Berenschot

Screening van gemeenteambtenaren

Verkennend onderzoek naar grip op integriteitsrisico's door inzet van screening

mr. I.S. Sloover
mr. L.J. Vellekoop
drs. R.M. Postma

4 april 2018

57387

Berenschot

Screening van gemeenteambtenaren

Verkennend onderzoek naar grip op integriteitsrisico's door inzet van screening

Inhoud **Pagina**

Berenschot

Berenschot

1. Inleiding

1.1 Achtergrond en aanleiding

De maatschappij is constant in ontwikkeling. Dit heeft zijn weerslag op het openbaar bestuur en de kaders rondom integriteit. Deze ontwikkelingen vergen aandacht voor kwetsbare werkprocessen en functies. Uit een analyse van Andersson, Elffers en Felix (2014) in opdracht van BZK[1] kwam naar voren dat flexibilisering van de arbeidsmarkt, informatisering en de veranderende relatie van het openbaar bestuur met de omgeving nieuwe vraagstukken met zich meebrengen op het gebied van integriteit. Zo wordt het lastiger voor organisaties om normen, waarden en regelgeving te borgen en continuïteit in het integriteitsbeleid te behouden. De grenzen tussen publiek, privaat en burger vervagen waardoor ambtenaren in situaties terecht kunnen komen waarin hun integriteit op de proef wordt gesteld. Naast deze ontwikkelingen is ook sprake van een verhoogde aandacht voor de integriteit van de overheid[2] en voor cybersecurity. Incidenten met betrekking tot bewuste of onbewuste datalekken worden in de media breed uitgemeten[3] en vormden de aanleiding voor enkele wetenschappelijke onderzoeken met name gericht op politie en andere opsporingsdiensten.

Deze ontwikkelingen vragen in toenemende mate om bescherming van vertrouwelijke overheidsinformatie en persoonsgegevens tegen ongeautoriseerde toegang en misbruik door werknemers en externen. Met de juiste beveiliging wordt niet alleen de privacy van personen beschermd, maar ook de integriteit van de overheid. De vertrouwelijkheid van informatie wordt met name bewaakt door organisatorische en technische maatregelen. Het sluitstuk van de beveiliging betreft screening van personen die toegang hebben tot vertrouwelijke informatie. Daarbij ligt de primaire verantwoordelijkheid voor informatiebeveiliging en integriteit bij de werkgever, zoals ook is vastgelegd in wet- en regelgeving met betrekking tot ambtelijke rechtsposities en in andere wet- en regelgeving met betrekking tot screening.

Integriteit binnen het veiligheidsdomein

Door decentralisaties in het sociaal domein nemen de taken van gemeenten toe. Ook binnen het veiligheidsdomein nemen gemeentelijke taken toe. Deze taken worden veelal, maar niet uitsluitend, uitgevoerd binnen samenwerkingsverbanden.

---

[1] Rapportage 'Integriteit in ontwikkeling' van Andersson, Elffers & Felix (2014). AEF heeft in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijkrelaties onderzoek gedaan naar de meest urgente integriteitsrisico's in het openbaar bestuur.

[2] Zie het gestegen aantal aanvragen voor de aanwijzing van vertrouwensfuncties hetgeen leidde tot wijziging van de Wiv (zie TK 33 673, nr. 3) & zie het gestegen aantal aanvragen voor VOG: https://www.volkskrant.nl/economie/verklaring-omtrent-gedrag-wordt-populairder-heeft-het-effect~a4456691/

[3] Zie bericht in de Telegraaf van 28 februari 2017 'Corruptie uit beeld: Laatste grote onderzoek dateert alweer van 2005', zie ook https://www.telegraaf.nl/nieuws/67206/corruptie-uit-beeld.

Onder andere binnen de Regionale Informatie en Expertise Centra en Veiligheidshuizen wordt samengewerkt met diverse partners. Daarnaast heeft de gemeente op diverse onderwerpen op het gebied van veiligheid een regierol waar zij nauw samenwerkt met lokale actoren en politie en Openbaar Ministerie (OM). Deze samenwerking gaat gepaard met de uitwisseling van informatie tussen gemeenten en ketenpartners. Het gaat hierbij zowel om vertrouwelijke overheidsinformatie als (bijzondere) persoonsgegevens. De aard van deze gegevens stelt eisen aan de infrastructuur en werkprocessen van gemeenten met betrekking tot informatieveiligheid en integriteit.

Gemeentelijke medewerkers werken soms nauw samen met de politie in een situatie waarin onder andere politie-informatie wordt uitgewisseld. Daardoor is een uitvoeringspraktijk ontstaan waarbij de politie ook externen en medewerkers van samenwerkingspartners screent.[4] De laatste categorie personen zijn bijvoorbeeld medewerkers van het OM, gemeenten en de Landelijke en Regionale Informatie en Expertise Centra (LIEC en RIEC). Voor het screenen van externen en medewerkers van ketenpartners heeft de politie nu geen wettelijke bevoegdheid.

