3 en 4**

In **fase 3** van het protocol bepaalt de privacy officer in het kader van **Privacy check 1** of en zo ja welke gemeentelijke bronnen naar aanleiding van het concrete signaal kunnen worden geraadpleegd. In **fase 4** stelt de privacy officer in het kader van **Privacy check 1** vast:

- i) welke in de fases 1 t/m 3 verzamelde gegevens met de relevante, bij het signaal betrokken, gemeentelijke onderdelen mogen worden gedeeld ten behoeve van de vaststelling van de verdere aanpak; en
- ii) welke binnengemeentelijke gegevensuitwisseling nodig is voor het verwezenlijken van die aanpak en of dat toelaatbaar is.

De vraag welke binnengemeentelijke gegevensdeling is toegestaan moet steeds worden beantwoord aan de hand van de specifieke wettelijke regeling die op de betreffende gemeentelijke informatie van toepassing is.

Dat is nog niet zo eenvoudig: niet alleen zijn op de verschillende soorten gemeentelijke bronnen verschillende wettelijke regelingen van toepassing, ook is iedere casus anders en zal daarom steeds een op het geval toegespitste afweging moeten worden gemaakt. Er is dan ook niet één simpel antwoord te geven op de vraag wie, wanneer, welke informatie binnen de gemeente mag delen ter bestrijding van ondermijning.

Privacy check 1 (start van fase 3)

Privacy check 1 vormt de belangrijkste privacybeoordeling en vindt plaats in het kader van de hit/no hit-analyse (start van fase 3). Per geval moeten steeds de volgende privacyvragen worden beantwoord.

A. Wat is de wettelijke basis voor het primaire gebruik?

Allereerst wordt bepaald welke gegevens nodig zijn voor het onderzoek naar een signaal. Op basis daarvan wordt vastgesteld op basis van welke gemeentelijke taak deze gegevens aanvankelijk zijn verkregen (ook wel: het primaire gebruik van de gegevens). Deze taak zal steeds een wettelijke basis hebben, bijvoorbeeld in de Gemeentewet of een andere sectorale wet.

De wettelijke regeling op basis waarvan gegevens aanvankelijk zijn verkregen, is in sterke mate bepalend voor de vraag of gegevens (ook) kunnen worden gebruikt voor de bestrijding van ondermijning. Zo kan die wettelijke regeling een geheimhoudingsbepaling bevatten die het (verdere) gebruik van gegevens beperkt of anderszins regelen of en zo ja, in hoeverre de gegevens voor bepaalde doeleinden of taken mogen worden gebruikt.

B. Is bestrijding van ondermijning verenigbaar met het oorspronkelijk doel waarvoor de gegevens zijn verzameld?

In aanvulling daarop geldt dat het gebruik van gegevens ter bestrijding van ondermijning een toelaatbare verdere verwerking moet zijn. Van een toelaatbare verdere verwerking is sprake als het gebruik van de gegevens verenigbaar is met het doel waarvoor de gegevens aanvankelijk zijn verkregen. Daarbij moeten de volgende vragen worden beantwoord:

1. Wat is het doel van de wet en/of de wettelijke bepaling op basis waarvan de gegevens aanvankelijk zijn verkregen?
2. Is het bestrijden van ondermijning verenigbaar met dat primaire doel?
3. Wat is het kader waarin de persoonsgegevens zijn verzameld?
4. Wat is de aard van de verwerkte persoonsgegevens?
5. Wat zijn de mogelijke gevolgen voor de betrokkene?
6. Worden er passende waarborgen getroffen?¹⁷

Van verenigbaarheid in de zin van de vragen 1 en 2¹⁸ zal sneller sprake zijn als de wettelijke basis voor het primaire gebruik gerelateerd is aan het bestrijden van ondermijning, bijvoorbeeld een openbare orde bevoegdheid van de burgemeester. Dat wordt lastiger als de wettelijke basis betrekking heeft op een geheel ander domein, zoals het sociaal domein.

“Het bestrijden van ondermijning” als doel voor een verdere verwerking is breed. In het concrete geval wordt dit doel daarom gepreciseerd door het te vertalen naar de gemeentelijke wettelijke bevoegdheden die de gemeente ten behoeve van de aanpak van het signaal zou willen inzetten. Het zal hierbij veelal gaan om wettelijke taken en gemeentelijke bevoegdheden die zien op openbare orde bevoegdheden en bevordering van de leefbaarheid. Van belang hierbij is dat aan het voorzienbaarheids criterium wordt voldaan: een betrokkene moet kunnen voorzien dat de bedoelde gegevensverstrekking zou kunnen plaatsvinden.

Indien de privacy officer concludeert dat sprake is van onverenigbaarheid, kan het gebruik van de gegevens ter bestrijding van ondermijning toch toelaatbaar zijn als er een expliciete wettelijke grondslag voor dat gebruik is (zie onder het kopje: *Wat is de wettelijke basis voor het primaire gebruik?*).

Bijlage 2 bevat voorbeelden van bovenstaande analyse met betrekking tot wetten op basis waarvan gegevens kunnen worden verkregen die vaak relevant zullen zijn voor het tegengaan van ondermijning door gemeenten (als gezegd zal het hierbij veelal

¹⁷ Zie artikel 6, vierde lid, AVG voor de factoren waar rekening mee moet worden gehouden bij de vraag of een verdere verwerking verenigbaar is met het doel waarvoor (persoons)gegevens aanvankelijk zijn verkregen.

¹⁸ Zie hierna achter C voor de vragen 3 t/m 6.

gaan om wettelijke taken en bevoegdheden die zien op openbare orde bevoegdheden en bevordering van de leefbaarheid).

Voor de verwerking van bijzondere en strafrechtelijke persoonsgegevens geldt een bijzonder regime: die gegevens mogen in beginsel alléén worden verwerkt als uit de wet op basis waarvan die gegevens zijn verkregen blijkt dat dat – voor de in die wet genoemde doelen – mag. Voor strafrechtelijke gegevens geldt nog een andere relevante uitzonderingsgrond: een gemeente zal die gegevens mogen verwerken als zij krachtens de Wet politiegegevens of Wet justitiële en strafvorderlijke gegevens zijn verkregen (zie voor een uitwerking van verstrekking op grond van de Wet politiegegevens bijlage 2).

C. Is het gebruik van de gegevens noodzakelijk en proportioneel en wordt aan het subsidiariteitsvereiste voldaan?

Gegevens mogen alleen worden gebruikt voor de bestrijding van ondermijning als dat gebruik noodzakelijk en proportioneel is en er geen minder ingrijpende middelen voorhanden zijn. Bij de vraag of een verstrekking noodzakelijk en proportioneel is, spelen onder meer de volgende omstandigheden een rol:

- de aard en ernst van een binnengekregen signaal. Bij aanwijzingen dat er ernstige feiten spelen, zal informatie eerder mogen worden gedeeld;
- de ernst van de inbreuk die op de persoonlijke levenssfeer van de betrokkene wordt gemaakt. Daarbij kan onder meer acht worden geslagen op:
 - de voorzienbaarheid van de (cumulerende) inbreuk die op de persoonlijke levenssfeer wordt gemaakt;
 - de vraag in hoeverre een compleet beeld van de betrokkene ontstaat;
 - in hoeverre een betrokkene negatieve gevolgen zal ondervinden van de gemaakte inbreuk;
 - de aard van de gegevens (hoe gevoeliger, hoe terughoudender ermee moet worden omgegaan);
 - of een betrokkene zich effectief kan verweren tegen gemaakte inbreuken (bijv. rechtsbescherming).

In het kader van de vraag naar subsidiariteit moet bijvoorbeeld, als is vastgesteld dat sprake is van een verenigbare verdere verwerking of een expliciete wettelijke grondslag voor het gebruik, eerst een 'hit/no hit'-check worden gedaan (met andere woorden: eerst nagaan dat er bepaalde informatie bij de gemeente berust), alvorens de informatie zelf kan worden geraadpleegd (wat is de informatie waarover de gemeente beschikt). In sommige gevallen kan de eerste vorm van informatie volstaan (subsidiariteit).

Aanvullende waarborg: privacy check 2A en 2B

Als aanvullende waarborg is in dit protocol een tweede privacy beoordelingsmoment opgenomen: privacy check 2A en 2B.

Deze wordt door de privacy officer uitgevoerd voorafgaand aan het signaaloverleg (start fase 4). De privacy officer stelt bij iedere casus vast of en zo ja welke verzamelde gegevens daadwerkelijk mogen worden gedeeld met de/het relevante, bij het signaal betrokken, gemeentelijke onderdeel/de relevante gemeentelijke onderdelen ten behoeve van de verdere aanpak. De privacy officer kan daarbij ook beoordelen of eventuele onderliggende gegevens uit een concreet dossier voor de verdere aanpak van de casus binnengemeentelijk mogen worden gedeeld en zo ja, met welk gemeentelijk onderdeel / gemeentelijke onderdelen. Met name de beoordeling van de *noodzaak* om informatie te delen, zal daarbij centraal staan. Het gaat dan niet alleen om de hoeveelheid gegevens, maar ook om de vraag of alle deelnemers de betreffende informatie nodig hebben. Denkbaar is bijvoorbeeld dat een signaal op maar 3 domeinen ziet en de informatie ten aanzien van dat signaal dus ook alleen aan de deelnemers vanuit die domeinen mag worden verstrekt (in plaats van aan alle domeinen die aan tafel zitten).

Zoals aangegeven in paragraaf 3.2 kan ook in fase 4 – bij het bepalen van het plan van aanpak voor een casus – een privacy check nodig zijn, te weten om te bepalen of de verzamelde gegevens daadwerkelijk mogen worden gedeeld met het relevante gemeentelijke onderdeel/de relevante gemeentelijke onderdelen ten behoeve van de verdere aanpak en beoogde inzet van bevoegdheden. Daartoe zullen dezelfde vragen moeten worden gesteld als hierboven omschreven.

Bijlage 1: checklist ten behoeve van de signaalanalyse (niet limitatief)¹⁹

Aan de hand van onderstaande checklist wordt stapsgewijs beoordeeld of het signaal betrekking heeft op ondermijning. De checklist is afhankelijk van maatschappelijke ontwikkelingen en kan reeds daarom niet als limitatief worden beschouwd. Vanzelfsprekend kan de checklist worden aangepast al naar gelang de eigen gemeentelijke praktijk en ervaringen.

De ontvangst van een signaal door de regisseur ondermijning vormt het startpunt voor het protocol. Er wordt tot uitgangspunt genomen dat het delen van signalen met de regisseur ondermijning op rechtmatige wijze geschiedt. Vanzelfsprekend zal een verstrekker van een signaal wel steeds moeten vaststellen of die verstrekking in lijn is met de privacyregelgeving.

Stap 1:

Het signaal heeft betrekking op een dan wel meer van de volgende categorieën personen.

Openbare inrichtingen

- a. pandeigenaar
- b. verhuurder
- c. huurder/pachter
- d. exploitant
- e. beheerder/Leidinggevende
- f. tussenpersoon
- g. geldschietters

Georganiseerde hennepteelt/drugs(-handel)

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Tussenpersoon (verhuurmakelaar, evt. andere vormen?)

Mensenhandel, -smokkel en uitbuiting (o.a. illegale prostitutie)

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. eigenaar (illegale) seksinrichting
- e. eigenaar (illegale) massagesalon
- f. exploitant van een vergunde seksinrichting
- g. beheerder van een vergunde seksinrichting
- h. illegaal werkende prostituee (dwz zonder vergunning)

¹⁹ De checklist is overgenomen uit het eerder genoemde privacyprotocol van de gemeente Rotterdam.

Fraude in de vastgoedsector

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Tussenpersoon (verhuurmakelaar, andere vormen?)
- e. stichting, vereniging of andere ondernemingsvorm (of bestuurders hiervan)

Misbruik in de vastgoedsector

- a. Huis/pandeigenaar
- b. Verhuurder
- c. Huurder
- d. Tussenpersoon (verhuurmakelaar, andere vormen?)
- e. stichtingvereniging of andere ondernemingsvorm (of bestuurders hiervan)

Fraude en/of witwassen en daaraan gerelateerde vormen of andere vormen van financieel-economische criminaliteit

(o.a. ook illegaal gokken/heling/underground banking)

- a. ontvanger/begunstigde uitkering vanuit de gemeente
- b. ontvanger/begunstigde subsidie vanuit de gemeente
- c. andersoortige begunstigende beschikking vanuit de gemeente
- d. een tussenpersoon/gemachtigde met betrekking tot zorg
- e. pandeigenaar

Overig

- a. overige faciliteerders die ondermijnende of criminele activiteiten mogelijk maken en/of (on)bewust in stand houden;
- b. en/of personen die een rol spelen bij een regionaal thema of een handhavingsknelpunt.

Stap 2:

Het signaal kan een van onderstaande kenmerken omvatten:

Kader/begripsbepaling 'ondermijnende criminaliteit'	
Aantasting van instituten die zich richten op legale perspectieven en de werking van het samenlevingssysteem borgen en sturen	
Aantasting van de gezagspositie van bestuur, politie en/of andere overheidsorganen	
Aantasting of latente c.q. mogelijke aantasting van de openbare orde en veiligheid	
Ontwrichting of latente c.q. mogelijke ontwrichting van de maatschappelijke, politieke en/of economische structuren	
Onrechtmatigheden, maatschappelijke bedreigingen en/of georganiseerde criminaliteit	

In aanvulling is tenminste sprake van één van onderstaan- de locatie-, persoons- en/of bedrijfsgebonden indicatoren binnen het grondgebied van gemeente.

Indicator 'situatieve en lokale verankering'	
Gelegenheidsstructuren (of criminaliteit bevorderende condities) in de bestuurlijke omgeving (wet en regelgeving; toezicht en handhaving)	
Gelegenheidsstructuren (of criminaliteit bevorderende condities) in de (sociaal-)maatschappelijke omgeving (fysieke omgevingskenmerken, maatschappelijke ontwikkelingen, sociale relaties of netwerken, informele controle)	
Gelegenheidsstructuren (of criminaliteit bevorderende condities) in de zakelijke / economische omgeving (beroepen, branches, marktpartijen).	
Processen, procedures, instructies en/of structuren binnen (een) (publieke) organisatie(s) die het mogelijk maakt (on-)bewust te faciliteren	
Bij de gelegenheidsstructuren is een locatie (zoals een pand of bedrijf/onderneming), een persoon, een groep, een familie en/of netwerk (meerdere personen die samenwerken) betrokken	

Stap 3

En kan tenminste sprake zijn van één van onderstaande indicatoren, hetgeen nader uitgewerkt is in de bijbehorende lijst met 'red flags'.

Indicator 'signalering'	
Incongruenties (omstandigheden en gedragingen); feit dat indicaties niet goed bij elkaar passen, niet goed overeenstemmen in aard, omvang en intensiteit	
Malafide en/of criminele activiteiten, hinder en/of overlast	
Veelal systematisch en structureel gepleegd	
Latent aanwezig	
Complex	

Lijst met 'red flags'

Algemeen	
• Salaris uitbetalen per week en/of per kas. • Financiële man/financieel 'directeur' kan factuur niet plaatsen en moet navraag doen/fiat vragen bij de baas. • Sterke waardeestijging van moeilijk waardeerbare aandelen. • Grootaandeelhouder heeft geen weet van wat überhaupt in de onderneming gaande is. • De officiële eigendomsverhoudingen in rechtspersoon zijn niet in verhouding met de daadwerkelijke gezagsverhoudingen. • Huurders/gebruikers/kopers die ook op een andere wijze een functie bij koper of verkoper van een onroerende zaak vervullen • Onmogelijkheid om gezien inkomen en/of vermogen onroerende zaken te kopen en/of financiering te krijgen. • Waarde van afzonderlijke appartementsrechten na splitsing (in het bijzonder indien een deel in de privé- en een deel de zakelijke sfeer terecht komen. • Leningen met aflossingen/geldstromen, waarvan de herkomst niet of onvoldoende herleidbaar is. • Plotselinge stijgingen in vermogensopstellingen box 3 inkomstenbelasting. • Niet gebruikelijke juridische vastgoedconstructies, mede in combinatie met verzoek om vrijstelling ex art. 15 lid 1 letter h WBR. • Vastgoedondernemingen die volgens het handelsregister geen werkzame personen hebben. • Aangifte door huurder van bedreiging/ intimidatie omdat hij het idee heeft dat de verhuurder hem uit de woning wil hebben. (Een dergelijke aangifte kan duiden op een criminele verhuurder.) • Meerdere provisies naar verschillende personen. Personen die voor elkaar betalen. • Onlogische geldstromen en/of facturen. • Vaste 'functionele' relatie tussen bankmedewerker en specifieke personen van overige zakelijke dienstverleners. • Onvoldoende waarborgen binnen de financiële onderneming voor de bescherming van de integriteit van medewerkers door functiescheiding.	

- Exclusieve relatie tussen medewerker van hypotheekbank, notaris en belastingadviseur.
- Geconstateerd is dat grote bedragen niet opvallen en vertrouwen wekken. Juist bij grote bedragen dient de financiële onderneming echter alert te zijn omdat daarin schijn en wezen kunnen verschillen
- Het gebruik van waardeverklaringen in plaats van officiële taxatierapporten.
- Afwijkend tarief voor (ogenschijnlijke) standaardopdracht.
- Waardebepaling van panden met krakers en panden met mogelijke bestemmingswijziging.
- Het gebruik van oude beschikbare bronnen (bijvoorbeeld oud kadastraal uittreksel of bewijs van eigendom).
- Meerdere sterk wisselende taxaties voor eenzelfde vastgoed in een relatief korte periode.
- Exclusieve relatie (volume- en/of prijsafspraken) tussen de makelaar/taxateur en de intermediair/financiële onderneming voor taxaties ten behoeve van de financiering.
- Eigen belang bij de uitkomst van de taxatie of de hoogte van het taxatiebedrag.
- Retourprovisie of commerciële afspraken met intermediairs en financiële onderneming.
- Ontbreken van vaste onderdelen in het onderzoek ten behoeve van de waardebepaling door de makelaar/taxateur (informatie over vergelijkbare panden, WOZ-waarden, gebruik van het puntensysteem voor het vaststellen van de waarde of de hoogte van de huren, sloop-/handhaven-afweging).
- Ontbreken standaarddossieropbouw met onderliggende documentatie en uitzonderingsrapportages
- Onvoldoende waarborgen bij de makelaar/taxateur voor de bescherming van de integriteit van medewerkers door functiescheiding (afhankelijk van omvang kantoor; bijvoorbeeld scheiding tussen de intake en de uitvoering van opdrachten en review van uit te brengen taxatierapporten en waardeverklaringen).
- Exclusieve relatie tussen notaris, belastingadviseur en medewerker van hypotheekbank.
- Aparte belastingadviseur voor offshore structuur.
- Hoge vergoeding voor belastingadviseur (vast maandbedrag en uurtarief).
- De koper verricht betalingen aan de (fiscaal) adviseur van de verkoper.
- Exclusieve relatie tussen belastingadviseur, notaris en medewerker van hypotheekbank.
- Bedrijfskosten van de onderneming zijn zeer laag.
- Een combinatie van een beperkt inkomen en een grote investering in vastgoed.
- Personen die bij volmacht handelen (dit kan wijzen op het buiten beeld houden van de 'ultimate beneficial owner').
- Doorverwijzen van cliënten naar banken, waar men gebruik maakt van (bank)rekeningen waarvan de eigenaar of begunstigde niet bekend is (zoals anonieme coderekeningen).
- Trustkantoor geeft opdracht terug en/of beëindigt de relatie.
- Aanpassen jaarstukken door accountant t.b.v. het verkrijgen van hypothecaire lening.
- Van de investeerder zijn het vermogen en/of de herkomst daarvan niet of onvoldoende inzichtelijk is.
- Een combinatie van een beperkt inkomen en een grote investering in vastgoed.
- Grote afhankelijkheid overige zakelijke dienstverlener van één klant.
- Iemand met een minderheidsbelang heeft feitelijke leiding over de onderneming, terwijl de overige partijen met een belang opvallend passief zijn en blijven.

- Makelaar/verhuurmakelaar/tussenpersoon die bij meerdere panden betrokken is geweest waar overtredingen zijn geconstateerd

Loveboys: minderjarigen (< 18 jaar)

- Spijbelen
- Haalt ('ineens') slechte cijfers
- Lijkt ineens veel geld te hebben (dure kleding, telefoon etc.)
- Keert zich af van ouders/vrienden
- Grensoverschrijdend gedrag
- Komt alleen nog thuis om te slapen
- Heeft onverklaarbare schulden
- Loopt regelmatig weg, is veel weekenden en nachten weg

Financiering

T.a.v. partijen

- Ontbreken van een overzicht dan wel registratie van aandeelhouders.
- Combinatie van een offshore vennootschap en een geldstroom die uit een land met een bankgeheim komt, waardoor de herkomst van gelden niet of onvoldoende inzichtelijk is.
- Complexe vennootschappelijke constructies.

T.a.v. kredietdossiers

- Onvoldoende CDD.
- Onvolledig kredietdossier en (te) oude stukken (bijvoorbeeld niet aantreffen van originele door de makelaar/taxateur gewaarmerkte taxatierapporten).
- Financiële onderneming gaat akkoord met passeren akte, terwijl het dossier nog incompleet is.
- Kredietdossier is in één keer compleet/ spoed.
- Kredietbeoordelaar controleert niet de door kredietaanvrager opgegeven vermogensbestanddelen, inkomen en/of winst.
- Bij financiering wordt verkoopwaarde van een pand meegenomen, terwijl persoon pand niet op naam heeft staan.
- ABC-constructie (specifiek igv financiële problemengeld- lener: risico dat A voor te lage waarde uit boedel wordt getild, B-C transactie wel tegen normale waarde)
- Hypotheken worden verstrekt aan personen met (financiële) antecedenten (bijvoorbeeld persoon staat opgenomen in BKR als wanbetaler van geldleningen).
- Meerdere malen BKR getoetst in korte tijd.
- BKR-registratie recent beëindigd (check BKR historie)
- Op de loonstrook die wordt overgelegd aan de hypotheekverstrekker staat aangegeven dat het salaris per kas wordt uitbetaald.
- Vormfouten in aangeleverde documenten, zoals loonstrook, werkgeversverklaringen, taxatierapporten en depotnota's.
- Recente datum indiensttreding.
- Afwijkende adressen op verschillende documenten.
- Aanvragers hebben meerdere onderpanden.
- Gefingeerd samenwonen (personen 'bij elkaar geplakt').
- Taxatierapporten zijn niet in fysieke originele vorm opgenomen in het kredietdossier.
- Het aantreffen van meerdere – kort na elkaar – vervaardigde / gedateerde taxatierapporten (kan wijzen op een situationeel gebruik hiervan).
- Aanvraag financiering voor verbouwing terwijl verbouwing al (nagenoeg) gereed is.
- Makelaar/taxateur/notaris/bouwkundig deskundige betrokken bij transactie die niet afkomstig is uit 'de streek'.

T.a.v. de taxatie

- Huren die gezien de locatie / pand opvallend hoog zijn (hiermee kan een te hoge taxatie worden bewerkstelligd en kan worden witgewassen).
- Aanwezigheid van risicovolle ondernemingen en/of bedrijfsomschrijvingen volgens gegevens van de KvK op het adres van het te financieren vastgoed.
- Taxaties voor financieringsaanvraag die de waarde na verbouwing vermelden, zonder dat de financiële onderneming een goede controle laat plaatsvinden op de relatie waardevermeerdering vs. verbouwing en op de nota's.
- Exclusieve relatie tussen de financiële onderneming en de makelaar/taxateur die taxaties verricht ten behoeve van de financiering.
- Opdrachtgever taxatie is (onbekende) derde.
- Het als financiële onderneming slechts gebruik maken van één vaste makelaar/taxateur voor taxaties, zonder dat er een controle plaatsvindt indien de gevraagde kredietfaciliteit onder een bepaald bedrag blijft.

T.a.v. verstrekking hypotheek en bouwdepot

- De bewuste bankmedewerker (accountmanager) is de medewerker met hoogste provisie.
- Het verstrekte bedrag van de hypotheek staat niet in verhouding tot de (legale) inkomsten (salaris, huur of uit onderneming)/ verhouding leeftijd vs. inkomen vs. Beroep
- Meerdere hypotheek gevestigd op één pand in combinatie met herhaaldelijk oversluiten.
- Hypotheken worden in korte tijd meerdere keren substantieel verhoogd.
- Onttrekkingen aan bouwdepots zonder facturen.

Financiering

- (Ver)bouw nota's worden onwaarschijnlijk snel achter elkaar ter uitbetaling ingezonden.
- Offertes ingediend als factuur.
- Werkzaamheden op factuur zijn niet gespecificeerd (indicator valse factuur)/ hoogte van het uit te betalen bedrag staat in geen verhouding tot de uitgevoerde werkzaamheden/geleverde goederen.
- Op factuur wordt niet verwezen naar de termijn van de aannemingsovereenkomst (indicator valse factuur).
- Het onttrekken van gelden inclusief omzetbelasting aan bouwdepots van zakelijke entiteiten.
- Nationale Hypotheek Garantie (NHG) meerdere keren verstrekt tbv dezelfde partij.
- Adres volgens Basisregistratie Personen (BRP) wijkt af van adres volgens NHG.

T.a.v. transport hypotheekakte

- Discrepancie aan begin of eind van transactie tussen degene die het geld fourneert en degene die eigenaar wordt.
- Op het moment van transport wordt de hypotheek doorgehaald. Het lijkt alsof (een deel van) de verkoopopbrengst voor verrekening wordt gebruikt. Dit is echter niet het geval. Op de afrekening van de notaris staat ("aflossing hoofdsom X: nihil").
- Waarborg wordt niet ingeroepen dan wel niet opgeëist (wijst op gelieerde partijen).

T.a.v. gebruik rekeningen

- Omschrijving 'one of our clients' op bankafschriften.

- Contante stortingen middels sealbags op rekeningen waarvoor geen dergelijke overeenkomst is afgesloten met de bank.
- Sealbagstortingen op derdengeldenrekeningen (of andere rekeningen) van advocatenkantoren of notariskantoren (verschoningsgerechtigden).
- Kosten voor contante geldtransporten in opdracht van de bank die worden doorbelast aan de cliënt.
- Grote aflossing hypotheek zonder dat dat onderbouwd kan worden door verkoop vorige woning of andere bronnen.
- Ontvangen aflossingen vanaf derdengeldenrekeningen van advocaten, terwijl geen sprake is van een boedel- scheiding of een faillissement.
- Taxaties voor financieringsaanvraag die de waarde na verbouwing vermelden.

T.a.v. financierende partijen

- Financierende partij is een niet-financiële instelling.
- Financierende partij is een vennootschap waarvan de aandelen aan toonder zijn
- Financiering door verkoper.
- De waarborgsom wordt bijeengebracht door anderen dan de juridische eigenaar of diens hypotheeknemer.
- Financierende partij is een niet-zakelijke partij.
- Financierende partij is onbekend.
- Financierende partij is een vennootschap waarvan de aandelen aan toonder zijn.

T.a.v. financiering zelf

- Hypotheek is niet beschikbaar op datum van levering.
- Financiering, waarbij geen hypotheek wordt gesteld.
- Grote aankoop vindt plaats zonder financiering.
- Koper blijft bedrag schuldig aan verkoper.
- Financiering door verkoper, waarbij ten gunste van verkoper een hypotheek wordt gevestigd.
- Financiering vindt plaats door verkoper tegen een hoge rente.
- Niet betaalde interest, waar geen (juridisch) gevolg aan wordt gegeven (Dit kan duiden op een feitelijke macht en/of eigendomsverhouding die niet strookt met de geregistreerde juridische overeenkomsten).
- Herfinanciering gaat niet naar de verkoper, de verkoper wordt uit andere bron betaald.
- Financiering, waarbij geen hypotheek wordt gesteld.

T.a.v. geldstroom

- Geldstroom komt van een niet-financiële instelling.
- Geldstroom komt vanuit (constructie met) offshore structuur en/of komt uit een land met een bankgeheim, waardoor de herkomst van gelden niet of onvoldoende inzichtelijk is.
- Geldstroom komt van een vennootschap waarvan de aandelen aan toonder zijn.
- Geldstroom is afkomstig van een anonieme bankrekening, zoals een coderekening.
- Uitbetaling aan derde partij die niet betrokken is bij de akte.
- Aflossing niet aan degene die oorspronkelijk heeft gefinancierd.

Financiering

T.a.v. ongebruikelijke geldstroom

- Geldstroom komt van een niet zakelijke partij.
- Geldstroom komt van een vennootschap waarvan de aandelen aan toonder zijn.

- Geldstroom afkomstig van de derdengeldenrekeningen van verschoningsgerechtigden.
- Betalingen provisies, commissies, advieskosten.

Koop/verkoop

T.a.v. partijen

- De koper heeft geen kennis van het te kopen object / de te kopen objecten.
- Koperde partij 'houdt' voor een ander.
- Levering aan verschillende rechtspersonen die door dezelfde persoon worden vertegenwoordigd.
- Gebrek aan transparantie m.b.t. uiteindelijke koper ('nader te noemen meester').
- Transacties tussen gelieerde partijen(privé/B.V., familieleden)
- De personen in de koopovereenkomst komen niet allen terug in de akte van levering.
- Koper in koopakte en in uiteindelijke leveringsakte verschillen, er is een partij bijgekomen (mutaties in partijen gedurende traject).
- Betrokkenheid bij transport van een persoon die niet aanwijsbaar bij de transactie is betrokken.

T.a.v. transport vastgoed

- ABC-transactie met opvallende waardeestijgingen.
- Groot aantal transporten bij de notaris in een zeer kort tijdsbestek.
- Naadloze aansluiting tussen taxatiewaarde en koopsom.

T.a.v. financiële afwikkeling

- Bij verkoop stort de notaris het aankoopbedrag op een door de verkoper opgegeven rekening, niet zijnde zijn eigen rekening of die van de kredietverstrekker (hypotheeknemer).
- Notaris stort aanbetaling van cliënt terug op andere rekening(en).
- Bij het niet doorgaan van de transactie omdat de koper niet afneemt, betaalt de verkoper een afkoopsom aan de partij die zou kopen.

Algemeen

- Een combinatie van een beperkt inkomen en een grote investering in vastgoed.
- Verhouding koopsom t.o.v. huur is heel hoog.
- Verlies op vastgoedtransactie na recente verkrijging.
- Overdracht economisch eigendom.
- Bij ABC-transactie: Verkoop B-C vindt plaats vóór A-B transactie (wijst op orkestreren, gelieerde partijen).
- In het jaar voorafgaand aan de koop/verkoop door de institutionele belegger heeft een ABC-transactie plaats- gevonden waarbij sprake is van onverklaarbare waar- de-stijgingen en/of dubieuze partijen.
- In het jaar na de koop/verkoop door de institutionele belegger heeft een ABC-transactie plaatsgevonden waarbij sprake is van onverklaarbare waardeestijgingen en/of dubieuze partijen.
- 'Handelingsvrijheid' vermogensbeheerder.
- In het jaar voorafgaand aan de koop/verkoop door het pensioenfonds heeft een ABC-transactie plaatsgevonden waarbij sprake is van onverklaarbare waardeestijgingen en/of dubieuze partijen.
- In het jaar na de koop/verkoop door het pensioenfonds heeft een ABC-transactie plaatsgevonden waarbij sprake is van onverklaarbare waardeestijgingen en/of dubieuze partijen.
- Commissiebetalingen/winstdelingen/aanbrengprovisies.
- Provisiebetalingen zonder zichtbare tegenprestatie.

- De verkoper factureert ten tijde van de verkoop aan koper voor advieskosten.
- Beoordeling sociaal netwerk (familielid/relatie). Betrokken partijen melden een verschillende koopsom. (Sommige partijen hebben het over de officiële koopsom, andere partijen bedoelen vermoedelijk de totale koopsom inclusief betalingen buiten de akte om.)

Koop/verkoop

- Transactie wordt met terugwerkende kracht ongedaan gemaakt.
- Grote afwaardering in het jaar van aankoop ten laste van de (fiscale) winst.
- Zeer snel groeiende vastgoedportefeuille.
- Onverklaarbare waardesprongen (in verhouding tot verstreken tijdspanne).
- 'Handelingsvrijheid' vermogensbeheerder.
- De naadloze aansluiting van de taxatiewaarde bij de koopsom op het moment van verkoop.

Gebruik/exploitatie van een pand

Algemeen

- Wijziging van beheerder vastgoed of andere adviseur kan duiden op wijziging van de ubo.
- De als stroman naar voren geschoven koper, bestuurder en/of aandeelhouder heeft geen daadwerkelijke bemoeienis met exploitatie, maar komen alleen met een volmacht naar voren bij de notaris. Voorts heeft bijv. een belasting- adviseur of advocaat een relatief grote rol.
- Criminelen zijn direct (loondienst) of indirect (verrichten van diensten, inzet sociaal netwerk) betrokken bij exploitatie in risicovolle sectoren.
- Commissies voor het aanbrengen van werkzaamheden aan een partij buiten de directe keten.
- Huurder wordt geïnformeerd over het vestigen van een hypotheek op het gehuurde.
- Niet betaalde huren, waar geen (juridisch) gevolg aan wordt gegeven. (Dit kan duiden op een feitelijke macht en/of eigendomsverhouding die niet strookt met de geregistreerde juridische overeenkomsten.)
- Verzekeringsclaims voor brand- en/of opstalverzekeringen, net voordat een grote verbouwing gaat plaatsvinden.
- Contante huurontvangsten (op rekening van persoon die het betreffende pand niet in bezit heeft).
- Grote contante opnamen.
- Betalingen protectiegelden.
- Een vreemde verhouding tussen ontvangen huren en getaxeerde waarde.
- Huren die gezien de locatie / pand opvallend hoog zijn (hiermee kan een te hoge taxatie worden bewerkstelligd en kan worden witgewassen).
- De als stroman naar voren geschoven koper, bestuurder en/ of aandeelhouder heeft geen daadwerkelijke bemoeienis met exploitatie, maar komen alleen met een volmacht naar voren bij de notaris. Voorts heeft bijv. een belastingadviseur of advocaat een relatief grote rol.
- Criminelen zijn direct (loondienst) of indirect (verrichten van diensten, inzet sociaal netwerk) betrokken bij exploitatie in risicovolle sectoren.
- Commissies voor het aanbrengen van werkzaamheden aan een partij buiten de directe keten.
- Huurder wordt geïnformeerd over het vestigen van een hypotheek op het gehuurde.

T.a.v. gebruik pand voor mensenhandel

- Er is geen arbeidsovereenkomst, de arbeidsvoorwaarden zijn slecht gedefinieerd of de arbeidsovereenkomst is opgesteld in een taal die de betreffende persoon niet machtig is.
- Lijkt bang te zijn voor de man/vrouw die hem/haar begeleidt
- De personen beschikken niet zelf over eigen identiteitspapieren
- Slechte huisvesting
- Er is sprake van hoge huren
- Huur wordt inhoudten op salaris
- Ontbreken van huurcontracten
- Vertoont tekenen van angst of lijkt zich ongemakkelijk te voelen, vooral in de aanwezigheid van de supervisor,
- Tijdens gesprek vertelt hij/zij tegenstrijdigheden
- De persoon/personen lijken niet goed te weten waar men is/verblijft
- Iemand anders voert steeds het woord, er lijkt sprake te zijn van controle/gezagsverhouding
- De betalingen vinden onregelmatig en/of vaak te laat plaats.
- Weet niet hoeveel hij/zij verdient.
- Niet vrijelijk kunnen beschikken over (een deel) van de eigen verdiensten, geen eigen bankrekening/ bankpas in bezit)
- Inhoudten boetes, (onduidelijke) kosten werkgever en/of borg
- Verplicht om transport, levensmiddelen en/of andere diensten bij één aanbieder (werkgever) af te nemen
- Illegaal verblijf.
- Moet een buitensporige vergoeding terugbetalen voor werving, vervoer, huisvesting, eten, gereedschap of veiligheidsuitrusting en die vergoeding wordt rechtstreeks ingehouden op zijn/haar loon.
- De terugbetalingsregeling voor voorschotten op het loon is onduidelijk of gemanipuleerd.

Gebruik/exploitatie van een pand

- Personen verklaren lange werkdagen te moeten maken
- Bevindt zich in een situatie waarin hij/zij op meerdere manieren van anderen afhankelijk is (hij/zij is bijvoorbeeld afhankelijk van de werkgever voor onderdak, eten, banen voor familieleden of voor andere behoeften).
- Men beschikt niet over eigen inkomsten
- Schaars gekleed en weinig bezit
- Er zijn diverse telefoons en/of laptops in de woning
- Wonen en slapen op de werkplek
- Er lijkt een vorm van toezicht te zijn (een persoon in de woning aanwezig, of de telefoon gaat zeer regelmatig over tijdens pandcontrole)
- Vertoont tekenen van angst of lijkt zich ongemakkelijk te voelen, vooral in de aanwezigheid van de supervisor,
- Weet niet wat zijn/haar verblijfplaats of adres is.
- Heeft regelmatig klanten, maar geen geld om bijv. huur te betalen
- Wordt bij ziekte of zwangerschap gedwongen te werken
- Huren de woning niet zelf
- Alle vragen worden door de begeleidende persoon beantwoordt in plaats van door het potentiële slachtoffer.
- De opmerkingen van het potentiële slachtoffer vertonen geen samenhang of komen ingestudeerd over, door middel van indoctrinatie.

Bijlage 2: analyses van de ruimte voor binnengemeentelijke gegevensuitwisseling in relevante wet- en regelgeving

A. APV/Openbare orde-bevoegdheden

Doelstelling

Zowel in de Gemeentewet als in de meeste APV's zijn bevoegdheden voor de burgemeester opgenomen op het terrein van de openbare orde en bevordering van de leefbaarheid. De burgemeester is in artikel 172 lid 1 Gemeentewet belast met de handhaving van de openbare orde, en op grond van artikel 172 lid 2 Gemeentewet bevoegd overtredingen van wettelijke voorschriften die betrekking hebben op de openbare orde te beletten of te beëindigen. Voorbeelden van meer concrete taken en bevoegdheden zijn artikel 172a Gemeentewet (gebiedsverbod), toezicht houden op openbare samenkomsten en verzamelingen en op voor het publiek openstaande gebouwen (artikel 174 Gemeentewet), diverse sluitingsbevoegdheden (zoals artikel 174a Gemeentewet, artikel 13b Opiumwet, en sluitingsbevoegdheden in APV's) en toezicht en regulering van activiteiten als de exploitatie van seksinrichtingen en evenementen (zie daarvoor ook APV-bepalingen).

De doelstellingen van deze taken en bevoegdheden zijn gelegen op het terrein van de handhaving van de openbare orde, waaronder het voorkomen van (veiligheids)risico's, tegengaan van overlast en bevorderen van de leefbaarheid.

Wettelijke grondslag²⁰

De Gemeentewet en APV's kennen geen specifieke bepalingen die de burgemeester de bevoegdheid geven bepaalde persoonsgegevens te verwerken. Daarvoor moet worden teruggevallen op de algemene grondslagen voor een rechtmatige gegevensverwerking in de AVG, in het bijzonder de grond dat de verwerking noodzakelijk is voor de vervulling van een taak in het kader van een taak van algemeen belang of de uitoefening van het openbaar gezag dat aan de burgemeester is opgedragen.

In het kader van de vergunningverlening – bijvoorbeeld een evenementenvergunning of een vergunning voor de exploitatie van een seksbedrijf – is de burgemeester dus in ieder geval bevoegd de gegevens te verwerken die nodig zijn om de vergunningaanvraag te kunnen beoordelen, waaronder de gegevens die de aanvragers hebben verstrekt.

Voor zover in het kader van de vergunningverlening een Bibob-toets wordt uitgevoerd, wordt verwezen naar de juridische analyse over de Wet Bibob.

²⁰ Veelal in verbinding met artikel 6 onder c en/of e AVG.

In het kader van het uitoefenen van toezicht geldt in algemene zin voor toezichthouders dat zij op grond van de Awb inlichtingen kunnen vorderen (artikel 5:16 Awb) en zakelijke gegevens en bescheiden kunnen opvragen (artikel 5:17 Awb). Op grond van deze bepalingen kunnen ook kopieën van stukken en bescheiden worden gevorderd. In beginsel kunnen inlichtingen van een ieder worden gevorderd, mits dat in lijn is met het evenredigheidsbeginsel (artikel 5:13 Awb). Het uitgangspunt is dat de toezichthouder zijn bevoegdheden niet mag uitoefenen als dat niet noodzakelijk is en dat hij zijn bevoegdheden op een voor de burger zo min mogelijk belastende wijze uitoefent. Deze gegevens mogen ook worden verwerkt voor zover dat voor de uitoefening van het toezicht nodig is.

In het kader van de handhaving van de openbare orde geldt dat evenzeer.

Voor zover de burgemeester bij de uitvoering van zijn taken gebruik maakt van persoonsgegevens die in bestuurlijke rapportages van de politie zijn opgenomen, wordt verwezen naar de juridische analyse over de Wet politiegegevens.

Geheimhoudingsplicht

De Gemeentewet en APV's bevatten geen specifieke geheimhoudingsplicht.

Doelbinding

Het doelbindingsbeginsel vindt zijn uitwerking in artikel 5 lid 1 sub b en 6 lid 4 AVG. De openbare ordebevoegdheden van de burgemeester in de Gemeentewet en APV's bieden de mogelijkheid om gegevens te verwerken met als doel om een goede invulling aan die bevoegdheden te kunnen geven, en kort gezegd de openbare orde te handhaven, risico's in dat verband tegen te gaan, overlast te bestrijden en de leefbaarheid te bevorderen.

Vraag is vervolgens of deze gegevens ook kunnen worden geraadpleegd als ter bestrijding van ondermijning de inzet van gemeentelijke bevoegdheden wordt overwogen. Voor zover het daarbij ook om de mogelijke inzet van bevoegdheden van de burgemeester gaat op het terrein van openbare orde, bestrijden van overlast en bevordering van leefbaarheid – wat bij de bestrijding van ondermijning vaak het geval zal zijn – zal al snel aan het doelbindingsbeginsel zijn voldaan. Als de mogelijke inzet van eventuele andere bevoegdheden wordt onderzocht, zal de vraag of aan het doelbindingsvereiste wordt voldaan, scherp moeten worden beoordeeld en van geval tot geval moeten worden bezien.

Conclusie

- In de Gemeentewet en APV's zijn taken en bevoegdheden van de burgemeester op het terrein van openbare orde, bestrijden van overlast, en bevorderen van de leefbaarheid opgenomen.
- Die regelingen kennen geen specifieke bepalingen omtrent geheimhouding of doelbinding.
- De ratio achter de bestrijding van ondermijning ligt op het terrein van openbare orde, bestrijden van overlast en bevorderen van de leefbaarheid.
- Als de inzet van bevoegdheden op die terreinen wordt overwogen, kunnen in aangewezen gevallen gegevens die zijn verkregen bij de uitoefening van burgemeestersbevoegdheden worden geraadpleegd ter bestrijding van ondermijning.

B. Wet politiegegevens

Doelstelling

De Wet politiegegevens (hierna: Wpg) regelt de verwerking van politiegegevens. Politiegegevens zijn persoonsgegevens die worden verwerkt in het kader van de uitoefening van de politietaak (artikel 1, sub a, Wpg). De Wpg voorziet naast bepalingen over de verwerking van gegevens binnen de politie, ook in bepalingen over de verstrekking van politiegegevens aan anderen buiten de politie, waaronder aan gezagdragers.²¹ Onder gezagdragers vallen ingevolge artikel 16, lid 1, sub b, Wpg ook burgemeesters.

Wettelijke grondslag

Artikel 16, lid 1, sub b, onder 1 en 2 Wpg bepaalt dat de verwerkingsverantwoordelijke²² politiegegevens aan burgemeesters verstrekt voor zover zij deze behoeven (i) in verband met hun gezag en zeggenschap over de politie, of (ii) in het kader van de handhaving van de openbare orde.

De taak van de burgemeester met betrekking tot het gezag en zeggenschap over de politie volgt uit artikel 11 Politiewet 2012. Die bepaling luidt:

"1 Indien de politie in een gemeente optreedt ter handhaving van de openbare orde en ter uitvoering van de hulpverleningstaak, staat zij onder gezag van de burgemeester.

2 De burgemeester kan de betrokken ambtenaren van politie de nodige aanwijzingen geven voor de vervulling van de in het eerste lid bedoelde taken."

In het kader van het gezag dat en de zeggenschap die de burgemeester binnen de gemeente over de politie heeft, voert de burgemeester onder meer overleg met de officier van justitie, het hoofd en zo nodig de politiefchef van de regionale politie-eenheid over de taakuitvoering van de politie en het beleid ten aanzien van de taakuitvoering (het zogenoemde driehoeksoverleg). Zie daarover artikel 13 Politiewet 2012:

"1 De burgemeester en de officier van justitie overleggen regelmatig tezamen met het hoofd van het territoriale onderdeel van de regionale eenheid binnen welker grondgebied de gemeente geheel of ten dele valt, en zo nodig met de

²¹ *Kamerstukken II 2005-06, 30327, nr. 3, p. 5.*

²² Dat is bij de politie de korpschef, bij de rijksrecherche het College van procureurs-generaal, bij de Koninklijke marechaussee de Minister van Defensie en bij een gemeenschappelijke verwerking de verwerkingsverantwoordelijke die is belast met de feitelijke zorg voor de verwerking en het treffen van de maatregelen ten behoeve van onder meer de juistheid, volledigheid en de beveiliging van de gegevens (artikel 1, sub f, Wpg).

politiechef van een regionale eenheid, over de taakuitvoering van de politie en over het beleid ten aanzien van de taakuitvoering (driehoeksoverleg).

2 In het driehoeksoverleg worden door de burgemeester en de officier van justitie afspraken gemaakt over de inzet van de politie ten behoeve van de handhaving van de openbare orde en de hulpverlening, onderscheidenlijk ten behoeve van de strafrechtelijke handhaving van de rechtsorde en de taken ten dienste van de justitie. De afspraken worden mede gemaakt op basis van de doelen, bedoeld in artikel 38b, eerste lid.

3 Op verzoek van de burgemeester vindt het driehoeksoverleg plaats op gemeentelijk niveau.

4 In het driehoeksoverleg worden door de burgemeester en de officier van justitie afspraken gemaakt over lokale prioriteiten en criminaliteitsbestrijding.”

De taak van de burgemeester met betrekking tot de handhaving van de openbare orde volgt uit artikel 172 Gemeentewet:

"1 De burgemeester is belast met de handhaving van de openbare orde.

2 De burgemeester is bevoegd overtredingen van wettelijke voorschriften die betrekking hebben op de openbare orde, te beletten of te beëindigen. Hij bedient zich daarbij van de onder zijn gezag staande politie.

3 De burgemeester is bevoegd bij verstoring van de openbare orde of bij ernstige vrees voor het ontstaan daarvan, de bevelen te geven die noodzakelijk te achten zijn voor de handhaving van de openbare orde.

4 De commissaris van de Koning geeft, indien een ordeverstoring van meer dan plaatselijke betekenis dan wel ernstige vrees voor het ontstaan van zodanige ordeverstoring zulks noodzakelijk maakt, de burgemeesters in de provincie zoveel mogelijk na overleg met hen, de nodige aanwijzingen met betrekking tot het door hen ter handhaving van de openbare orde te voeren beleid. De aanwijzingen worden zo enigszins mogelijk schriftelijk gegeven.”

Daarnaast bevatten artikel 19 en 20 Wpg grondslagen voor de verwerkingsverantwoordelijke²³ om, in overeenstemming met het bevoegd gezag,²⁴ te beslissen incidenteel politiegegevens te verstrekken aan personen of instanties respectievelijk structureel politiegegevens te verstrekken ten behoeve van een samenwerkingsverband van de bevoegde autoriteiten met personen of instanties. De verstrekking moet daarbij steeds noodzakelijk zijn met oog op een zwaarwegend algemeen belang en bedoeld zijn voor de volgende doeleinden:

a. het voorkomen en opsporen van strafbare feiten;

²³ Zie voetnoot 21.

²⁴ Als bedoeld in de artikelen 11, 12 en 14 van de Politiewet 2012.

- b. het handhaven van de openbare orde;
- c. het verlenen van hulp aan hen die deze behoeven;
- d. het uitoefenen van toezicht op het naleven van regelgeving.

Een bestuursorgaan van de gemeente zou een dergelijke persoon of instantie kunnen zijn.²⁵

Geheimhoudingsplicht

Artikel 7 Wpg bevat een geheimhoudingsplicht voor politiegegevens. Deze geldt zowel voor degenen binnen de politie aan wie politiegegevens ter beschikking zijn gesteld (artikel 7 lid 1 Wpg) als voor personen buiten de politie aan wie politiegegevens zijn verstrekt (artikel 7 lid 2 Wpg).

In artikel 7 lid 1 Wpg is voor de ambtenaar van de politie bepaald dat de geheimhoudingsplicht niet geldt voor zover een bij of krachtens de wet gegeven voorschrift tot verstrekking verplicht, de bepalingen van paragraaf 3 verstrekking toelaten of de politietaak in bijzondere gevallen tot verstrekking noodzaakt. De mogelijkheid om politiegegevens te verstrekken aan burgemeesters (artikel 16, lid 1, sub b, onder 1 en 2, de Wpg) is opgenomen in paragraaf 3 van de Wpg en is daarmee een toelaatbare doorbreking van de geheimhoudingsplicht.

De burgemeester is vervolgens op grond van artikel 7 lid 2 Wpg verplicht tot geheimhouding, behoudens voor zover een bij of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt.

Doelbinding

In artikel 3 Wpg is het vereiste van doelbinding opgenomen. Uit het vierde lid volgt dat politiegegevens voor een ander doel dan de politietaak kunnen worden verwerkt door personen of instanties die bij of krachtens de wet met het oog op een zwaarwegend algemeen belang of wetgeving van de Europese Unie zijn aangewezen.

Conclusie

- Burgemeesters krijgen politiegegevens verstrekt voor zover zij deze behoeven (i) in verband met hun gezag en zeggenschap over de politie of (ii) in het kader van de handhaving van de openbare orde. Ook kunnen bestuursorganen van de gemeente bijvoorbeeld incidenteel politiegegevens verstrekt krijgen dan wel structureel ten behoeve van een samenwerkingsverband.

²⁵ Hiervoor is geen uitputtend overzicht gegeven van de mogelijkheden om politiegegevens aan (bestuursorganen binnen) gemeenten te verstrekken op basis van de Wet politiegegevens (en daarop gebaseerde regelgeving, zoals het Besluit politiegegevens, het Besluit politiegegevens buitengewoon opsporingsambtenaren en het Besluit politiegegevens bijzondere opsporingsdiensten). Zo kan bijvoorbeeld ook nog worden gewezen op artikel 18 Wpg jo. artikel 4:3 Besluit politiegegevens.

- Gelet op (de expliciete doelbindingsbepaling en) de strikte geheimhoudingsplicht in de Wpg zien wij geen ruimte voor burgemeesters om politiegegevens binnen de gemeente verder te verwerken voor andere doeleinden. Dat betekent ons inziens dat niet bij ieder signaal een hit/no hit-vraag kan worden gesteld aan de burgemeester met betrekking tot de politiegegevens die hij heeft ontvangen.
- Wel kan een signaal op zichzelf aanleiding vormen voor de burgemeester om informatie op te vragen bij de politie in het kader van zijn openbare orde-taak of om de politie op te dragen op te treden ten aanzien van bepaalde verstoringen.
- Verder staat de geheimhoudingsplicht van de Wpg niet in de weg aan het delen van *het gegeven dat de burgemeester een besluit heeft genomen* op basis van politiegegevens binnen de gemeente. Daarvoor achten wij relevant dat het gegeven dat een bepaald besluit is genomen op zichzelf geen politiegegeven is, nu dat gegeven niet wordt verwerkt in het kader van de uitvoering van de politietaak (vgl. artikel 1, sub a, Wpg).

C. Drank- en Horecawet

Doelstelling

Het doel van de Drank- en Horecawet (hierna: DHW) is gezondheidsschade door alcohol bij (met name) jongeren voorkomen en verstoring van de openbare orde door alcoholmisbruik terug te dringen. De DHW regelt de bevoegdheid om horecavergunningen te verlenen en hierop toezicht te houden. De gemeente is verantwoordelijk om het toezicht op en de handhaving van deze wet te organiseren. Bij gemeentelijke verordening kunnen voorts nadere regels worden gesteld over het verstrekken van alcoholhoudende dranken (artikel 25a e.v. DHW).

Wettelijke grondslag²⁶

Verstrekking van gegevens aan de burgemeester in het kader van vergunningverlening

De burgemeester is bevoegd kennis te nemen van de informatie die een aanvrager van een horecavergunning verstrekt op grond van artikel 3 DHW jo. artikel 26 DHW jo. Regeling aanvraaggegevens en formulieren DHW.

- Zie voor de inhoud van het aanvraagformulier artikel 26 DHW jo. Regeling aanvraaggegevens en formulieren DHW.
- In de vergunning zelf worden diverse gegevens opgenomen (artikel 29, eerste lid, DHW).²⁷
- Ook vermeldt het aanhangsel bij de vergunning de leidinggevende(n) (artikel 29, tweede lid, DHW).

De burgemeester kan vervolgens een horecavergunning verlenen op grond van artikel 3 DHW. Een horecavergunning wordt geweigerd indien de leidinggevende(n) in enig opzicht van slecht leefgedrag is/zijn (artikel 27 lid 1 sub a DHW jo. artikel 8 lid 1 sub b DHW).

Wat slecht leefgedrag precies inhoudt, wordt nader uitgewerkt in het Besluit eisen zedelijk gedrag Drank- en Horecawet 1999. Het gaat hier onder andere om:

- Plaatsing in een psychiatrisch ziekenhuis;
- Veroordeling tot een gevangenisstraf wegens een misdrijf binnen de afgelopen vijf jaar;
- Veroordeling tot een geldboete van 500 euro of meer binnen de afgelopen vijf jaar;

²⁶ Veelal in verbinding met artikel 6 onder c en/of e AVG.

²⁷ In de vergunning worden vermeld (i) de vergunninghouders, (ii) tot welke bedrijfsuitoefening de vergunning strekt, (iii) de plaats waar de inrichting zich bevindt (iv) de situering en de oppervlakten van de horeca- en slijterijlokaliteiten en terrassen en (v) de voorschriften of beperkingen welke aan de vergunning zijn verbonden.

- Leiderschap over een inrichting waarvan de vergunning is ingetrokken of die tenminste een maand is gesloten binnen de afgelopen vijf jaar.

In het kader van de vergunningverlening is de burgemeester bevoegd de gegevens te verwerken die nodig zijn om te kunnen beoordelen of de leidinggevende(n) in enig opzicht van slecht leefgedrag is/zijn. Bij deze beoordeling kunnen dus bijvoorbeeld strafrechtelijke gegevens worden verwerkt.

Verder kan zowel de burgemeester als de DHW-toezichthouder een register raadplegen dat wordt bijgehouden door de minister van VWS en waarin bewijsstukken zijn opgenomen over de kennis en het inzicht van de leidinggevende in sociale hygiëne. Dat is mogelijk op grond van artikel 8 lid 5 DHW. Dit register bevat de volgende bewijsstukken:

- een verklaring afgegeven door de examencommissie van de Stichting Vakbekwaamheid Horeca 2.0; en
- een verklaring van vakbekwaamheid.²⁸

Raadpleging van het register door de burgemeester is toegestaan in het kader van:

- het verlenen van een horecavergunning;
- het verlenen van een ontheffing;
- het beoordelen van een melding van het instellen van een nieuwe leidinggevende.

Raadpleging van het register door de DHW-toezichthouders is mogelijk zonder nadere voorwaarden (artikel 8 lid 5 sub b DHW).²⁹

Ook geldt een meldingsplicht van een vergunninghoudende inrichting aan de burgemeester indien zich voor de vergunning relevante wijzigingen voordoen (artikel 30 DHW).

De burgemeester is bevoegd meldingen te ontvangen van een vergunninghoudende instelling over wijzigingen ten aanzien van de leidinggevende op grond van artikel 30a DHW.

De burgemeester kan toepassing geven aan de Wet Bibob en het Landelijk Bureau Bibob om een advies vragen in het kader van de vergunningverlening (artikel 27 lid 3 en 4 DHW), van een verzoek tot het bijschrijven van een leidinggevende (artikel 30a lid 5 en lid 6 DHW) en om een reeds verleende vergunning intrekken (artikel 31 lid 3 sub a DHW).

²⁸ Artikel 1 Regeling bewijsstukken sociale hygiëne Drank- en Horecawet 2015.

²⁹ Het register is overigens voor een ieder toegankelijk via www.svh.nl.

Verwerking van gegevens in het kader van toezicht en handhaving

De DHW kent geen specifieke bepalingen die DHW-toezichthouders de bevoegdheid verschaffen bepaalde persoonsgegevens te verwerken, afgezien van de bevoegdheid van zowel de burgemeester als de DHW-toezichthouders het register te raadplegen dat wordt bijgehouden door de minister van VWS en waarin bewijsstukken zijn opgenomen over de kennis en het inzicht van de leidinggevende in sociale hygiëne (artikel 8 lid 5 sub b DHW).

In algemene zin geldt voor toezichthouders dat zij op grond van de Awb inlichtingen kunnen vorderen (artikel 5:16 Awb) en zakelijke gegevens en bescheiden kunnen opvragen (artikel 5:17 Awb). Op grond van deze bepalingen kunnen ook kopieën van stukken en bescheiden worden gevorderd. In beginsel kunnen inlichtingen van een ieder worden gevorderd, mits dat in lijn is met het evenredigheidsbeginsel (artikel 5:13 Awb). Het uitgangspunt is dat de DHW-toezichthouder zijn bevoegdheden niet mag uitoefenen als dat niet noodzakelijk is en dat hij zijn bevoegdheden op een voor de burger zo min mogelijk belastende wijze uitoefent. Ook ligt het in de rede dat de DHW-toezichthouder zijn vordering motiveert. In beginsel is een ieder verplicht tot medewerking aan dergelijke vorderingen (artikel 5:20 Awb).

Geheimhoudingsplicht

De DHW bevat geen specifieke geheimhoudingsplicht.

Doelbinding

Het doelbindingsbeginsel vindt zijn uitwerking in artikel 5 lid 1 sub b en 6 lid 4 AVG. De DHW biedt mogelijkheden gegevens te verwerken met als doel het al dan niet verlenen van horecavergunningen en – breder – de regulering van alcoholgebruik.

Vraag is vervolgens of DHW-gegevens ook kunnen worden geraadpleegd ter bestrijding van ondermijning. Ons lijkt dat op voorhand niet uitgesloten, omdat zowel de regulering van alcoholgebruik als de bestrijding van ondermijning verband houden met de leefbaarheid en goede zeden binnen een gemeente. Ook wordt in de memorie van toelichting op de DHW het tegengaan van criminaliteit als een van de doelstellingen van de Drank- en Horecawetgeving genoemd.³⁰ Gelet op deze tot op zekere hoogte vergelijkbare doelen kunnen wij ons voorstellen dat DHW-gegevens in voorkomende gevallen kunnen worden geraadpleegd als ter bestrijding van ondermijning de inzet van gemeentelijke bevoegdheden wordt overwogen die soortgelijke doelen dienen (bevoegdheden van de burgemeester op het terrein van openbare orde, bestrijden van overlast en bevordering van leefbaarheid). Eventuele

³⁰ Kamerstukken II 1997-1998, 25 969, nr. 3, p. 4-5.

stafrechtelijke gegevens zullen alleen kunnen worden bekeken als de betrokken medewerkers van de gemeente daarvoor een expliciete grondslag hebben.

Conclusie

- De DHW regelt de bevoegdheid om horecavergunningen te verlenen en daarop toezicht te houden;
- De DHW kent geen specifieke bepalingen omtrent geheimhouding of doelbinding;
- De ratio achter de bestrijding van ondermijning en achter de drank- en horecawetgeving ligt in zekere zin in elkaars verlengde, nu in beide gevallen wordt beoogd de leefbaarheid en goede zeden in een gemeente te bevorderen;
- Gelet daarop kunnen in aangewezen gevallen DHW-gegevens worden geraadpleegd ter bestrijding van ondermijning.

D. Huisvestingswet

Doelstelling

Doelstelling van de Huisvestingswet 2014 is om gemeenten een instrumentarium te bieden om in te grijpen in de woonruimteverdeling en de samenstelling van de woonruimtevoorraad voor het bestrijden van onevenwichtige en onrechtvaardige effecten van schaarste aan woonruimte³¹. Als er schaarste is, kunnen maatregelen om in te grijpen op de samenstelling van de woonruimtevoorraad ook de bevordering van leefbaarheid als motief hebben³².

De Huisvestingswet 2014 biedt gemeenten een grondslag voor het vaststellen van een huisvestingsverordening. Daarin kunnen regels over woonruimteverdeling worden opgenomen; denk aan regels over urgentie, en regels over het verplicht stellen van een huisvestingsvergunning. Daarnaast kunnen daar regels over de samenstelling van de woonruimtevoorraad worden opgenomen. Denk bijvoorbeeld aan vergunningplichten voor onttrekking aan de bestemming tot bewoning, voor het samenvoegen van woonruimte, voor het omzetten van zelfstandige in onzelfstandige woonruimte, voor het verbouwen van één woonruimte tot twee of meer woonruimten en voor het splitsen van gebouwen (artikel 21 en 22 Huisvestingswet 2014).

De doelstelling van de gemeentelijke huisverordening is dus eveneens ingrijpen in de woonruimteverdeling en/of ingrijpen in de samenstelling van de woonruimtevoorraad om onevenwichtige en onrechtvaardige effecten van schaarste te bestrijden, en leefbaarheid te bevorderen.

Wettelijke grondslag

Ten behoeve van deze doelstellingen en de daarmee verbonden gemeentelijke taken zullen gemeenten onder meer de volgende soorten gegevens verwerken:

- gegevens die woningzoekenden aan de gemeente verstrekken als zij een huisvestingsvergunning aanvragen, zoals: naam, adres, samenstelling van het huishouden en een verklaring over de hoogte en bron van het inkomen;
- gegevens die eigenaren aan de gemeente verstrekken als zij een onttrekkingsvergunning, een vergunning voor kamerbewoning, een vergunning voor woningvorming of een splitsingsvergunning aanvragen, zoals: naam, adres, aantal personen dat van de om te zetten woonruimte gebruik zal maken (o.a. bij kamerbewoning), namen eventuele huidige bewoners;
- gegevens die de gemeente verkrijgt als zij toezicht houdt op de naleving van de Huisvestingswet 2014 en de huisvestingsverordening, zoals: gegevens

³¹ Kamerstukken II, 2009/2010, 32 271, nr. 3, blz. 1.

³² ABRvS 19 juni 2013, ECLI:NL:RVS:2013:CA3620; Kamerstukken I, 2013/2014, 32 271, nr. C, blz. 7.

over illegale kamerbewoning, splitsing of woningvorming (artikel 32 e.v. Huisvestingswet 2014).

Vooraf die laatste soort gegevens lijken relevant in het kader van binnengemeentelijke gegevensuitwisseling ter bestrijding van ondermijning. In algemene zin geldt daarvoor dat toezichthouders op grond van de Awb inlichtingen kunnen vorderen (artikel 5:16 Awb) en zakelijke gegevens en bescheiden kunnen opvragen (artikel 5:17 Awb). Op grond van deze bepalingen kunnen ook kopieën van stukken en bescheiden worden gevorderd. In beginsel kunnen inlichtingen van een ieder worden gevorderd, mits dat in lijn is met het evenredigheidsbeginsel (artikel 5:13 Awb). Het uitgangspunt is dat de toezichthouder zijn bevoegdheden niet mag uitoefenen als dat niet noodzakelijk is en dat hij zijn bevoegdheden op een voor de burger zo min mogelijk belastende wijze uitoefent. Ook ligt het in de rede dat de toezichthouder zijn vordering motiveert. In beginsel is een ieder verplicht tot medewerking aan dergelijke vorderingen (artikel 5:20 Awb).

In de Huisvestingswet 2014 is geen specifieke regeling voor gegevensverwerking of gegevensuitwisseling opgenomen.

Geheimhoudingsplicht en doelbinding

De Huisvestingswet 2014 bevat ook geen specifieke geheimhoudingsplicht. Het doelbindingsbeginsel van artikel 5 lid 1 aanhef en onder b en 6 lid 4 AVG is vanzelfsprekend van toepassing.

De vergunningplicht voor kamerbewoning, splitsing en woningvorming wordt gehandhaafd om de gewenste samenstelling van de woonruimtevoorraad te bevorderen, maar kan door gemeenten ook worden ingezet om, als er schaarste is, de leefbaarheid te bevorderen. Zo kunnen illegale kamerbewoning of illegale splitsing van woonruimte tot overlast en verloedering leiden, met negatieve effecten op de leefbaarheid tot gevolg. Dat geldt ook voor onttrekking van woonruimte ten behoeve van bijvoorbeeld hennepwekerijen. Handhaving van de huisvestingsverordening kan in dit soort gevallen nauw samenhangen met de bestrijding van ondermijning. Als de inzet van andere bevoegdheden wordt overwogen die doelen hebben die dicht tegen de doelstellingen van de gemeentelijke huisvestingsverordening aan liggen, zal uitwisseling van die gegevens mogelijk snel gerechtvaardigd zijn. Daarbij zou ook een rol kunnen spelen of op basis van ervaring kan worden aangenomen dat bijvoorbeeld illegale kamerverhuur vaak samengaat met en dus een risico vormt op gebreken in de brandveiligheid. Daarbij kan gedacht worden aan gebruik van gegevens ten behoeve van bevoegdheden in het kader van bouw- en woningtoezicht.

Er zal in het concrete geval moeten worden afgewogen of de bevoegdheden die men overweegt in te zetten, dicht genoeg tegen de doelstellingen van de

huisvestingsverordening aanliggen om de uitwisseling en verder gebruik van persoonsgegevens te rechtvaardigen.

Conclusie

- Doelstellingen van de Huisvestingswet 2014 zijn: bestrijding van nadelige effecten van schaarste aan woonruimtevoorraad door in te grijpen in de verdeling van woonruimte en de samenstelling van de woonruimtevoorraad, en, als er schaarste is, door ingrijpen in de samenstelling van de woonruimtevoorraad de leefbaarheid te bevorderen.
- De Huisvestingswet 2014 kent geen specifieke geheimhoudingsbepaling.
- Gegevens mogen worden verwerkt voor zover aan het vereiste van doelbinding wordt voldaan.
- De regisseur ondermijning zal in het concrete geval moeten afwegen of de bevoegdheden die de gemeente wil inzetten, dicht genoeg tegen de doelstellingen van de huisvestingsverordening aanliggen om de uitwisseling en verder gebruik van persoonsgegevens te rechtvaardigen.
- Denk daarbij bijvoorbeeld aan bouw- en woningtoezicht.

E. Wet bijzondere maatregelen grootstedelijke problematiek

Doelstelling

De Wet bijzondere maatregelen grootstedelijke problematiek (Wbmgp) heeft tot doel de leefbaarheid in bepaalde buurten of wijken te vergroten door middel van selectieve woningtoewijzing. De gemeenteraad kan hiervoor wooncomplexen, straten of gebieden laten aanwijzen door de minister op basis van bepaalde selectiecriteria te weten: (i) aard van het inkomen, (ii) sociaal-economische kenmerken en (iii) overlast en crimineel gedrag.

Wettelijke grondslag

Algemene verwerkingsgrondslagen³³

Op grond van artikel 5 lid 3 juncto artikel 10b lid 9 Wbmgp is het Besluit verwerking persoonsgegevens bij selectieve woningtoewijzing ter beperking van overlastgevend en crimineel gedrag (het Besluit) van toepassing indien de burgemeester of het college persoonsgegevens verwerkt in het kader van het afgeven van een woonverklaring of in het kader van een besluit op aanvraag van een huisvestingsvergunning voor een complex, straat of gebied. Het Besluit bevat zowel verwerkingsgrondslagen voor het college als voor de burgemeester. De volgende grondslagen kunnen worden onderscheiden:

- Verwerking van persoonsgegevens door het college in een bestand in het kader van de aanvraag van een huisvestingsvergunning door een woningzoekende waarvoor een verklaring omtrent gedrag is vereist (artikel 3 lid 1 Besluit).

Indien in de huisvestingsverordening is bepaald dat een verklaring omtrent gedrag is vereist voor het verlenen van een huisvestingsvergunning in het aangewezen gebied, dan verwerkt het college de volgende persoonsgegevens in een bestand:

- a. de datum van de aanvraag;
- b. de naam, de geboortedatum, de geboorteplaats en het adres, bedoeld in artikel 1.1, onderdeel q, van de Wet basisregistratie personen, van de woningzoekende;
- c. het adres van de woonruimte waarvoor de huisvestingsvergunning wordt aangevraagd;

³³ Het is mogelijk dat de bevoegdheden van het college op basis van artikel 19 Huisvestingswet 2014 zijn gemandateerd aan eigenaren of beheerders van woonruimte. Op basis van artikel 10 Besluit verwerking persoonsgegevens bij selectieve woningtoewijzing ter beperking van overlastgevend en crimineel gedrag hebben zij dan dezelfde bevoegdheden (in het kader van de Wbmgp) als het college.

- d. de bereidverklaring;
- e. de verklaring omtrent het gedrag van de woningzoekende.

- Verwerking van persoonsgegevens van de woningzoekende door het college in een bestand ten behoeve van de beoordeling van een aanvraag waarvoor een woonverklaring is vereist (artikel 3 lid 2 Besluit).

Indien in de huisvestingsverordening is bepaald dat bij een aanvraag van een huisvestingsvergunning een onderzoek op basis van politiegegevens is vereist, dan verwerkt het college de volgende gegevens in een bestand:

- a. de datum van de aanvraag;
- b. de naam, de geboortedatum, de geboorteplaats en het adres, bedoeld in artikel 1.1, onderdeel q, van de Wet basisregistratie personen, van de woningzoekende;
- c. het adres van de woonruimte waarvoor de huisvestingsvergunning wordt aangevraagd;
- d. de bereidverklaring.

- Komt de woningzoekende op basis van de criteria die zijn opgenomen in de huisvestingsverordening en die geen betrekking hebben op gedragingen uit de politiegegevens, bedoeld in artikel 10a lid 2 Wbmgp in aanmerking voor een huisvestingsvergunning, dan stelt het college de burgemeester in kennis van de aanvraag en verstrekt het college de gegevens als bedoeld in artikel 3 lid 2 sub a-c van het Besluit aan de burgemeester (artikel 4 lid 2 Besluit).
- Op grond van artikel 5 lid 5 Wbmgp houdt het college voor de evaluatie van de maatregel die op grond van de aanwijzing in een complex, straat of gebied is toegepast noodzakelijke gegevens bij. Welke gegevens dit betreffen is geregeld in artikel 9 van het Besluit. In artikel 10b lid 9 Wbmgp juncto artikel 13 lid 1, onder a, Besluit is bepaald dat het college ervoor zorgdraagt dat de persoonsgegevens in het bestand als bedoeld in artikel 3 van het Besluit worden bewaard voor de evaluatie van de maatregel.
- Verwerking van de beslissing/woonverklaring van de burgemeester in het bestand door het college (artikel 9 Besluit).

Het college is bevoegd tot het verwerken in een bestand van:

- de verlening of weigering van de huisvestingsvergunning door de burgemeester;
- de woonverklaring;
- de persoonsgegevens verkregen van eigenaren of beheerders van woonruimte.

- Als de burgemeester in kennis is gesteld van de aanvraag van een huisvestingsvergunning, dan moet hij volgende persoonsgegevens in een bestand verwerken (artikel 7 Besluit):
 - de persoonsgegevens verkregen van het college;
 - de politiegegevens ontvangen van de politiechef;
 - het hoorverslag (indien de woningzoekende op grond van artikel 10b lid 6 Wbmgp is gehoord);
 - de woonverklaring;
 - een afschrift van de mededeling die de burgemeester heeft verstrekt aan de aanvrager van de huisvestingsvergunning.
- Het bijhouden van een bestand van namen door de burgemeester van personen die onder zijn verantwoordelijkheid werkzaam zijn met betrekking tot de taken als bedoeld in artikel 5 lid 1, 6, 7, 11 en 13 lid 2 van het Besluit (artikel 8 lid 1 Besluit).

Verstrekking van gegevens aan de burgemeester

De beoordeling van de vergunningaanvraag is in handen van de burgemeester. Met het oog daarop zijn voor de burgermeester verschillende verstrekingsgrondslagen opgenomen in het Besluit:

- Verstrekking van de gegevens van de woningzoekende door het college aan de burgemeester (artikel 4 lid 2 Besluit).³⁴
- Verstrekking van een overzicht van de politiegegevens door de politiechef van de lokale eenheid van de betreffende gemeente aan de burgemeester ten behoeve van de beoordeling van de aanvraag van een huisvestingsvergunning in een aangewezen gebied waarvoor een woonverklaring is vereist (artikel 10b lid 1 Wbmgp jo. artikel 5 Besluit).
 - Er mag slechts een overzicht van de relevante politiegegevens van de vier jaren vóór het tijdstip van de aanvraag van de huisvestingsvergunning worden verstrekt door de politiechef;
 - Deze periode bedraagt ten hoogste twee jaren indien de betrokkene op het tijdstip van die aanvraag nog niet de leeftijd van 18 jaar heeft bereikt;
 - De politiechef geeft duiding aan de politiegegevens;³⁵

³⁴ Het is mogelijk dat de bevoegdheden van het college op basis van artikel 19 Huisvestingswet 2014 zijn gemandateerd aan eigenaren of beheerders van woonruimte. Op basis van artikel 10 van het Besluit hebben zij dan dezelfde bevoegdheden (in het kader van de Wbmgp) als het college.

³⁵ Artikel 10b lid 3 Wbmgp.

- De politiegegevens bevatten geen tot andere personen dan de woningzoekende herleidbare persoonsgegevens.³⁶

Verstreking van gegevens door de burgemeester

Tot slot biedt de Wbmgp ook grondslagen voor gegevensverstrekking door de burgemeester:

- Verstreking van de woonverklaring door de burgemeester aan het college (artikel 6 lid 2 Besluit).
- Verlenen van inzage in de in het bestand opgenomen persoonsgegevens over de woningzoekende door de burgemeester bij bezwaar en beroep aan het bestuursorgaan dat belast is met de beslissing op bezwaar respectievelijk aan de bestuursrechter (artikel 11 Besluit).

Geheimhoudingsplicht

De Wbmgp bevat geen specifieke geheimhoudingsplicht. Wel geldt een geheimhoudingsplicht voor politiegegevens die op basis van de Wet politiegegevens zijn verkregen (artikel 7 Wet politiegegevens).³⁷

Doelbinding

De Wbmgp en het onderliggende Besluit kennen een strikte doelbinding ten aanzien van de te verwerken gegevens. Dit blijkt uit de volgende bepalingen:

- De politiegegevens en de duiding daarvan die de burgemeester heeft verkregen van de politiechef in het kader van het onderzoek naar de woonverklaring mag uitsluitend worden gebruikt voor de beoordeling van de aanvraag van de huisvestigingsvergunning (artikel 10b lid 7 Wbmgp).
- Daarnaast is de burgemeester verplicht om te voorkomen dat onder zijn verantwoordelijkheid werkzame personen de persoonsgegevens in het bestand voor andere doeleinden dan de uitvoering van de Wbmgp gebruiken (artikel 8 lid 3 Besluit).
- Persoonsgegevens in het bestand van de burgemeester als bedoeld in artikel 7 van het Besluit moeten – na het onherroepelijk worden van het besluit – door de burgemeester worden verwijderd en vernietigd (artikel 13 lid 2 Besluit).
- Uit artikel 13 lid 3, onder a, van het Besluit volgt dat de persoonsgegevens die het college verwerkt in een bestand als bedoeld in artikel 3 van het Besluit

³⁶ Artikel 5 lid 2 van het Besluit.

³⁷ Artikel 18 Wpg jo. artikel 4:3 lid 1 sub b onder 2 en sub m Besluit politiegegevens.

mogen worden bewaard in het kader van de evaluatie van de maatregel en de evaluatie ten behoeve van het verslag. Na het onherroepelijk worden van het besluit tot het al dan niet verlenen van een huisvestingsvergunning, mogen deze persoonsgegevens daarom uitsluitend ter beschikking worden gesteld aan degenen die belast zijn met de evaluatie op basis van een schriftelijke machtiging van het college, na raadpleging door het college van de functionaris gegevensbescherming (artikel 13 lid 3, onder b, Besluit). Zodra de desbetreffende gegevens niet meer noodzakelijk zijn voor de evaluatie(s) dient over te worden gegaan tot verwijdering en vernietiging van de gegevens (artikel 13 lid 3, onder c, Besluit).

Uit het voorgaande kan worden afgeleid dat de gegevens in het bestand als bedoeld in artikel 7 van het Besluit dat door de burgemeester wordt bijgehouden alleen mogen worden gebruikt voor de uitvoering van de Wbmgp. Voor de politiegegevens is daar nog een specifieke bepaling (artikel 10b Wbmgp) aan toegevoegd en bovendien moeten al deze gegevens in het bestand zo snel mogelijk na het onherroepelijk worden van het besluit worden vernietigd. De gegevens die het college verwerkt in een bestand als bedoeld in artikel 3 van het Besluit mogen na het onherroepelijk worden van het besluit uitsluitend voor evaluatiedoeleinden ter beschikking worden gesteld aan degenen die belast zijn met de evaluatie(s). Wanneer deze gegevens hiervoor niet meer noodzakelijk zijn moeten ook deze gegevens worden verwijderd en vernietigd. Ieder andere vorm van verwerking is niet toegestaan, met uitzondering van het geven van inzage aan degene wiens persoonsgegevens zijn verwerkt.

Zie in dit verband ook de Nota van Toelichting bij het Besluit, p. 10:

“Gezien de privacygevoeligheid van de persoonsgegevens is in de wet uitdrukkelijk bepaald dat de burgemeester de aan hem verstrekte politiegegevens, de duiding ervan en de periode waarop deze gegevens betrekking hebben, mag gebruiken voor de beoordeling van de aanvraag van een huisvestingsvergunning waarvoor hij een woonverklaring afgeeft aan het college van burgemeester en wethouders. De overige persoonsgegevens mogen op basis van deze algemene maatregel van bestuur worden bewaard voor evaluatie van deze maatregel. Deze persoonsgegevens kunnen na het onherroepelijk worden van het besluit van het college van burgemeester en wethouders tot het al dan niet verlenen van een huisvestingsvergunning uitsluitend ter beschikking worden gesteld nadat het college van burgemeester en wethouders daartoe een machtiging heeft gegeven aan personen die zijn belast met de evaluatie van de screeningsmaatregel op lokaal niveau of de evaluatie van de wet op rijksniveau. Zulke een machtiging wordt slechts verleend nadat het college de functionaris voor de gegevensbescherming hierover heeft geraadpleegd. Ieder andere vorm van verwerking is niet toegestaan met uitzondering van het op verzoek van de

persoon wiens persoonsgegevens in het bestand zijn verwerkt, inzage geven in diens persoonsgegevens.”

Conclusie

- De Wbmgp heeft tot doel de leefbaarheid in bepaalde buurten of wijken te vergroten door middel van selectieve woningtoewijzing. Om dit doel te verwezenlijken wordt onder andere rekening gehouden met de mate van criminaliteit.
- Op grond van de Wbmgp kunnen verscheidene gegevens worden verwerkt, waaronder politiegegevens over de aanvrager van een huisvestingsvergunning.
- Deze gegevens zijn gebonden aan een strikte wettelijke doelbinding en, waar het politiegegevens betreft, een strikte geheimhoudingsplicht.
- Gezien deze strikte doelbinding (en geheimhoudingsplicht) kunnen de gegevens die op grond van de Wbmgp zijn verzameld in de regel niet verder worden verwerkt voor de bestrijding van ondermijnende criminaliteit.

F. Woningwet

Doelstelling

De Woningwet stelt regels over het handelen van woningcorporaties en over de algemene (bouwkundige) staat van woningen en overige bouwwerken. Voor de aanpak van ondermijning is vooral van belang dat het college zorgdraagt voor de bestuursrechtelijke handhaving van de regels uit hoofdstuk I tot en met III van de Woningwet. In deze hoofdstukken staan onder andere voorschriften waaraan woningen moeten voldoen. De bestuursrechtelijke handhaving van deze voorschriften heeft als doel dat er geen gevaar ontstaat voor de gezondheid of veiligheid van bewoners en omwonenden.

Wettelijke grondslag

In de Woningwet staan verschillende grondslagen voor verkrijging van gegevens door het college. Bij de aanpak van ondermijning kan met name gedacht worden aan:

- Het verkrijgen van gegevens en bescheiden in het kader van de aanvraag van vergunningen voor bouw- of sloopwerkzaamheden (artikel 2 lid 3 Woningwet).
- Het verkrijgen van een verplicht gesteld onderhoudsplan van de vereniging van eigenaars (artikel 12d lid 4 Woningwet).
- De bepaling die het bevoegd gezag (veelal het college) verplicht zorg te dragen voor de bestuursrechtelijke handhaving van hetgeen is bepaald in hoofdstuk I tot en met III Woningwet (artikel 92 lid 1 Woningwet). Het college kan gegevens verzamelen bij de handhaving van onder andere de volgende voorschriften:
 - De eigenaar van een bouwwerk moet voorkomen dat als gevolg van de staat van het bouwwerk, open erf of terrein gevaar voor de gezondheid of veiligheid ontstaat dan wel voortduurt (artikel 1a Woningwet). Deze bepaling dient als vangnet om in te kunnen grijpen bij een noodsituatie.³⁸
 - De eigenaar moet bepaalde (technische of omgevingsrechtelijke/ruimtelijke) voorschriften over het bouwen, de staat van bestaande bouwwerken, het gebruik van bepaalde bouwwerken en het slopen daarvan hanteren (artikel 1b jo. 2-12c Woningwet).
- De bepaling op basis waarvan het bevoegd gezag, indien dat naar zijn oordeel noodzakelijk is, de eigenaar (of een ander die bevoegd is tot het treffen van voorzieningen) van een gebouw of bouwwerk kan verplichten tot het treffen van de nodige voorzieningen (artikel 13 Woningwet). Deze voorzieningen moeten ervoor zorgen dat de staat van het gebouw daarna komt te liggen

³⁸ Kamerstukken II 2003/04, 29392, 3 p. 21 en 26

tussen het niveau voor bestaande bouw en het niveau voor nieuwbouw. Deze voorwaarden worden verder uitgewerkt in het Bouwbesluit.

In algemene zin geldt voor toezichthouders dat zij op grond van de Awb inlichtingen kunnen vorderen (artikel 5:16 Awb) en zakelijke gegevens en bescheiden kunnen opvragen (artikel 5:17 Awb). Op grond van deze bepalingen kunnen ook kopieën van stukken en bescheiden worden gevorderd. In beginsel kunnen inlichtingen van een ieder worden gevorderd, mits dat in lijn is met het evenredigheidsbeginsel (artikel 5:13 Awb). Het uitgangspunt is dat de toezichthouder zijn bevoegdheden niet mag uitoefenen als dat niet noodzakelijk is en dat hij zijn bevoegdheden op een voor de burger zo min mogelijk belastende wijze uitoefent. Ook ligt het in de rede dat de toezichthouder zijn vordering motiveert. In beginsel is een ieder verplicht tot medewerking aan dergelijke vorderingen (artikel 5:20 Awb).

Geheimhoudingsplicht en doelbinding

De Woningwet bevat, behoudens de geheimhoudingsplicht voor woningcorporaties met betrekking tot inkomensgegevens van de huurders (55 lid 4 Woningwet), geen specifieke geheimhoudingsplicht.

In de Woningwet is geen specifiek doelbindingsbeginsel opgenomen. Rekening moet worden gehouden met het algemene doelbindingsbeginsel uit artikel 5 lid 1 sub b en 6 lid 4 AVG.

De hierboven opgesomde verwerkingsgrondslagen hebben veelal betrekking op de bouwkundige staat van de woning. Handhaving van de voorschriften heeft tot doel de veiligheid en gezondheid van bewoners en omwonenden te waarborgen. Vraag is vervolgens of de ter uitvoering van de Woningwet verkregen gegevens ook kunnen worden geraadpleegd als ter bestrijding van ondermijning de inzet van gemeentelijke bevoegdheden wordt overwogen. Er zal in het concrete geval moeten worden afgewogen of de bevoegdheden die men overweegt in te zetten, dicht genoeg tegen de doelstellingen van de Woningwet aanliggen om de uitwisseling en verder gebruik van persoonsgegevens te rechtvaardigen.

Conclusie

- De Woningwet stelt, voor zover relevant in dit kader, regels met betrekking tot de handhaving van bepaalde woningvoorschriften. Het gaat daarbij veelal om voorschriften met betrekking tot gebouwen;
- De Woningwet kent, behoudens voor woningcorporaties met betrekking tot de inkomensgegevens, geen specifieke bepalingen omtrent geheimhouding of doelbinding;

- De informatie die verwerkt wordt op grond van de Woningwet zou onder omstandigheden gebruikt kunnen worden voor de aanpak van ondermijning. Daarbij dient te vraag te worden beantwoord of de bevoegdheid die de gemeente wil inzetten dicht genoeg aanligt tegen de doelstellingen van de Woningwet, te weten: het voorkomen van gevaar voor de veiligheid en gezondheid van bewoners en omwonenden.

G. Wet bevordering integriteitsbeoordelingen door het openbaar bestuur

Doelstelling

De Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (hierna: Wet Bibob) verschaft bestuursorganen³⁹ de mogelijkheid om een vergunning, ontheffing of subsidie (gedeeltelijk) te weigeren of in te trekken indien zich het gevaar voordoet dat de beschikking wordt gebruikt voor – kort gezegd – het plegen van strafbare feiten dan wel voor het benutten van uit gepleegde strafbare feiten verkregen of te verkrijgen op geld waardeerbare voordelen. Ook bij vastgoedtransacties en bij bepaalde aanbestedingen kunnen bestuursorganen onderzoek doen naar de integriteit van de natuurlijke persoon of rechtspersoon met wie een vastgoedtransactie wordt aangegaan respectievelijk die in aanmerking komt voor het uitvoeren van een overheidsopdracht.

Een bestuursorgaan verkrijgt bij het onderzoek dat het doet bij toepassing van de Wet Bibob (het zgn. “eigen onderzoek”) persoonsgegevens over de aanvrager/gedagigde (hierna: de betrokkene). Daarnaast kan een bestuursorgaan zich wenden tot het Landelijk Bureau Bibob voor een advies over de mate van gevaar dat een vergunning, ontheffing, subsidie, vastgoedtransactie of opdracht wordt misbruikt. Een dergelijk advies zal ook persoonsgegevens bevatten. Het Landelijk Bureau Bibob heeft toegang tot meer relevante (gesloten) bronnen dan dat bestuursorganen bij het eigen onderzoek hebben.

Wettelijke grondslag

Een bestuursorgaan kan voor het eigen onderzoek in het kader van de Wet Bibob verschillende bronnen gebruiken:⁴⁰

- Dat betreft allereerst de door de betrokken (rechts)persoon aangeleverde informatie via het Bibob-vragenformulier (artikel 30 Wet Bibob);
- Daarnaast kunnen bestuursorganen ten behoeve van het eigen onderzoek in openbare bronnen zoeken en – in beperkte mate – uit niet-openbare bronnen informatie opvragen over de betrokkene. Voor wat betreft de niet-openbare bronnen gaat het om gegevens die gemeenten bij of krachtens andere wetten mogen ontvangen ten behoeve van de toepassing van de Wet Bibob. Het gaat dan bijvoorbeeld om justitiële gegevens, politiegegevens en strafvorderlijke gegevens (artikel 15 Besluit justitiële en strafvorderlijke

³⁹ Afhankelijk van de omstandigheden van het concrete geval gaat het hier om het college of de burgemeester.

⁴⁰ Op het moment van schrijven van deze analyse is een voorstel tot wijziging van de Wet Bibob aanhangig. Dat wetsvoorstel beoogt onder meer de informatiepositie van bestuursorganen bij het eigen onderzoek te verbeteren. Het wetsvoorstel bevat onder andere een rechtstreekse tipfunctie van het Landelijk Bureau Bibob aan bestuursorganen. Zie *Kamerstukken II* 2018/19, 35 152, nr. 2. Zie ook de toelichting op dat wetsvoorstel, *Kamerstukken II* 2018/19, 35 152, nr. 3, p. 11-12. Met deze wijzigingen is in onderstaande analyse nog geen rekening gehouden.

gegevens; artikel 4:3, eerste lid, onder I, Besluit politiegegevens; en artikel 39f lid 1, onder d en g, en lid 2 Wet justitiële en strafvorderlijke gegevens jo. hoofdstuk III, onderdeel 3, onder d en g, van de Aanwijzing Wet justitiële en strafvorderlijke gegevens). Ook kunnen bestuursorganen netwerktekeningen ontvangen van de Dienst Justis, waarin de onderlinge relaties tussen bevroegde natuurlijke personen en/of rechtspersonen worden weergegeven, evenals relevante faillissementen en ontbindingen (artikel 6, onder g, Besluit controle op rechtspersonen);

- Ook kan gebruik worden gemaakt van een mededeling van het Landelijk Bureau Bibob over eerdere advisering ten aanzien van dezelfde betrokkene (artikel 11a Wet Bibob), van de tipfunctie van de officier van justitie (artikel 26 Wet Bibob) en van informatie die in een Regionaal Informatie en Expertise Centrum (RIEC) wordt gedeeld (artikel 28, tweede lid, onder d, Wet Bibob);
- Tot slot kunnen bestuursorganen gebruikmaken van interne bronnen die gegevens bevatten die in het kader van andere taken zijn verzameld, bijvoorbeeld van de bij een vergunningaanvraag door de aanvrager aangeleverde informatie.⁴¹

Daarnaast kan een bestuursorgaan het Landelijk Bureau Bibob verzoeken advies uit te brengen over de mate van gevaar. Dat advies wordt vervolgens aan het bestuursorgaan verstrekt (artikel 9 Wet Bibob). Het advies mag gedurende twee jaar worden gebruikt voor een andere beslissing (artikel 29 Wet Bibob).

Geheimhoudingsplicht

Artikel 28 lid 1 Wet Bibob bevat een geheimhoudingsplicht voor een ieder die krachtens de Wet Bibob de beschikking krijgt over gegevens met betrekking tot een derde, tenzij de verstrekking uitdrukkelijk is toegestaan in de Wet Bibob.

Artikel 28 lid 2 Wet Bibob bepaalt vervolgens dat bestuursorganen de gegevens uit het Bibob-advies niet mogen doorgeven, behalve aan de in datzelfde lid genoemde (potentiële) ontvangers. Op grond van artikel 30 lid 6 Wet Bibob is artikel 28 lid 2 Wet Bibob van overeenkomstige toepassing op de bevindingen van het eigen onderzoek van het bestuursorgaan.

Uit het voorgaande volgt dat informatie die wordt verkregen door toepassing van de Wet Bibob alleen mag worden gedeeld met de in artikel 28 lid 2 Wet Bibob genoemde ontvangers. Een team dat verantwoordelijk is voor de aanpak van ondermijning en/of een ander gemeentelijk team wordt niet genoemd als ontvanger. In het kader van het eigen onderzoek verkregen informatie en de via het Landelijk Bureau Bibob verkregen informatie mag dus niet worden gedeeld met een ondermijningsteam en/of een ander team van de gemeente. Andersom mogen de medewerkers van de gemeente die

⁴¹ Vgl. de conceptmemorie van toelichting tot wijzigingen van de Wet Bibob (www.internetconsulatie.nl/wetbibob), p. 3; en *Kamerstukken II* 2018/19, 35 152, nr. 3, p. 11-12.

belast zijn met de toepassing van de Wet Bibob wel kennisnemen van de informatie die bij andere gemeentelijke teams berust.

Doelbinding

Het doelbindingsbeginsel wordt ingekleurd door de geheimhoudingsplicht van artikel 28 en 30 lid 6 Wet Bibob. Genoemde artikelen staan eraan in de weg dat een bestuursorgaan de gegevens die het krachtens de Wet Bibob heeft verkregen aanwendt voor andere doeleinden.

Conclusie

- De Wet Bibob biedt bestuursorganen de mogelijkheid de integriteit van partijen te beoordelen in het kader van vergunningen, ontheffingen, subsidies, (bepaalde) aanbestedingen en vastgoedtransacties, met als uiteindelijk doel om de integriteit van het bestuursorgaan te beschermen;
- Daartoe kan een bestuursorgaan zelf onderzoek doen (het zogenoemde eigen huiswerk) en zo nodig advies vragen van het Landelijk Bureau Bibob;
- Op de in het kader van de Wet Bibob verkregen gegevens rust een geheimhoudingsplicht. Een ieder die krachtens de Wet Bibob over gegevens beschikking krijgt, is verplicht tot geheimhouding. De partijen met wie wel gegevens mogen worden gedeeld, zijn limitatief opgesomd in artikel 28 lid 2 Wet Bibob. Daaruit volgt dat de gegevens die zijn verkregen in het kader van de Wet Bibob niet mogen worden gebruikt voor andere taken/doelen van de gemeente;
- Tegelijkertijd hebben de medewerkers van gemeenten die belast zijn met de Wet Bibob toegang tot verschillende open, gesloten en interne bronnen over een betrokkene. Daarmee bestaat binnen gemeenten bij (beslissingen rondom de verlening van) vergunningen, ontheffingen, subsidies, (bepaalde) aanbestedingen en vastgoedtransacties de mogelijkheid om een grote verscheidenheid aan informatie te verzamelen over natuurlijke personen en rechtspersonen.

H. Algemene wet inzake rijksbelastingen

Doelstelling

In de Algemene wet inzake rijksbelastingen (AWR) zijn regels opgenomen met betrekking tot het heffen van de rijksbelastingen. De AWR en de bijbehorende Uitvoeringsregeling AWR 1994 bevatten verschillende grondslagen voor gegevensverwerking, met name voor de Belastingdienst en de inspecteur. Een deel van de bepalingen uit de AWR is ook van toepassing bij de heffing van gemeentelijke belastingen.

Wettelijke grondslag

Algemene verwerkingsgrondslagen

De AWR bevat voornamelijk informatieverplichtingen aan en verwerkingsgrondslagen voor de inspecteur/Belastingdienst. In het kader van de gemeentelijke belastingheffing moet in plaats van de inspecteur/Belastingdienst gelezen worden: de gemeenteambtenaar die belast is met de heffing van gemeentelijke belastingen. Op grond van de AWR:⁴²

- verkrijgt de inspecteur of gemeenteambtenaar gegevens of bescheiden die noodzakelijk zijn voor het doen van aangifte van belastingplichtigen (artikel 7 jo. artikel 8 AWR);
- ontvangt de inspecteur of gemeenteambtenaar mededelingen van belastingplichtige / inhoudingsplichtige over eventuele onjuistheden / onvolledigheden in de relevante gegevens (artikel 10a lid 1 AWR);
- is de inspecteur of gemeenteambtenaar belast met het bijhouden en uitvoeren van de basisregistratie inkomen (artikel 21b jo. 21a AWR);
- verkrijgt de inspecteur alle gegevens en inlichtingen die noodzakelijk zijn voor de belastingheffing en die vallen onder de informatieverplichting van artikel 47 en 47b AWR.⁴³

⁴² Op grond van artikel 231 Gemeentewet gelden de opgesomde bepalingen in de AWR ook voor de gemeentelijke belastingheffing.

⁴³ Vgl. voor de overige informatieverplichtingen en bijkomende verplichtingen artikelen 47b – 51 AWR.

Verstrekking van inkomensgegevens aan het college/de gemeente

Het verstrekken van inkomensgegevens uit de basisregistratie inkomen (inclusief authentieke gegevens uit andere basisregistraties) door de inspecteur aan het college⁴⁴ is geoorloofd op grond van artikel 21b lid 1 jo. artikel 21e AWR.

Geheimhoudingsplicht

Het is een ieder op grond van artikel 67 AWR verboden hetgeen hem uit of in verband met de uitvoering van de belastingwet over de persoon of zaken van een ander blijkt of wordt meegedeeld, verder bekend te maken dan noodzakelijk is voor de uitvoering van de belastingwet of voor de invordering van een rijksbelasting als bedoeld in de Invorderingswet 1990. Deze geheimhoudingsverplichting kan volgens het tweede lid slechts doorbroken worden:

- d. indien er een wettelijk voorschrift is dat tot bekendmaking verplicht (een voorbeeld is artikel 64 lid 1, onderdeel c, Participatiewet, dat de Belastingdienst verplicht tot verstrekking aan het college);
- e. indien de Minister van Financiën in een regeling heeft bepaald dat de bekendmaking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak van een bestuursorgaan. Dat is uitgewerkt in artikel 43c van de Uitvoeringsregeling AWR 1994. Artikel 43c lid 1 aanhef en onder j,⁴⁵ m⁴⁶ en w⁴⁷ van de Uitvoeringsregeling AWR geven een mogelijkheid tot verstrekking van bepaalde gegevens aan de gemeente voor specifiek bepaalde doelen;
- f. indien gegevens worden verstrekt aan degene op wie de gegevens betrekking hebben en die gegevens ook door of namens diegene zijn verstrekt.

⁴⁴ Het college is een afnemer in de zin van artikel 21, onder f, AWR voor zover hij bevoegd is tot het uitvoeren van inkomensafhankelijke regelingen zoals bijvoorbeeld de Participatiewet.

⁴⁵ Dat zijn: 1) gegevens over winst uit onderneming, loon, en resultaat uit overige werkzaamheden in de zin van de Wet inkomsten belasting 2001 over een bepaalde periode en identificerende gegevens van een eventuele inhoudingsplichtige in de zin van de Wet op de loonbelasting 1964 van (voormalige) ambtenaren, ten behoeve van de vaststelling van en controle op betalingen van werkloosheidsuitkeringen op grond van gemeentelijke verordeningen; 2) gegevens over het inkomen van voormalige ambtsdragers ter uitvoering van de wachtgeldregeling; 3) gegevens over uit te betalen voorlopige teruggaven inkomstenbelasting wegens toegekende heffingskortingen, op naam van de belastingschuldige staande bankrekeningnummers, kentekenregistergegevens en identificeerbare gegevens van een eventuele inhoudingsplichtige ten behoeve van de inning van gemeentelijke belastingen; 4) gegevens over bewoning van eigen woning ten behoeve van het tegengaan van permanente bewoning van recreatiewoningen; 5) kentekenregistergegevens van circus- en kermisauto's ten behoeve van de uitvoering en handhaving van het gemeentelijke ontheffingenbeleid inrijverbod milieuzones; 6) NAW-gegevens van erfgenamen voor het innen van openstaande gemeentelijke belastingschulden van de overledene; en 7) gegevens die van belang kunnen zijn voor vergunningverlening en het houden van toezicht in het kader van de Wet milieubeheer.

⁴⁶ Het gaat daarbij om gegevens die nodig zijn om de samenwerking in het kader van de integrale toepassing en handhaving van overheidsregelingen effectief en efficiënt te laten verlopen voor zover een convenant is gesloten met deze bestuursorganen, zoals het RIEC-convenant.

⁴⁷ Het gaat daarbij om gegevens die nodig zijn voor de uitvoering van samenwerkingsprojecten door middel van interventieteams ter voorkoming en terugdringing van belasting- en premiefraude, toeslagenfraude, uitkeringsfraude, overtredingen van arbeidswetgeving en de daarmee samenhangende misstanden.

Daarnaast kan de minister ontheffing verlenen voor het doorbreken van de geheimhoudingsplicht (artikel 67 lid 3 AWR).

De geheimhoudingsplicht van artikel 67 AWR is ook van toepassing op 'gemeentelijke belastinggegevens'. In artikel 67 AWR staat, zoals besproken, onder meer dat de geheimhoudingsplicht niet geldt als bij regeling van de minister is bepaald dat bekendmaking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak van een bestuursorgaan. Die regeling is de Uitvoeringsregeling AWR (artikel 43c), zoals eveneens reeds is toegelicht. De vraag is dan of de doorbrekingsgronden uit artikel 43c van de Uitvoeringsregeling AWR óók gelden voor zover het gaat om gemeentelijke belastinggegevens. Dat is niet zo, omdat de Uitvoeringsregeling AWR (anders dan de AWR en de Iw 1990 zelf) níet van overeenkomstige toepassing is.⁴⁸ Daar staat echter tegenover dat het college ter zake gemeentelijke belastinggegevens een soortgelijke doorbrekingsregeling kan treffen in de vorm van een college-besluit, mits de bekendmaking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak van een bestuursorgaan. In dat besluit zal dan heel precies moeten worden uitgewerkt ten behoeve van welke publiekrechtelijke taken van welke bestuursorganen het noodzakelijk is dat de geheimhoudingsplicht ten aanzien van de gemeentelijke belastinggegevens niet geldt (zie artikel 231 lid 3 Gemeentewet⁴⁹).

Ook ten aanzien van inkomensgegevens uit de basisregistratie inkomen geldt een geheimhoudingsplicht. Het college is niet bevoegd om een inkomensgegeven verder bekend te maken dan noodzakelijk voor de uitvoering van de hiervoor bedoelde wettelijke bevoegdheid (artikel 21f lid 2 AWR).

Doelbinding

Artikel 67 AWR bevat, als gezegd, een strikte geheimhoudingsplicht die alleen in een aantal limitatief bedoelde gevallen kan worden doorbroken. Dat kleurt het doelbindingsbeginsel in. Bij de bespreking van de doorbreking van de geheimhoudingsplicht is genoemd dat gemeenten fiscale gegevens verkrijgen voor specifiek bepaalde doelen. Deze gegevens mogen alleen voor die doelen worden gebruikt. Verdere verwerking voor andere doelen is niet toegestaan.

Voorts geldt ten aanzien van de inkomensgegevens uit de basisregistratie inkomen een specifieke doelbindingsbepaling. Het college mag deze inkomensgegevens als afnemer uitsluitend gebruiken voor bij de uitoefening van een op grond van een wettelijk voorschrift verleende bevoegdheid tot gebruik van dit gegeven (artikel 21f lid 1 AWR).

⁴⁸ *Kamerstukken II 1995/96, 24 771, nr. 3, p. 26.*

⁴⁹ En zie *Kamerstukken II 1995/96, 24 771, nr. 3, p. 26* en *Kamerstukken II 1996-1997, 25 280, nr. 3, p. 70-71.*

Conclusie

- In de AWR zijn regels opgenomen met betrekking tot het heffen van de rijksbelastingen. Deze regels zijn deels van overeenkomstige toepassing op het heffen van gemeentelijke belastingen. Daarnaast kan het college voor zover hij bevoegd is tot het uitvoeren van inkomensafhankelijke regelingen inkomensgegevens uit de basisregistratie inkomen ontvangen.
- De AWR kent een strikte geheimhoudingsplicht, die alleen in limitatief omschreven gevallen kan worden doorbroken.
- Fiscale gegevens kunnen worden geraadpleegd ten behoeve van de aanpak van ondermijnende criminaliteit, voor zover dat is te brengen onder de in de Uitvoeringsregeling AWR omschreven gevallen of, waar het gaat om gemeentelijke belastinggegevens, een eventueel college-besluit dat een doorbrekingsgrond bevat.
- Ten aanzien van de inkomensgegevens uit de basisregistratie inkomen geldt nog een specifieke doelbindingsbepaling. Het college mag deze inkomensgegevens als afnemer uitsluitend gebruiken voor bij de uitoefening van een op grond van een wettelijk voorschrift verleende bevoegdheid tot gebruik van dit gegeven.

I. Invorderingswet 1990

Doelstelling

De Invorderingswet 1990 (Iw 1990) regelt de invorderingsbevoegdheden van de ontvanger. De ontvanger is in de eerste plaats de invorderingsambtenaar van de Belastingdienst. Dit kan ook de gemeenteambtenaar zijn die is belast met de invordering van gemeentelijke belastingen.⁵⁰ Een deel van de bepalingen uit de Iw 1990 is ook van toepassing op de heffing van gemeentelijke belastingen.

Wettelijke grondslag

De invorderingsbevoegdheden van de (gemeentelijke) invorderingsambtenaren gaan gepaard met diverse informatieverplichtingen en bijbehorende verwerkingsgrondslagen. Wij wijzen onder meer op:⁵¹

- de inlichtingenverplichting, met betrekking tot gegevens die van belang kunnen zijn voor de invordering, van een ieder jegens de ontvanger (artikel 58 Iw 1990) en van bepaalde financiële ondernemingen (artikel 62bis Invorderingswet);
- de inlichtingenverplichting van rechtspersonen om gegevens over te leggen aan de ontvanger die noodzakelijk zijn voor de vaststelling van de betalingsonmacht of voor de bepaling van de financiële situatie, indien blijkt dat de rechtspersoon niet in staat is belasting te betalen (artikel 36 lid 2 Iw 1990 jo. artikel 8 Uitvoeringsbesluit Invorderingswet 1990).

Geheimhoudingsplicht

De Iw 1990 bevat een geheimhoudingsplicht die vergelijkbaar is met de geheimhoudingsplicht van artikel 67 Algemene wet inzake rijksbelastingen (artikel 67 Iw 1990). Wij verwijzen op dit punt dan ook naar hetgeen bij de AWR is opgemerkt over de geheimhoudingsplicht.

Artikel 43c Uitvoeringsregeling AWR 1994, waarin de doorbrekingsgronden van de geheimhoudingsplicht staan opgesomd, geldt ook voor de geheimhoudingsplicht van artikel 67 Iw 1990. Goed verdedigbaar is dat het college ter zake gemeentelijke invorderingsgegevens een soortgelijke doorbrekingsregeling kan treffen in de vorm van een college-besluit, mits de bekendmaking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak van een bestuursorgaan. In dat besluit zal dan heel precies moeten worden uitgewerkt ten behoeve van welke publiekrechtelijke

⁵⁰ Artikel 3 Iw 1990 belast de ontvanger met de invordering van Rijksbelastingen. Artikel 231 lid 2 Gemeentewet bepaalt kort gezegd dat voor 'ontvanger' de 'gemeenteambtenaar' moet worden gelezen bij gemeentelijke belastingheffingen.

⁵¹ Op grond van artikel 231 Gemeentewet gelden de volgende bepalingen in de AWR ook voor de gemeentelijke belastingheffing.

taken van welke bestuursorganen het noodzakelijk is dat de geheimhoudingsplicht ten aanzien van de gemeentelijke invorderingsgegevens niet geldt (zie artikel 231 lid 3 Gemeentewet⁵²).

Doelbinding

Zie de bespreking van de geheimhouding en doelbinding bij de AWR. Hier zijn de doelen genoemd waarvoor de gemeente op grond van de Iw 1990 verkregen gegevens mag gebruiken. Verdere verwerking voor andere doelen zal niet zijn toegestaan.

Conclusie

- De Iw 1990 regelt de invorderingsbevoegdheden van de (gemeentelijke) ontvanger.
- De Iw 1990 kent een strikte geheimhoudingsplicht, die alleen in limitatief omschreven gevallen kan worden doorbroken.
- Op grond van de Iw 1990 verkregen gegevens kunnen worden geraadpleegd ten behoeve van de aanpak van ondermijnende criminaliteit, voor zover dat is te brengen onder de in de Uitvoeringsregeling AWR omschreven gevallen of, waar het gaat om gemeentelijke invorderingsgegevens, een eventueel college-besluit dat een doorbrekingsgrond bevat.

⁵² En zie *Kamerstukken II* 1995/96, 24 771, nr. 3, p. 26 en *Kamerstukken II* 1996-1997, 25 280, nr. 3, p. 70-71. Vgl. daarnaast onderdeel H hiervoor bij geheimhoudingsplicht

J. Wet basisregistratie personen

Doelstelling

De Brp is een centrale database met persoonsgegevens van inwoners van Nederland (ingezetenen) en van personen die Nederland hebben verlaten (niet ingezetenen). Overheidsorganen die voor de uitvoering van hun taken persoonsgegevens nodig hebben en derden⁵³, kunnen verzoeken om informatie uit de Brp. Beide verstrekkingen worden geregeld in de Wet basisregistratie personen en het besluit Brp. Zoals blijkt uit de artikelen 3.1 t/m 3.9 Wet Brp, moet daarbij onderscheid gemaakt worden tussen verstrekkingen door de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK)) en verstrekkingen door colleges van B&W van een gemeente. Verstrekkingen door colleges van B&W kunnen onderscheiden worden in verstrekkingen over alle ingeschrevenen en verstrekkingen over (in beginsel) de ingezetenen van de eigen gemeente.

Een bestuursorgaan dat bij de vervulling van zijn taak informatie over een ingeschrevene nodig heeft die in de vorm van een authentiek gegeven beschikbaar is in de basisregistratie (zoals het woonadres van ingezetenen⁵⁴) is op grond van de Wet Brp *verplicht* dat authentieke gegevens te gebruiken, enkele uitzonderingen daargelaten.⁵⁵

Wettelijke grondslag

De minister van BZK verstrekt Brp-gegevens aan een overheidsorgaan⁵⁶, voor zover dat is bepaald in een zogenaamd autorisatiebesluit van de minister van BZK. Criterium daarbij is dat de gegevens noodzakelijk zijn voor de goede vervulling van de taak van het overheidsorgaan dat om de autorisatie verzoekt. Het betreft een zogenaamde systematische verstrekking, waarbij het gaat om Brp-gegevens over zowel binnengemeentelijke als buitengemeentelijke inwoners.⁵⁷

Daarnaast kan het college van B&W op verzoek van een overheidsorgaan aan hem Brp-gegevens verstrekken, voor zover deze gegevens noodzakelijk zijn voor de goede vervulling van de taak van dat overheidsorgaan.⁵⁸ Voorwaarde daarbij is wel dat het aantal verstrekkingen per jaar aan het overheidsorgaan naar redelijke verwachting van het college niet meer zal zijn dan vijfduizend verstrekkingen.⁵⁹ Het gaat hier om Brp-gegevens over zowel binnengemeentelijke als buitengemeentelijke inwoners.

⁵³ Gelet op de irrelevantie daarvan voor het onderwerp zal hierna geen aandacht meer worden besteed aan de verstrekking aan derden.

⁵⁴ Zie artikel 1.1 aanhef en onder n jo. artikel 1.6 Wet Brp jo. artikel 2 en bijlage 1 Besluit Brp. Het woonadres van de niet-ingezetene is geen authentiek gegeven.

⁵⁵ Zie artikel 1.7 Wet Brp.

⁵⁶ Dat is i) een orgaan van een rechtspersoon die krachtens publiekrecht is ingesteld, of ii) een ander persoon of college, met enig openbaar gezag bekleed.

⁵⁷ Artikel 3.1 t/m 3.3 Wet Brp.

⁵⁸ Artikelen 3.4 en 3.5 Wet Brp.

⁵⁹ Artikel 3.5 Wet Brp j. artikel 40 Besluit Brp.

Tot slot wijzen wij op artikel 3.8 Wet Brp. Op grond van dat artikel kunnen bij of krachtens gemeentelijke verordening regels gesteld worden omtrent de verstrekking van Brp-gegevens aan overheidsorganen die een orgaan zijn van de gemeente. Daarbij geldt wel de eis dat slechts Brp-gegevens aan een overheidsorgaan worden verstrekt voor zover deze gegevens noodzakelijk zijn voor de goede vervulling van zijn taak. Het gaat hierbij slechts om gegevens over *binnengemeentelijke* inwoners.⁶⁰

Geheimhoudingsplicht

De Wet Brp geen specifieke geheimhoudingsplicht. Overheidsorganen (zoals gemeentelijke bestuursorganen) hebben juist een ruime bevoegdheid – en soms zelfs een verplichting – om van Brp-gegevens gebruik te maken, namelijk voor zover dat noodzakelijk is voor de goede vervulling van hun taak.

Doelbinding

Voor zover de raadpleging van Brp-gegevens is te koppelen aan de vervulling van die taak, hetgeen bij de bestrijding van ondermijning (waarbij wordt aangeknoopt bij gemeentelijke wettelijke taken en bevoegdheden) al snel aan de orde zal zijn, speelt het doelbindingsbeginsel niet: er wordt dan primair (en geen secundair) gebruik van Brp-gegevens gemaakt.

Conclusie

- Gemeentelijke bestuursorganen hebben een ruime bevoegdheid – en soms zelfs een verplichting – om van Brp-gegevens gebruik te maken, namelijk voor zover dat noodzakelijk is voor de goede vervulling van hun taak.
- Bij de bestrijding van ondermijning (waarbij wordt aangeknoopt bij gemeentelijke wettelijke taken en bevoegdheden) is van een dergelijke publieke taak al snel sprake.
- Dat betekent dat ten behoeve van de bestrijding van ondermijning Brp-gegevens zullen kunnen worden geraadpleegd.

⁶⁰ "over ingeschrevenen ten aanzien van wie het college op grond van artikel 1.4 verantwoordelijk is voor de bijhouding van de persoonslijst", zie art. 3.7 lid 2 Wet Brp.

K. Wet algemene bepalingen omgevingsrecht

Doelstelling

Doelstelling van de Wet algemene bepalingen omgevingsrecht (Wabo) is om de regels over de toestemmingen om te slopen, te bouwen, op te richten of (in strijd met het bestemmingsplan) te gaan gebruiken te verzamelen in één wettelijke regeling. Het samenvoegen van deze toestemmingen in één omgevingsvergunning heeft administratieve (schaal)voordelen en zorgt voor een betere dienstverlening aan de burger en bedrijven. Daarnaast moest de samenvoeging leiden tot een impuls om samenwerking binnen en tussen overheden te verbeteren. De Wabo zorgt ervoor dat er voor een fysiek project één integrale vergunningprocedure kan worden doorlopen. Er is dan ook één bestuursorgaan eindverantwoordelijk voor de beoordeling van het fysieke project. De Wabo heeft een reguliere en een uitgebreide procedure om tot een oordeel over de verzochte omgevingsvergunning te kunnen komen met het oog op de fysieke leefomgeving. Ook de handhaving wordt in de Wabo zo veel mogelijk geüniformeerd. In paragraaf 5.2 Wabo zijn regels opgenomen omtrent de samenwerking tussen verschillende bestuursorganen. Hier komt ook de onderlinge uitwisseling van gegevens aan de orde.

In het Besluit omgevingsrecht (Bor) en de Regeling omgevingsrecht (Ror) worden de regels uit de Wabo nader uitgewerkt.

Wettelijke grondslag

De specifieke verwerkingsgrondslagen uit de Wabo gaan uit van het 'bevoegd gezag'. Het bevoegd gezag is het bestuursorgaan dat bevoegd is tot het nemen van een besluit ten aanzien van een aanvraag om een omgevingsvergunning of ten aanzien van een al verleende omgevingsvergunning. Dat is in beginsel het college van burgemeester en wethouders, maar kunnen ook gedeputeerde staten of de betrokken minister zijn. In dat geval zijn de hiernavolgende wettelijke grondslagen van belang.

Aanvraag omgevingsvergunning

De aanvrager van een omgevingsvergunning is verplicht tot het verstrekken van gegevens en bescheiden aan het bevoegd gezag (artikel 2.8 lid 1 Wabo jo. artikel 4.4 Bor jo. artikel 1.3 Ror). Het gaat daarbij om de volgende gegevens:

- a. de naam, het adres en de woonplaats van de aanvrager, alsmede het elektronisch adres van de aanvrager, indien de aanvraag met een elektronisch formulier wordt ingediend;
- b. het adres, de kadastrale aanduiding dan wel de ligging van het project;
- c. een omschrijving van de aard en omvang van het project;

- d. indien de aanvraag wordt ingediend door een gemachtigde: zijn naam, adres en woonplaats, alsmede het elektronisch adres van de gemachtigde, indien de aanvraag met een elektronisch formulier wordt ingediend;
- e. indien het project wordt uitgevoerd door een ander dan de aanvrager: zijn naam, adres en woonplaats.

De aanvrager en de vergunninghouder dienen diverse persoonsgegevens te vermelden bij het doen van een melding aan het bevoegd gezag van de overgang van een omgevingsvergunning (artikel 2.25 lid 2 van de Wabo en artikel 4.8 Bor). Het gaat daarbij om de volgende gegevens:

- a. zijn naam en adres;
- b. de omgevingsvergunning of omgevingsvergunningen krachtens welke de activiteiten worden verricht;
- c. de naam, het adres en het telefoonnummer van degene voor wie de omgevingsvergunning zal gaan gelden;
- d. een contactpersoon van degene voor wie de omgevingsvergunning zal gaan gelden;
- e. het beoogde tijdstip dat de omgevingsvergunning zal gaan gelden voor de onder c bedoelde persoon.

Het bevoegd gezag moet de gegevens en bescheiden die betrekking hebben op aanvragen van omgevingsvergunningen opnemen in de landelijke voorziening (Omgevingsloket online). Deze gegevens kunnen worden geraadpleegd door het bevoegd gezag en overige bestuursorganen die betrokken zijn bij de verlening van de omgevingsvergunning. Het bevoegd gezag is verantwoordelijk voor het beheer en de verstrekking van de gegevens aan de overige bestuursorganen (artikel 7.6 Wabo en artikel 1.2 Ror).

Handhaving Wabo

Het bevoegd gezag kan gegevens die nodig zijn voor de bestuursrechtelijke handhaving van de geldende voorschriften verzamelen en registreren (artikel 5.2 lid 1 onder a en b, van de Wabo). Daarbij kunnen de betrokken ministers en betrokken bestuursorganen aan elkaar en aan instanties die belast zijn met strafrechtelijke handhaving van de Wabo gegevens delen die zij/de omgevingsdienst hebben verkregen (artikel 5.8 Wabo). Het gaat daarbij om gegevensuitwisseling van gegevens die het bestuursorgaan/de omgevingsdienst hebben verkregen in het kader van de uitvoering en handhaving van de Wabo.⁶¹

⁶¹ Juridisch gezien wijst artikel 5.8 lid 1 Wabo naar artikel 5.3 lid 4 Wabo, waarin geregeld is dat bij amvb taken worden aangewezen voor de omgevingsdienst. In artikel 7.1 Bor worden deze taken uitgewerkt. Het gaat daarbij om toezicht op de naleving van omgevingsvergunningen en andere ruimtelijke voorschriften.

Het college is op grond van artikel 7.2 Bor verplicht tot het opstellen van een handhavingsbeleid inzake vergunningverlening, toezicht en handhaving van het omgevingsrecht. Het handhavingsbeleid wordt jaarlijks uitgewerkt in een uitvoeringsprogramma (artikel 7.3 Bor). Ter monitoring van het handhavingsbeleid is het college op grond van artikel 7.6 Bor verplicht om de gegevens verkregen in het kader van de handhaving van het Bor te verwerken in de landelijke voorziening. Volgens artikel 10.6 Ror bevat het geautomatiseerde systeem in ieder geval een overzicht van:

- a. uitgevoerde controles;
- b. geconstateerde overtredingen;
- c. opgelegde bestuurlijke sancties;
- d. processen-verbaal;
- e. over mogelijke overtredingen ontvangen klachten.

Het doel van deze verwerking in de landelijke regeling is het monitoren en bewaken van de resultaten en de voortgang van (a) de uitvoering van het uitvoeringsprogramma en (b) het bereiken van de doelen van het handhavingsbeleid (artikel 7.6 Bor).

In sommige (uitzonderlijke) gevallen is het college weliswaar niet het bevoegd gezag, maar verwerkt het college of de burgemeester toch gegevens. Hiervan is in de volgende gevallen sprake:

- Het toezenden van een afschrift van de beschikking op aanvraag door het bevoegd gezag aan het college (artikel 6.13 Bor).
- Het toezenden van de aanvraag voor een activiteit binnen een hogedrempelinrichting en de bijbehorende (persoons)gegevens en bescheiden door het bevoegd gezag aan de burgemeester voor zover de inrichting geheel of gedeeltelijk gelegen is in de gemeente (artikel 6.15, eerste lid, Bor).
- Het toezenden van een afschrift van een omgevingsvergunning voor een BRZO-inrichting door het bevoegd gezag aan het college (artikel 6.15, tweede lid, Bor).
- Het toezenden van (een samenvatting van) de risicoanalyse door het bevoegd gezag aan de burgemeester, voor zover de betreffende inrichting geheel of gedeeltelijk is gelegen in de gemeente (artikel 6.16 Bor).
- Het toezenden van het veiligheidsrapport door het bevoegd gezag aan de burgemeester van de gemeente die kan worden getroffen door een zwaar

ongeval bij een inrichting waarop het veiligheidsrapport betrekking heeft (artikel 6.17, eerste lid, Bor).

Inspectieview Milieu

Vanaf 1 januari 2018 bestaat de mogelijkheid voor toezichthouders en vergunningverleners om gebruik te maken van de zgn. Inspectieview Milieu. Dit is ingevoerd met het *Besluit verbetering vergunningverlening, toezicht en handhaving*. Deze nieuwe manier van gegevensuitwisseling is opgenomen in artikel 7.8-7.12 van het Bor en dient ter uitwerking van de bovengenoemde mogelijkheid (of eigenlijk verplichting) om gegevens te delen in verband met de handhaving van de Wabo.

In de toelichting bij het Besluit wordt de Inspectieview Milieu als volgt omschreven:

“Inspectieview Milieu is een beveiligde website die vooral toezichthouders, maar ook vergunningverleners in staat stelt via een gestandaardiseerd format informatie over (toezicht)objecten te raadplegen die afkomstig is van de database van andere inspectie- en omgevingsdiensten. Het systeem voorziet in de mogelijkheid van enkelvoudige bevraging, maar ook in de mogelijkheid van bulkbevraging. In het eerste geval worden de inspectiegegevens van één enkel bedrijf door een inspecteur opgevraagd en bekeken. Dat kan zijn vanwege een vergunningaanvraag, een melding of het voorbereiden van een concrete toezichtactie. In het tweede geval wordt informatie door een analist opgevraagd, bijvoorbeeld over een groep bedrijven binnen een bepaalde branche of binnen een bepaalde regio, voor de analyse en selectie ten behoeve van de prioritering van inspecties.” (Stb. 2017, 193, p. 16)

Hierbij moet opgemerkt worden dat de Inspectieview slechts een tool is om gegevens onderling uit te wisselen:

“Het systeem wordt uitsluitend gebruikt voor het voor elkaar toegankelijk maken van gegevens. Met Inspectieview Milieu wordt geen dossier opgebouwd, maar kunnen gegevens worden opgevraagd en ingezien. Inspectieview Milieu voorziet niet in de mogelijkheid om gegevens op te slaan of te bewaren. Na bevraging verdwijnen de opgevraagde gegevens uit Inspectieview Milieu. De gegevens, belegd bij inspectie- en omgevingsdiensten door het bevoegde gezag, blijven aanwezig in de eigen database van die diensten en zijn opnieuw opvraagbaar.” (Stb. 2017, 193, p. 16)

Geheimhoudingsplicht

De Wabo, het Bor en de Ror bevatten geen specifieke geheimhoudingsplicht.

Doelbinding

In de Wabo is geen specifiek doelbindingsbeginsel opgenomen. Rekening moet worden gehouden met het algemene doelbindingsbeginsel uit artikel 5 lid 1 sub b en 6 lid 4 AVG.

De vraag is dan of gegevens verkregen op grond van de Wabo (en het Bor en de Ror) ook kunnen worden geraadpleegd ter bestrijding van ondermijning. Op voorhand is lastig in te zien hoe de bestrijding van ondermijning zich verhoudt tot het doel van de Wabo, te weten het samenvoegen van regels omtrent de fysieke leefomgeving.

Conclusie

- De Wabo (alsmede het Bor en de Ror) regelt de samenvoeging van regels omtrent de fysieke leefomgeving, waarbij onder meer regels worden gesteld over de toestemming om te slopen, te bouwen, op te richten of grond (in strijd met het bestemmingsplan) te gaan gebruiken.
- De Wabo kent geen specifieke bepalingen omtrent geheimhouding of doelbinding.

De ratio achter de bestrijding van ondermijning en achter de Wabo verschillen dusdanig van elkaar, dat op voorhand lastig denkbaar is in welke gevallen de bestrijding van ondermijning verenigbaar is met doel waarvoor gegevens op grond van de Wabo zijn verkregen. In specifieke gevallen kan wellicht tot een andere conclusie worden gekomen.

L. Participatiewet

Doelstelling

De Participatiewet (hierna: Pw) vervangt de Wet werk en bijstand, de Wet sociale werkvoorziening en een gedeelte van de oude Wajong. De Pw bundelt de regelingen op het terrein van werk en inkomen. Het college van burgemeester en wethouders (hierna: het college) is verantwoordelijk voor verschillende taken, waaronder het vaststellen van het recht op bijstand, het verlenen van individuele inkomenstoeslag en het verlenen van tijdelijke ontheffing van de arbeidsverplichting (artikelen 43/44, 36 en 9 Pw). Bij de uitvoering van de Pw spelen onder meer het college, het UWV en de SVB een belangrijke rol. De Pw biedt specifieke verwerkingsgrondslagen, gekoppeld aan bijbehorende geheimhoudingsplichten en doelbindingsprincipes. Deze onderwerpen komen hierna achtereenvolgend aan de orde.

Wettelijke grondslag

De Pw bevat verschillende bepalingen over de uitwisseling van gegevens, waaronder begrepen persoonsgegevens als bedoeld in de Algemene verordening gegevensbescherming (hierna: AVG).⁶² Meer in het bijzonder gaat het daarbij om de artikelen 17 en 53a (inlichtingenplicht belanghebbende), 47e (gegevensverstrekkingen aan en door de Sociale Verzekeringsbank), 63 (inlichtingen van werkgever), 64 (inlichtingen van instanties), 66 (vermoeden misdrijf) en 67 (inlichtingen door college) Pw.

De verwerking van gegevens voor, kort gezegd, de aanpak van ondermijnende criminaliteit zal niet kunnen worden gebaseerd op de artikelen 17, 53a, 63 en 64 Pw, nu die artikelen verstrekking van anderen, buiten de gemeente, *aan* de gemeente (het college) mogelijk maken.⁶³ Ook artikel 47e Pw zal geen uitkomst bieden, reeds omdat geen verstrekking aan de SVB is beoogd.

Aan de artikelen 66 en 67 Pw besteden wij nadere aandacht. Artikel 66 verplicht het college ertoe om het "betrokken orgaan" ervan in kennis te stellen als er een gegrond vermoeden bestaat dat een misdrijf is gepleegd ten nadele van, voor zover van belang, i) een uitvoeringsorgaan van de sociale verzekeringswetten of ii) een overheidsorgaan, voorzover dit is belast met het verrichten van uitkeringen, het doen van verstrekkingen dan wel het heffen van bijdragen. Een team of afdeling binnen de gemeente dat verantwoordelijk is voor het bestrijden van ondermijning (hierna ook:

⁶² Zie artikel 6a Pw: "In deze wet en de daarop berustende bepalingen wordt onder gegevens mede verstaan persoonsgegevens als bedoeld in de Algemene verordening gegevensbescherming."

⁶³ Een uitzondering hierop geldt voor artikel 53 lid 6 Pw, dat het college de bevoegdheid geeft om zo nodig onderzoek in te stellen naar gegevens die noodzakelijk zijn voor de verlening dan wel de voortzetting van bijstand. Deze bepaling lijkt geen ruimte te bieden voor binnengemeentelijke gegevensuitwisseling ter bestrijding van ondermijning, omdat de bepaling is gericht op de vaststelling van aanspraken van betrokkenen op basis van de Pw.

een ondermijningsteam) lijkt niet als een dergelijk betrokken orgaan te kunnen worden aangemerkt. Om die reden zal ook artikel 66 Pw geen soelaas kunnen bieden.

Artikel 67 Pw geeft het college de bevoegdheid om uit de administratie terzake van de uitvoering van de Pw aan verschillende instanties gegevens te verstrekken. Die instanties zijn genoemd in het eerste lid, samen met het doel waarvoor de gegevens aan de betreffende instanties verstrekt mogen worden. De ontvangers zijn:

- het UWV en de SVB;
- de Belastingdienst;
- het college van andere gemeenten (voor de uitvoering van de Pw, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers en de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen);
- het CAK, de Nederlandse Zorgautoriteit, zorgverzekeraars en Wlz-uitvoerders;
- derden die in het kader van de uitoefening van beroep op bedrijf de arbeidsinschakeling van personen bevorderen;
- buitenlandse organen (voor de vervulling van een taak van zwaarwegend algemeen belang);
- bestuursorganen van Aruba, Curaçao, en Sint Maarten (voor de vervulling van een taak van zwaarwegend algemeen belang);
- de minister van Sociale Zaken en Werkgelegenheid (voor de uitvoering van de Wet inburgering);
- de minister van Veiligheid en Justitie (in verband met de tenuitvoerlegging van vrijheidsstraffen en vrijheidsbenemende maatregelen).

Op grond van het eerste lid zullen ten behoeve van de aanpak van ondermijning door de gemeente dus geen gegevens mogen worden verstrekt. Mogelijk zou lid 5 van artikel 67 Pw op termijn echter uitkomst kunnen bieden. Op grond van dat lid kunnen bij algemene maatregel van bestuur namelijk andere instanties dan genoemd in het eerste lid worden aangewezen. Een dergelijke amvb is er nu nog niet, maar daarop zou wel aangestuurd kunnen worden.⁶⁴ Dit mede tegen de achtergrond dat aan *buitenlandse* organen (wel) Pw-gegevens kunnen worden verstrekt voor de vervulling van een taak van zwaarwegend algemeen belang.

Verder wijzen wij volledigheidshalve op artikel 76a Pw, waarin is bepaald dat het college bij besluit ambtenaren kan aanwijzen die met de toezicht op de naleving van de Pw zijn belast. Het biedt geen oplossing deze toezichthouder (ook) onderdeel uit te laten maken van het ondermijningsteam, omdat de gegevens waarover die persoon in

⁶⁴ In het concrete geval zou dan wel nog moeten worden nagegaan of, kort gezegd, degene van het ondermijningsteam die de gegevens ontvangt, bevoegd is te achten de gegevens te verkrijgen, zie artikel 65 lid 4 Pw.

zijn toezichthoudende rol beschikt, gelet op de strikte geheimhoudingsplicht van artikel 65 Pw (zie hierna), geheim zal moeten blijven.

Vraag is tot slot nog of kan worden teruggevallen op de grondslagen uit artikel 6 van de AVG. Dat zal gelet op de strikte geheimhoudingsplicht van artikel 65 Pw, waarop wij in het volgende onderdeel nog verder in gaan, slechts het geval zijn als de betrokkene toestemming heeft gegeven in de zin van artikel 6 lid 1 aanhef en onder a AVG en, als sprake zou zijn van bijzondere persoonsgegevens of strafrechtelijke persoonsgegevens⁶⁵, van uitdrukkelijke toestemming als bedoeld in artikel 9 lid 2 aanhef en onder a AVG jo. artikel 22 lid 2 aanhef en onder a Uitvoeringswet AVG (hierna: UAVG; voor bijzondere persoonsgegevens) respectievelijk artikel 32 aanhef en onder a UAVG (voor strafrechtelijke persoonsgegevens). Toestemming kan slechts een grondslag vormen indien sprake is van een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting (artikel 4 aanhef en onder 11 AVG). Van een vrije toestemming zal i.c. doorgaans geen sprake zijn, omdat de betrokkene in een afhankelijkheidsrelatie verkeert ten opzichte van de overheid. Dit nog afgezien van de vraag of een betrokkene bereid zou zijn toestemming te geven voor een gegevensverwerking waarvan hij of zij mogelijk nadeel zal ondervinden. Een andere optie zou kunnen zijn een wettelijke verplichting als bedoeld in artikel 6 lid 1 aanhef en onder c AVG. Met een dergelijke wettelijke verplichting zijn wij echter niet bekend.

Volledigheidshalve merken wij op dat als toestemming in een voorkomend geval (toch) als grondslag kan gelden, die toestemming dan óók zo zou kunnen worden begrepen dat de betrokkene geen bezwaar heeft tegen verstrekking van de gegevens. Dat is een doorbrekingsgrond van de geheimhoudingsplicht van artikel 65 Pw (zie hierna). Blijkens artikel 65 lid 4 Pw zal dan wel nog steeds moeten worden nagegaan of, kort gezegd, de ontvanger (de aangewezen persoon uit het ondermijningsteam) bevoegd is te achten de gegevens te verkrijgen.

Geheimhoudingsplicht

Artikel 65 Pw bevat een strikte geheimhoudingsplicht. Het is blijkens het eerste lid een ieder verboden om hetgeen hem uit of in verband met enige werkzaamheid bij de uitvoering van de Pw over de persoon of zaken van een ander blijkt of wordt meegedeeld, verder bekend te maken dan voor de uitvoering van de Pw noodzakelijk is (die situatie zal zich bij de beoogde verstrekking ten behoeve van de aanpak van ondermijning naar verwachting niet voordoen) dan wel op grond van de Pw is voorgeschreven of toegestaan (zoals hiervoor is beschreven is dat op dit moment niet het geval, maar zou dat anders kunnen worden als de verstrekkingmogelijkheid bij amvb zou worden geregeld).

⁶⁵ In artikel 9 AVG worden de bijzondere persoonsgegevens genoemd en in artikel 10 AVG strafrechtelijke persoonsgegevens.

De geheimhoudingsplicht kan blijkens het tweede lid worden doorbroken als i) enig wettelijk voorschrift tot bekendmaking verplicht, ii) degene op wie de gegevens betrekking hebben schriftelijk heeft verklaard tegen de verstrekking van gegevens geen bezwaar te hebben, of tot slot iii) de gegevens niet herleidbaar zijn tot individuele natuurlijke personen. De enige relevante uitzondering is die beschreven achter ii (geen bezwaar tegen verstrekking). Het is echter de vraag of een betrokkene bereid zou zijn toestemming te geven voor een gegevensverwerking waarvan hij of zij mogelijk nadeel zal ondervinden. Zou dat wel het geval zijn, dan bepaalt het vierde lid van artikel 65 Pw nog dat degene die op grond van, voor zover van belang, artikel 67 lid 5 en 65 lid 2 Pw gegevens verstrekt, moet nagaan of de ontvanger (de aangewezen persoon uit het ondermijningsteam) redelijkerwijs bevoegd is te achten om die gegevens te verkrijgen.

Het voorgaande neemt volgens ons niet weg dat het in zeer uitzonderlijke omstandigheden (conflict van plichten) toch mogelijk kan zijn om de geheimhoudingsplicht te doorbreken c.q. de gegevens verder te verwerken. Hierbij kan gedacht worden aan bijvoorbeeld levensgevaar of een zeer ernstig strafbaar feit.

De vraag zou nog kunnen rijzen of dat-informatie ('deze betrokkene is binnen het Participatiewet-domein bekend'), anders dan wat-informatie ('deze betrokkene maakt op grond van a, b en c aanspraak op x'), wellicht niet onder het bereik van de geheimhoudingsplicht valt, waarbij de redenering dan zou zijn dat de geheimhoudingsplicht zo moet worden uitgelegd dat deze slechts ziet op gegevens die de betrokkene zelf heeft verstrekt.⁶⁶ Wij achten de kans dat een dergelijke redenering zou slagen klein. Zou die redenering toch stand houden, dan zou vervolgens nog moeten worden beoordeeld of er een grondslag is voor de verstrekking in de zin van de AVG. Vraag is dan of verstrekking van de dat-informatie kan worden gebaseerd op artikel 6 lid 1 AVG – dat zal vermoedelijk niet het geval zijn, omdat de verstrekking niet de publieke (Participatiewet-)taak van de verstrekker zal dienen – of een verenigbare verdere verwerking vormt in de zin van artikel 6 lid 4 AVG. Bij de verstrekking van gegevens die zijn verkregen op grond van de Pw ten behoeve van de bestrijding van ondermijning valt lastig vol te houden dat sprake is van een verenigbare verdere verwerking. Daarvan zou bijvoorbeeld eerder sprake kunnen zijn bij (gegevens verkregen op grond van de Drank- en Horecawet (hierna: DHW), omdat de doelstellingen van de DHW meer raken aan het voorkomen van ondermijning, dan de doelstellingen van de Pw.

Volledigheidshalve merken wij op dat college desgevraagd wel Participatiewet-gegevens kan verstrekken aan het Landelijk Bureau Bibob. Dat betekent dat in het kader van een Bibob-onderzoek wel acht kan worden geslagen op relevante gegevens die zijn verkregen op basis van de Pw. Voorwaarde daarvoor is dat de gegevens

⁶⁶ Vgl. *Kamerstukken II* 2002/03, 28 870, nr. 3, p. 81: "Degenen die betrokken zijn bij de uitvoering van deze wet dragen kennis van persoonlijke informatie van degenen die bijstand aanvragen of ontvangen dan wel gebruik maken van een reïntegratietraject."

noodzakelijk zijn voor de uitoefening van de taak van het Bureau (artikel 27, lid 1, onder g, Wet Bibob) en geen van de uitzonderingen op deze verstrekingsgrondslag aan de orde is (zoals een zwaarwegend belang van het college bij het niet-verstrekken van de gegevens).

Ook gegevens die worden verwerkt voor de uitvoering van de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers en de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen kunnen desgevraagd aan het Landelijk Bureau Bibob worden verstrekt.

Doelbinding

De hiervoor beschreven geheimhoudingsplicht kleurt naar ons oordeel het doelbindingsbeginsel in. De Pw-gegevens zullen alleen verder mogen worden verwerkt voor de aanpak van ondermijning als dat in een op artikel 67 lid 2 Pw gebaseerde amvb wordt geregeld (artikel 67 lid 5 Pw) of als de betrokkene toestemming geeft (artikel 65 lid 2 Pw) én de ontvanger (de aangewezen persoon uit het ondermijningsteam) bevoegd is te achten de gegevens te verkrijgen.

Conclusie

- Het college is op grond van de Pw verantwoordelijk voor verschillende taken, waaronder het vaststellen van het recht op bijstand, het verlenen van individuele inkomensvoorziening en het verlenen van tijdelijke ontheffing van de arbeidsverplichting;
- Vanwege de geheimhoudingsbepaling van artikel 65 Pw zijn de mogelijkheden om Pw-gegevens te gebruiken ter bestrijding van ondermijning op dit moment beperkt;
- Er zal binnen het huidige stelsel van de Pw sprake zijn van een wettelijke grondslag voor de verstrekking van Pw-gegevens voor de aanpak van ondermijnende criminaliteit (en derhalve voor verstrekking aan de aangewezen persoon uit het ondermijningsteam) als dat in de in artikel 67 lid 5 Pw bedoelde amvb zou worden geregeld of als de betrokkene schriftelijk toestemming voor de verstrekking geeft (artikel 65 lid 2 Pw) én de ontvanger (de aangewezen persoon uit het ondermijningsteam) bevoegd is te achten de gegevens te verkrijgen (artikel 65 lid 4 Pw).
- Deze conclusie volgt (mede) uit de geheimhoudingsbepaling van artikel 65 Pw, welke bepaling ook het doelbindingsbeginsel inkleurt.
- Het Landelijk Bureau Bibob kan in het kader van zijn adviestaak wel gegevens verwerken die het college in verband met de Participatiewet verwerkt.

M. Wet maatschappelijke ondersteuning 2015

Doelstelling

Op grond van de Wet maatschappelijke ondersteuning 2015 (hierna: Wmo 2015) is de gemeente verantwoordelijk voor de maatschappelijke ondersteuning van haar inwoners op het gebied van zelfredzaamheid en participatie. Vanzelfsprekend verwerkt het college hierbij tal van persoonsgegevens, waaronder bijzondere (medische) persoonsgegevens.

Wettelijke grondslag

Algemene verwerkingsgrondslagen

Het Advies- en Meldpunt Kindermishandeling (hierna: AMHK)⁶⁷ is op grond van artikel 4.2.12 Wmo 2015 verplicht kosteloos gegevens aan het college te verstrekken ten behoeve van de verwerking als bedoeld in de artikelen 7.4.0 lid 1 en 7.4.1 lid 1 en 2 Jeugdwet (hierna: Jw) (kort gezegd: bepaalde jeugdwet-taken resp. beleid). Het kan daarbij ook gaan om persoonsgegevens, waaronder bijzondere persoonsgegevens en het burgerservicenummer (zie artikel 4.2.12 Wmo 2015 lid 2 jo. artikel 7.4.4 Jw).

Artikel 5.1.1 Wmo 2015 biedt het college de wettelijke grondslag voor de verwerking van bepaalde persoonsgegevens, over bepaalde personen en ten behoeve van bepaalde doelen (die verband houden met de uitvoering van Wmo-taken), soms gekoppeld aan bepaalde voorwaarden (zoals ondubbelzinnige toestemming van de betrokkene, bijvoorbeeld als het gaat om gegevens die het college heeft verkregen ten behoeve van de uitvoering van de taken die bij of krachtens de Jeugdwet, de Participatiewet en de Wet gemeentelijke schuldhulpverlening aan het college zijn opgedragen). Een en ander is uitgewerkt in artikel 5.1.1 Wmo 2015.

Artikel 5.1.5 Wmo 2015 biedt aan de toezichthoudende ambtenaren een grondslag om bepaalde persoonsgegevens over bepaalde personen te verwerken die noodzakelijk zijn voor een goede uitoefening van het toezicht of het nemen van maatregelen ter handhaving van wettelijke voorschriften. Met het toezicht is bedoeld het toezicht op de naleving van het bij of krachtens de Wmo 2015 bepaalde (artikel 4.3.1, 6.1 of 6.2 Wmo 2015). Hoewel het begrip 'wettelijke voorschriften' in de wet niet nader is uitgewerkt en daar ook in de parlementaire geschiedenis geen (expliciete) aandacht aan is besteed, moet naar ons oordeel worden aangenomen dat het ook bij wettelijke voorschriften gaat om het bij of krachtens de Wmo 2015 bepaalde, nu de

⁶⁷ Tegenwoordig heet het AMHK 'Veilig Thuis'. Omdat de wet nog wel spreekt van het AMHK doen wij dat ook in dit advies.

toezichthoudende ambtenaren juist zijn belast met het toezicht op de naleving van de Wmo 2015.⁶⁸

Hierna zal verder steeds worden gesproken over “noodzakelijk zijn voor een goede uitoefening van het toezicht of het nemen van maatregelen ter handhaving van wettelijke voorschriften”. Daarmee is dan het bovenstaande bedoeld.

De toezichthoudende ambtenaren zijn, voor zover dat voor de vervulling van hun taak noodzakelijk is en in afwijking van artikel 5:20, tweede lid, van de Algemene wet bestuursrecht, bevoegd tot inzage in dossiers.

Verstreking van gegevens aan het college

Op grond van artikel 5.2.4 lid 3 Wmo 2015 zijn de toezichthoudende ambtenaren bevoegd uit eigen beweging en desgevraagd verplicht persoonsgegevens, waaronder persoonsgegevens betreffende de gezondheid, die zijn verkregen ten behoeve van de uitoefening van het toezicht, bedoeld in artikel 6.1 Wmo 2015, te verstrekken aan het college, voor zover deze noodzakelijk zijn voor de uitvoering van de collegetaken genoemd in artikel 2.1.4, 2.1.5, 2.3.6, 2.3.9, 2.3.10 of 2.4.3 Wmo 2015.

Daarnaast zijn er nog een aantal andere partijen bevoegd om ten behoeve van bepaalde doelen bepaalde persoonsgegevens aan het college te verstrekken. Zie voor de wettelijke grondslagen en uitwerking daarvan de volgende artikelen in Wmo 2015:

- artikel 5.2.2 (aanbieder die een maatwerkvoorziening levert + een derde aan wie ten laste van een persoonsgebonden budget (PGB) betalingen worden gedaan);
- artikel 5.2.3 (rijksbelastingdienst);
- artikel 5.2.4 (CAK + de instantie die in de (gemeentelijke) verordening is aangewezen als instantie die de bijdragen voor een maatwerkvoorziening dan wel een PGB voor opvang vaststelt en int + de SVB);
- artikel 5.2.5 (zorgverzekeraar + zorgaanbieder als bedoeld in de Zorgverzekeringswet + CIZ).

Verstreking van gegevens door het college

Artikel 5.2.1 Wmo 2015 bevat een grondslag voor het college om bepaalde persoonsgegevens aan bepaalde derden te verstrekken ten behoeve van bepaalde doelen. Het gaat daarbij onder meer om toezichthoudende ambtenaren, aan wie het college de in lid 1 van het artikel bedoelde persoonsgegevens mag verstrekken voor

⁶⁸ Hierna zal verder steeds worden gesproken over “noodzakelijk zijn voor een goede uitoefening van het toezicht of het nemen van maatregelen ter handhaving van wettelijke voorschriften”.

zover die gegevens noodzakelijk zijn voor een goede uitoefening van het toezicht of het nemen van maatregelen ter handhaving van wettelijke voorschriften.

Geheimhoudingsplicht

De Wmo 2015 kent een strikte geheimhoudingsplicht (artikel 5.3.3 Wmo 2015). Blijkens het eerste lid is het – tenzij sprake is van toestemming van de betrokkene⁶⁹ – het college, een aanbieder, een derde aan wie ten laste van een persoonsgebonden budget betalingen worden gedaan, het CAK en een andere instantie als bedoeld in artikel 2.1.4, zevende lid Wmo 2015, de Sociale verzekeringsbank, toezichthoudende ambtenaren en het AMHK verboden aan anderen dan de betrokkene⁷⁰ inlichtingen over betrokkene, dan wel inzage in of afschrift van de bescheiden te verstrekken.

Voor de toezichthoudende ambtenaren kan daar nog een afgeleide geheimhoudingsplicht aan worden toegevoegd (artikel 6.1 lid 3 Wmo 2015). Hierbij geldt dat voor zover de toezichthoudende ambtenaar door inzage in bescheiden bij de vervulling van zijn taak dan wel door verstrekking van gegevens in het kader een melding als bedoeld in artikel 3.4 Wmo 2015 (een calamiteits- of geweldmelding), gegevens, daaronder begrepen bijzondere persoonsgegevens, heeft verkregen, ter zake waarvan de beroepskracht uit hoofde van zijn beroep tot geheimhouding verplicht is, een gelijke verplichting voor de toezichthoudende ambtenaar geldt, onverminderd het bepaalde in artikel 5.2.4 Wmo 2015.

Doelbinding

Voor gegevens verkregen in verband met de Wmo 2015 geldt een strikt doelbindingsprincipe. Om de doelbinding te waarborgen, is, zo staat in de MvT, per actor zo concreet en nauw mogelijk omschreven voor welke specifieke taken gegevensverwerking en gegevensverstrekking is toegestaan. Dat is gebeurd door in Wmo-bepalingen per actor de taak neer te leggen waarvoor gegevensverwerking of gegevensverstrekking mag plaatsvinden. Die artikelen zijn hiervoor in grote lijnen genoemd. Voor andere verwerkingen zal gelet op het doelbindingsprincipe in beginsel geen ruimte zijn.

De vraag naar de mogelijkheid van verdere verwerking en domeinoverstijgend gebruik van gegevens is in de Eerste Kamer (ook) aan de orde gekomen:

⁶⁹ Uit het tweede lid volgt dat indien de betrokkene minderjarig is, in plaats van diens toestemming de toestemming van zijn wettelijke vertegenwoordiger is vereist, indien hij jonger is dan twaalf jaren, of de leeftijd van twaalf jaren heeft bereikt en niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake.

⁷⁰ Het derde lid bepaalt dat onder 'anderen dan betrokkene' niet begrepen zijn degenen van wie beroepshalve de medewerking vereist is bij de uitvoering van de taken van het college, een aanbieder, een derde aan wie ten laste van een persoonsgebonden budget betalingen worden gedaan, het CAK en een andere instantie als bedoeld in artikel 2.1.4, zevende lid Wmo 2015, de Sociale verzekeringsbank, toezichthoudende ambtenaren en het AMHK.

“Als een vraag van verdere verwerking aan de orde komt, is het uitgangspunt in het kader van de decentralisaties (...) nadrukkelijk de hulpvraag. Het is deze hulpvraag die in het concrete geval het doel van het verzamelen en het verdere verwerken van gegevens bepaalt. In het beperkte aantal gevallen dat een hulpvraag zich uitstrekt over meerdere deeldomeinen en waarbij sprake is van multiproblematiek, is het deze hulpvraag die aanleiding geeft tot eventueel domeinoverstijgend gebruik van gegevens. Het gebruik van gegevens moet in relatie staan tot en noodzakelijk zijn voor het beantwoorden van de hulpvraag. In die zin is er dan ook geen sprake van (...) ‘grootschalig gebruik van gegevens’.”⁷¹

Het voorgaande neemt volgens ons niet weg dat het in zeer uitzonderlijke omstandigheden (conflict van plichten) toch mogelijk kan zijn om de geheimhoudingsplicht te doorbreken c.q. de gegevens verder te verwerken. Hierbij kan gedacht worden aan bijvoorbeeld levensgevaar of een zeer ernstig strafbaar feit.

Conclusie

- De Wmo 2015 regelt (onder meer) de gemeentelijke taak voor de maatschappelijke ondersteuning van haar inwoners op het gebied van zelfredzaamheid en participatie;
- In de Wmo 2015 is specifiek geregeld wie voor welke specifieke taken gegevens mag verzamelen en verstrekken. De Wmo 2015 kent geen bepaling om gegevens te verwerken ten behoeve van de bestrijding van ondermijning;
- Daar komt bij dat artikel 5.3.3 Wmo 2015 een geheimhoudingsplicht bevat. Alleen met toestemming van de betrokkene kunnen Wmo-gegevens worden gedeeld met anderen dan de betrokkene en de organisaties die Wmo-voorzieningen uitvoeren. In aanvulling daarop geldt voor de toezichthoudende ambtenaar een afgeleide geheimhoudingsplicht in voorkomende gevallen.
- Mede gezien de strikte geheimhoudingsplicht van artikel 5.3.3 Wmo 2015 is naar onze mening geen sprake van een wettelijke grondslag voor de verstrekking van Wmo-gegevens ten behoeve van de aanpak van ondermijning, tenzij sprake is van toestemming van de betrokkene. Hierbij is ook van belang dat de Wmo 2015 een strikt doelbindingsprincipe kent en het aanpakken van (ondermijnende) criminaliteit niet als een van de doelen wordt genoemd. Het voorgaande is slechts anders wanneer sprake is van een uitzonderlijke omstandigheid, zoals onderzoek naar een zeer ernstig strafbaar feit.

⁷¹ *Kamerstukken II 2013-2014, 33 841, nr. 3, p. 66.*

N. Jeugdwet

Doelstelling

Gemeenten zijn op grond van de Jeugdwet (hierna: Jw) verantwoordelijk voor (de organisatie van) verschillende jeugdzorgtaken. Vanzelfsprekend krijgt het college in dit kader de beschikking over persoonsgegevens, waaronder bijzondere (medische) persoonsgegevens van jeugdigen en andere betrokkenen. De Jw bevat strikte gegevensbeschermingsregels, afhankelijk van de soort gegevens.

Wettelijke grondslagen, geheimhoudingsplichten en doelbinding

Bij de beoordeling van de Jw maken wij een onderscheid naar type (persoons)gegevens:

1. gegevens in het kader van de verwijsindex risicjongeren;
2. gegevens uit het dossier van de jeugdhulpverlener;
3. 'gemeentelijke' gegevens ter uitvoering van de Jeugdwet; en
4. gegevens in het kader van gemeentelijk jeugdwetbeleid.

1. Gegevens in het kader van de verwijsindex risicjongeren

De verwijsindex risicjongeren is een landelijk elektronisch systeem, waarin persoonsgegevens alsmede andere gegevens worden verwerkt (artikel 7.1.2.1 lid 1 Jw). De verwijsindex heeft tot doel vroegtijdige en onderlinge afstemming tussen meldingsbevoegden te bewerkstelligen, opdat zij jeugdigen tijdig passende hulp, zorg of bijsturing kunnen verlenen om daadwerkelijke bedreigingen van de noodzakelijke condities voor een gezonde en veilige ontwikkeling naar volwassenheid te voorkomen, te beperken of weg te nemen (artikel 7.1.2.1 lid 2 Jw). De verwijsindex mag *uitsluitend* worden gebruikt voor dat doel (artikel 7.1.2.1 lid 3 Jw). Daar wordt in artikel 7.1.4.4 Jw nog aan toegevoegd dat de verwerking van gegevens betreffende gezondheid en strafrechtelijke persoonsgegevens *uitsluitend* plaatsvindt om meldingsbevoegden uit de domeinen jeugdgezondheidszorg, gezondheidszorg en politie en justitie in staat te stellen een jeugdige aan de verwijsindex te melden en andere meldingsbevoegden in staat te stellen van deze melding kennis te nemen. Reeds op dit samenstel van bepalingen zal er geen wettelijke grondslag zijn de gegevens, die in het kader van de verwijsindex worden verwerkt, aan een ondermijningsteam te verstrekken ten behoeve van de aanpak van ondermijning.

2. Gegevens uit het dossier van de jeugdhulpverlener

Een jeugdhulpverlener moet op grond van artikel 7.3.8 Jw een dossier inrichten.⁷² Wij gaan daar op in, omdat de jeugdhulpverlener, afhankelijk van de inrichting van het gemeentelijke jeugdstelsel, een gemeentelijke medewerker zou kunnen zijn.

De jeugdhulpverlener mag aan een ander alleen inlichtingen over de jeugdige geven en inzage in of afschrift van het betreffende dossier verstrekken als de jeugdige⁷³ daar toestemming voor verleent aan de jeugdhulpverlener (artikel 7.3.11 lid 1 Jw⁷⁴). Indien verstrekking plaatsvindt, mogen alleen gegevens worden verstrekt voor zover daardoor de persoonlijke levenssfeer van een ander niet wordt geschaad. Als die 'ander' wordt, voor zover van belang, niet gezien degene die rechtstreeks betrokken is bij de verlening van de jeugdhulp en degene die optreedt als vervanger van de jeugdhulpverlener, voor zover de verstrekking noodzakelijk is voor de door hen in dat kader te verrichten werkzaamheden (artikel 7.3.11 lid 2 aanhef en onder a Jw⁷⁵). Hierbij dient het te gaan om andere hulpverleners die ingeschakeld zijn en daadwerkelijk werkzaamheden verrichten bij de verlening van die *specifieke* hulp aan de jeugdige.

Er zijn wel uitzonderingen op deze geheimhoudingsplicht mogelijk. Naast de hiervoor al genoemde toestemming, is er een aantal gronden op basis waarvan de geheimhoudingsplicht van de jeugdhulpverlener kan worden doorbroken en dus informatie over de jeugdige aan een ander kan worden verstrekt:

- Als het belang van de jeugdige vereist dat informatie aan een ander wordt verstrekt (artikel 7.3.2 lid 3 Jw⁷⁶);
- Als er een wettelijke verplichting op de jeugdhulpverlener rust om informatie te verschaffen (artikel 7.3.11 lid 1 Jw⁷⁷ respectievelijk artikel 7:457 BW lid 1);
- Als sprake is van een zogenaamd conflict van plichten c.q. van een overmachtsituatie;

De jeugdhulpverlener mag zijn geheimhoudingsplicht doorbreken als dat noodzakelijk is om een belang te dienen dat zwaarder weegt dan het belang dat met de

⁷² Het gaat hier om jeugdhulp zónder dat sprake is van een geneeskundige behandelingsovereenkomst. Als wel van een geneeskundige behandelingsovereenkomst sprake is, geldt een zelfde dossierplicht, maar dan op grond van artikel 7:454 BW.

⁷³ In bepaalde gevallen is de toestemming van bijvoorbeeld de met het gezag belaste ouders vereist. Zie artikel 7.3.15 Jw / 7:465 BW.

⁷⁴ Zie artikel 7:457 als sprake is van een geneeskundige behandelingsovereenkomst. Op de BIG-geregistreerde professionals is bovendien artikel 88 van de Wet BIG van toepassing. Op grond van dat artikel is eenieder die zorg verleent op het gebied van de individuele gezondheidszorg verplicht tot geheimhouding van datgene wat hem in de uitvoering van het beroep is toevertrouwd.

⁷⁵ Zie artikel 7:457 lid 2 BW als sprake is van een geneeskundige behandelingsovereenkomst.

⁷⁶ Zie artikel 7:448 lid 3 BW als sprake is van een geneeskundige behandelingsovereenkomst.

⁷⁷ Zie artikel 7:457 lid 1 BW als sprake is van een geneeskundige behandelingsovereenkomst.

geheimhouding is gediend. De jeugdhulpverlener moet zelf afwegen of sprake is van een conflict van plichten en welk belang hij laat prevaleren. Een conflict van plichten mag niet snel worden aangenomen; het betreft hoogst uitzonderlijke situaties.⁷⁸ Er zal moeten zijn voldaan aan de eisen van proportionaliteit en subsidiariteit. Zo moet bijvoorbeeld alles in het werk zijn gesteld om toestemming tot doorbreking van het geheim te verkrijgen. Verder zal het niet doorbreken van het geheim een ernstig nadeel moeten opleveren en moet doorbreking van de geheimhoudingsplicht dat nadeel kunnen voorkomen of beperken. Daarnaast mag er geen andere weg zijn dan doorbreking van het geheim om het probleem op te lossen.

- Als sprake is van een zwaarwegend belang.

Een andere uitzonderingsgrond betreft de aanwezigheid van een zwaarwegend belang, zonder dat zich (direct) een conflict van plichten aandient. Als er voldoende concrete aanwijzingen zijn dat door handhaving van de geheimhoudingsplicht een ander zwaarwegend belang wordt geschaad en het medisch dossier of de inlichting opheldering kan verschaffen, welke opheldering niet op andere wijze kan worden verkregen, dan zal de geheimhoudingsplicht mogen worden doorbroken.⁷⁹ Een voorbeeld kan zijn de verdediging van de jeugdhulpverlener in een straf- of tuchtzaak. Ook kan gedacht worden aan de situatie dat de gegevensverwerking noodzakelijk is ter bescherming van een vitaal belang van de betrokkene (vgl. artikel 6 lid 1 sub d AVG).

Gelet op deze uitzonderingsmogelijkheden is dus niet uitgesloten dat het in zeer uitzonderlijke situaties ook mogelijk is om buiten het kader van de hulpvraag persoonsgegevens te verwerken. Gedacht kan bijvoorbeeld worden aan levensgevaar of een zeer ernstig strafbaar feit.

3. Gemeentelijke gegevens ter uitvoering van de Jeugdwet

De Jeugdwet geeft in artikel 7.4.0 Jw een grondslag aan, voor zover van belang, (een door) het college (aangewezen persoon) om (bijzondere) persoonsgegevens over de jeugdige en zijn ouders te verwerken voor die gegevens noodzakelijk zijn voor:

- de toeleiding naar, advisering over, bepaling van of het inzetten van een voorziening op het gebied van de jeugdhulp;
- het doen van een verzoek tot onderzoek bij de raad voor de kinderbescherming of de uitvoering van kinderbeschermingsmaatregelen of jeugdreclassering;

⁷⁸ *Kamerstukken II* 1989-90, 21 561, nr. 3, p. 40.

⁷⁹ Zie HR 20 april 2001, *NJ* 2001, 600.

- de bekostiging van preventie, jeugdhulp, kinderbeschermingsmaatregelen, jeugdreclassering of werkzaamheden als bedoeld in de artikelen 6.1.2, zesde lid, 6.1.3, derde lid, en 6.1.4, vierde lid Jw;⁸⁰
- het verrichten van controle of fraudeonderzoek.⁸¹

De verwerking van gegevens voor de aanpak van ondermijnende criminaliteit zal hier niet onder kunnen worden gebracht. De wetgever lijkt ook te hebben beoogd dat de (persoons)gegevens niet voor andere doelen mogen worden verwerkt, tenzij de betrokkene daarvoor toestemming geeft.⁸² Voor wat betreft het derde doel (bekostiging) kan in dit verband worden gewezen op artikel 6a.7 Regeling Jeugdwet, dat bepaalt dat de bekostigingsgegevens slechts mogen worden verwerkt voor zover zij noodzakelijk zijn ten behoeve van het verrichten van formele controle, het betalen van het gedeclareerde bedrag of het zo nodig bij de declarant opvragen van nadere persoonsgegevens. Ten aanzien van het vierde doel (controle of fraudeonderzoek) wijzen wij op artikel 6b.7 Regeling Jeugdwet, dat bepaalt dat het college bij het fraudeonderzoek verkregen gegevens slechts verder verwerkt voor zover dat noodzakelijk is voor het verrichten van werkzaamheden die uit dat onderzoek voortvloeien.

4. Gegevens in het kader van gemeentelijk jeugdwetbeleid

De Jeugdwet geeft in artikel 7.4.1 lid 2 en 7.4.4 Jw een grondslag aan het college voor de verwerking van (persoons)gegevens, waaronder het BSN en bijzondere persoonsgegevens ten behoeve van, kort gezegd, een doelmatig, doeltreffend en samenhangend gemeentelijk beleid ten aanzien van preventie, de toegang tot en verlening van jeugdhulp, de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering en het advies- en meldpunt huiselijk geweld en kindermishandeling. De verwerking van persoonsgegevens mag alleen plaatsvinden voor zover deze gegevens noodzakelijk zijn voor:

- het doelmatig en doeltreffend functioneren van de toegang tot de jeugdhulp, de uitvoering van kinderbeschermingsmaatregelen en jeugdreclassering;

⁸⁰ Zie de artikelen 6a.1 t/m 6a.8 van de Regeling Jeugdwet voor een nadere uitwerking hiervan.

⁸¹ Zie de artikelen 6b.1 t/m 6b.7 van de Regeling Jeugdwet voor een nadere uitwerking hiervan.

⁸² Vgl. *Kamerstukken II* 2013-14, 33 684, nr. 3, p. 71: "Het vereiste van doelbinding houdt in dat persoonsgegevens alleen worden gebruikt voor het doel waarvoor ze verzameld zijn. In hoofdstuk 7 van deze wet wordt omschreven in welke gevallen en voor welke doelen persoonsgegevens verwerkt mogen worden."; *Kamerstukken II* 2013-14, 33 684, F, p. 68 : "Dit betekent dat de gemeenten gebonden zijn aan de regels zoals deze gelden op grond van de Wet bescherming persoonsgegevens, de Jeugdwet en de wetgeving inzake de andere domeinen. Er is geen specifieke wettelijke grondslag voor domeinoverschrijdende uitwisseling van persoonsgegevens, buiten toestemming van de betrokkene."

- het doelmatig en doeltreffend functioneren van de aanbieders van preventie, de jeugdhulpaanbieders, gecertificeerde instellingen en van de raad voor de kinderbescherming;
- de doelmatigheid en doeltreffendheid van het aanbod van preventie, jeugdhulp en gecertificeerde instellingen;
- het waarborgen van de stelselverantwoordelijkheid.

Conclusie

- Op grond van de Jw zijn gemeenten verantwoordelijk voor jeugdzorgtaken.
- De gegevens die in het kader van de verwijsindex worden verwerkt zullen in beginsel niet aan de regisseur ondermijning kunnen worden verstrekt.
- Dat geldt ook voor gegevens uit het dossier van de jeugdhulpverlener, 'gemeentelijke' gegevens ter uitvoering van de Jeugdwet en gegevens in het kader van gemeentelijk jeugdwetbeleid, tenzij de betrokkene daarvoor toestemming geeft of sprake is van de uitzonderlijke situatie van een conflict van plichten / zwaarwegend belang.

O. Wet structuur uitvoeringsorganisatie werk en inkomen

Doelstelling

De Wet structuur uitvoeringsorganisatie werk en inkomen (hierna: Wet SUWI) bevat regels over de uitvoering van de regelingen op het gebied van werk en inkomen en de samenwerking die in dat kader plaatsvindt tussen onder meer het college van burgemeester en wethouders (hierna: het college), het Uitvoeringsinstituut werknemersverzekeringen (hierna: UWV) en de Sociale verzekeringsbank (hierna: SVB). De Wet SUWI maakt het mogelijk dat bij de uitvoering van de Wet SUWI betrokken personen en bestuursorganen samenwerkingsverbanden aangaan – en in dat kader persoonsgegevens met elkaar uitwisselen – ter voorkoming en bestrijding van onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de voorkoming en bestrijding van belasting- en premiefraude en het niet naleven van de arbeidswetten (hierna: bestrijding van sociale zekerheidsfraude). De Wet SUWI biedt in dat kader de mogelijkheid tot het verrichten van een Systeem risico indicatie (hierna: SyRY'-analyse).

Wettelijke grondslag

De Wet SUWI bevat verschillende bepalingen over de uitwisseling van gegevens. In artikel 1, tweede lid, Wet SUWI is bepaald dat onder 'gegevens' mede wordt verstaan persoonsgegevens als bedoeld in de AVG.

Artikel 9 lid 1 Wet SUWI bevat een samenwerkingsverplichting tussen het UWV, de SVB en het college. In het kader van deze samenwerking verstrekken de betrokken partijen elkaar uit eigen beweging en op verzoek alle gegevens en inlichtingen die noodzakelijk zijn (artikel 62 Wet SUWI). De samenwerking genoemd in artikel 9 lid 1 Wet SUWI ziet op de (doeltreffende en klantgerichte) uitvoering van de taken op grond van de Wet SUWI en enkele andere sociale wetten⁸³ en heeft ingevolge artikel 9 lid 2 Wet SUWI ook betrekking op andere taken waarmee de het UWV, de SVB en het college zijn belast. Deze andere taken moeten wel verband houden met de taken op grond van de Wet SUWI en de andere in artikel 9 lid 1 Wet SUWI genoemde wetten. Het gaat dan vooral om de andere taken dan de uitvoering van de Participatiewet en aanverwante wetten met betrekking tot gemeentelijke voorzieningen op grond van andere wetten die de colleges van B&W uitvoeren.⁸⁴ Hierbij kan worden gedacht aan de Wet maatschappelijk ondersteuning (WMO) en de Jeugdwet.

⁸³ Artikel 9, eerste lid, Wet SUWI noemt ook de Participatiewet, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen en de Wet gemeentelijke schuldhulpverlening.

⁸⁴ Kamerstukken II 2007/08, 31 514, nr. 3, p. 32

Een andere samenwerkingsvorm op grond van de Wet SUWI is, kort gezegd, die ter bestrijding van sociale zekerheidsfraude.⁸⁵ Met het oog daarop kunnen de in artikel 64 genoemde bestuursorganen en personen onder omstandigheden persoonsgegevens uitwisselen. Het gaat daarbij op dit moment om het UWV, de SVB, de Belastingdienst, toezichthouders op het beleidsterrein van de minister van Sociale Zaken en Werkgelegenheid (hierna: SZW) en de IND⁸⁶. (Partijen in) het samenwerkingsverband kan (kunnen) de Minister van SZW in dat kader ook vragen het instrument SyRI toe te passen. Met behulp van SyRI kunnen onder bepaalde strikte (wettelijke) voorwaarden⁸⁷ en afhankelijk van de opzet van het onderzoek in kwestie, (persoons)gegevens die partijen in het samenwerkingsverband hebben verkregen en die onder andere zijn verzameld om controle en toezicht te kunnen uitoefenen, met elkaar worden vergeleken. Die vergelijking wordt uitgevoerd door een derde partij, het Inlichtingenbureau⁸⁸, dat de gegevens pseudonimiseert. De vergelijking van gegevens strekt er toe op basis van risico-indicatoren discrepanties tussen de verschillende bestaande gegevens waar te nemen, en op die manier gevallen te selecteren waarin nader onderzoek kan worden gedaan naar de rechtmatigheid van aanspraken op bijvoorbeeld een uitkering.

De Wet SUWI bevat voorts nog enkele andere aan het college gerelateerde verstrekkingbepalingen. Zo kan de Minister van Sociale Zaken en Werkgelegenheid (hierna: SZW) aan het college alle gegevens verstrekken die het nodig heeft voor de goede uitvoering van zijn wettelijke taken (artikel 73 lid 8 Wet SUWI). Verder is het college bijvoorbeeld verplicht tot het desgevraagd verstrekken van gegevens en inlichtingen aan de Inspectie SZW (artikel 42, eerste lid, wet SUWI), en bevoegd (of op verzoek verplicht) gegevens en inlichtingen te verstrekken aan toezichthouders genoemd in artikel 5.4 Besluit SUWI.

Geheimhoudingsplicht

De Wet SUWI kent twee bepalingen inzake geheimhouding waar het college bij de vraag naar binnengemeentelijke uitwisseling ten behoeve van de aanpak van ondermijning rekening mee dient te houden.

Allereerst bevat artikel 74 Wet SUWI een geheimhoudingsplicht voor een ieder die bij de uitvoering van de Wet SUWI de beschikking krijgt over gegevens. Die gegevens mogen niet verder bekend worden gemaakt dan voor de uitvoering van de Wet SUWI noodzakelijk is dan wel op grond van de Wet SUWI is voorgeschreven of toegestaan.

⁸⁵ Het gaat meer precies om voorkoming en bestrijding van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de voorkoming en bestrijding van belasting- en premiefraude en het niet naleven van de arbeidswetten.

⁸⁶ Artikel 64 lid 1 sub d jo. *Stcrt.* 2017, 17799.

⁸⁷ Artikel 64 en 65 Wet SUWI en hoofdstuk 5a Besluit SUWI.

⁸⁸ Zie artikel 1, lid 1 aanhef en onder m Wet SUWI: "de als zodanig door Onze Minister aangewezen instelling die is belast met de coördinatie en dienstverlening ten behoeve van de gemeenten bij de verwerking van gegevens, voor zover dit noodzakelijk is voor de uitvoering van taken op het gebied van sociale zekerheid."

De geheimhoudingsplicht geldt niet indien i) een wettelijke voorschrift tot bekendmaking verplicht, ii) degene op wie de gegevens betrekking hebben schriftelijk heeft verklaard geen bezwaar tegen de verstrekking te hebben of iii) de gegevens niet herleidbaar zijn tot individuele natuurlijke personen (artikel 74, tweede lid, Wet SUWI).

Naast deze 'algemene' geheimhoudingsplicht bevat de Wet SUWI ook nog een aanvullende geheimhoudingsplicht ten aanzien van risicomeldingen die voortkomen uit toepassing van het instrument SyRI. Artikel 65, vierde lid, SUWI bepaalt dat een ieder die krachtens artikel 65 Wet SUWI de beschikking krijgt over in een risicomelding neergelegde gegevens verplicht is tot geheimhouding daarvan met overeenkomstige toepassing van de ten aanzien van die gegevens geldende wettelijke geheimhoudingsplicht. Dit betekent dat de geheimhoudingsplicht van de organisatie die de gegevens heeft verstrekt voor de betreffende SyRI-analyse onverkort van kracht blijft.⁸⁹

Het voorgaande neemt niet weg dat het in zeer uitzonderlijke omstandigheden (conflict van plichten) toch mogelijk kan zijn om de geheimhoudingsplicht te doorbreken c.q. de gegevens verder te verwerken. Hierbij kan gedacht worden aan bijvoorbeeld levensgevaar of een zeer ernstig strafbaar feit.

Doelbinding

De hiervoor beschreven generieke geheimhoudingsplicht van artikel 74 Wet SUWI kleurt naar ons oordeel het doelbindingsbeginsel in. Gegevens die het college op grond van de Wet SUWI heeft verkregen mogen alleen worden verwerkt (bekend gemaakt) voor zover dat voor de uitvoering van de Wet SUWI noodzakelijk is dan wel op grond van de Wet SUWI is voorgeschreven of toegestaan. Dat betekent bijvoorbeeld dat het college gegevens die het op grond van artikel 9 jo artikel 62 Wet SUWI heeft verkregen, alleen mag verwerken voor i) de taken die bij of krachtens de Wet SUWI, de Participatiewet, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze werknemers, de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte gewezen zelfstandigen, de Wet gemeentelijke schuldhulpverlening aan het college zijn opgedragen en ii) de taken die met deze wetten verband houden (artikel 9 jo. artikel 62 Wet SUWI).

Het voorgaande geldt ook voor de gegevens die het college binnen samenwerkingsverbanden gericht op, kort gezegd, de bestrijding van sociale

⁸⁹ Dit betekent bijvoorbeeld dat op gegevens afkomstig van de Belastingdienst de geheimhoudingsplicht van artikel 67 Algemene wet inzake rijksbelastingen van toepassing blijft (*Kamerstukken II* 2012/13, 33 579, nr. 3, p. 39).

zekerheidsfraude heeft verkregen.⁹⁰ Die verkregen gegevens mag het college alleen voor dat doel gebruiken.

Conclusie

- De Wet SUWI bevat diverse grondslagen die het voor het college (onder meer) mogelijk maakt om ter voorkoming en bestrijding van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de voorkoming en bestrijding van belasting- en premiefraude en het niet naleven van de arbeidswetten persoonsgegevens te verwerken.
- Hoewel de bestrijding van ondermijning in het verlengde kan liggen van de voorkoming en bestrijding van dergelijke sociale zekerheidsfraude, lijken de strikte geheimhoudingsbepalingen en de strikte doelbinding van de Wet SUWI een belemmering te vormen voor het binnengemeentelijk uitwisselen van persoonsgegevens die in het kader van de Wet SUWI door het college zijn verkregen ten behoeve van de aanpak van ondermijning.

⁹⁰ Het gaat meer precies om voorkoming en bestrijding van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de voorkoming en bestrijding van belasting- en premiefraude en het niet naleven van de arbeidswetten.