De Tweede Kamer is hierover geïnformeerd waarbij is toegezegd dat deze tijdelijke oplossing blijft bestaan in afwachting van het regelen van een structurele oplossing. De screenings door de politie zijn volgens de toenmalige minister van Veiligheid en Justitie niet alleen een middel om de integriteit en betrouwbaarheid van de medewerkers van de samenwerkingspartners te onderzoeken, maar zijn ook bevorderlijk voor de integrale samenwerking en informatiedeling tussen partijen. Het delen van (politie-)informatie tussen samenwerkingspartners is immers van groot belang voor de aanpak van criminaliteit, aldus de minister.[5]

Mede vanwege deze groter wordende rol van gemeenten bij de aanpak van criminaliteit hebben enkele gemeenten aandacht gevraagd voor een fundamentele discussie over het integriteitsvraagstuk.

1.2 Doelstelling en scope onderzoek

De doelstelling van dit onderzoek is om inzicht te geven in mogelijkheden en knelpunten omtrent screening van gemeentelijke ambtenaren als instrument om integriteitsrisico's te beperken. Op basis hiervan biedt het onderzoek inzicht in mogelijke oplossingsrichtingen met betrekking tot de inzet van bestaande methodieken en de eventuele ontwikkeling van nieuwe methodieken.

De centrale vraagstelling van het onderzoek luidt:

"Hoe kan de gemeentelijke werkgever integriteitsrisico's bij de uitvoering van gemeentelijke taken ten behoeve van het veiligheidsdomein optimaal beperken door de inzet van screeningsmethodieken?"

[4] TK 28 844, 2015-2016 nr. 101, p 1-2.

[5] TK 28 844, 2015-2016 nr. 101, p 2-3.

De onderzoeksvragen zijn als volgt:

1. Over welke instrumenten kan een gemeentelijke werkgever nu reeds beschikken als het gaat om het uitvoeren van screening?

2. Onder welke (rand)voorwaarden kan de gemeentelijke werkgever deze instrumenten inzetten?

De nader uit te zoeken vragen van het onderzoek zijn als volgt geformuleerd:

1. Hebben gemeenten in de praktijk voldoende zicht op risicovolle functies bij de uitoefening van taken ten behoeve van het veiligheidsdomein? Hierbij kan gedacht worden aan de volgende deelvragen:

   a. Wordt het beschikbare instrumentarium om risicovolle functies in beeld te krijgen ten volle benut? Zijn de beschikbare instrumenten om risicoanalyses uit voeren daarbij voldoende toegespitst op risico's in de uitvoering van gemeentelijke taken ten behoeve van het veiligheidsdomein?
   b. Welke (organisatorische en fysieke) maatregelen zetten gemeenten in om de risico's omtrent risicovolle functies te beperken alvorens wordt ingezet op screening?
   c. In hoeverre is er sprake van risicovolle functies en hoe worden risico's en risiconiveaus gedefinieerd?

2. Wordt het bestaande screeningsinstrumentarium ten volle benut gezien de aard van de risicovolle functies?

   a. Wordt er bij de toepassing van de mogelijkheden voor screening onderscheid gemaakt naar het risiconiveau van functies?

3. Op welke wijze organiseren gemeenten de uitvoering van screening, met name gezien de borging van de kwaliteit van de screening en gezien de noodzakelijke bescherming van de persoonlijke levenssfeer?

   a. In welke mate voeren gemeenten screening zelf uit, of laten ze deze uitvoeren door een externe partij (bijvoorbeeld werving- en selectiebureaus, recherchebureaus)?
   b. Op welke wijze kunnen gemeenten de integriteit van gedetacheerde medewerkers bewaken (zoals boa's die via externe bureaus worden ingeleend)?

4. Biedt het beschikbare instrumentarium voor het uitvoeren van risicoanalyses en screening, voldoende mogelijkheden voor de gemeentelijke werkgever om de eigen verantwoordelijkheden waar te maken, mede gezien de veranderingen ten aanzien van gemeentelijke taken en de veranderingen die zich hebben voorgedaan in het veiligheidsdomein, en ook mede gezien de mogelijkheden waarover andere overheidsorganisaties beschikken?

   a. Hoe verhoudt de beschikbaarheid en inzet van screeningsmethodieken en risico's bij gemeenten zich tot de beschikbaarheid en inzet van screeningsmethodieken en risico's bij relevante andere overheidsorganisaties (waaronder de politie)?

5. Indien het beschikbare instrumentarium van de gemeentelijke werkgever nu niet voldoende is, welke mogelijkheden zijn er dan om te komen tot een optimale beperking van de veiligheidsrisico's door middel van de inzet van risicoanalyses en screening? Hierbij kan gedacht worden aan de volgende deelvragen:

a. Is het mogelijk om specifieke risicovolle gemeentelijke functies af te bakenen voor eventuele voordracht tot opnemen in het Besluit justitiële en strafvorderlijke gegevens (Paragraaf 2. Verstrekking ten behoeve van het aannemen en ontslag van personeel), en in het Besluit politiegegevens? Hoe verhouden de risico's van deze functies zich in verhouding tot de huidige aangewezen risicovolle functies in de Bjsg en het Bpg?
b. Bieden de huidige gemeentelijke arbeidsrechtpositieregelingen voldoende basis tot het opdracht geven door de gemeentelijke werkgever tot een verregaandere onderzoeksmethodiek, waarbij gebruik gemaakt wordt van justitiële gegevens, politiegegevens en een gesprek over integriteit met de medewerker wordt aangegaan?
c. Zijn er aanpassingen nodig voor wat betreft de organisatorische inbedding van een goede uitvoering van risicoanalyses en screening?

Scope

De scope van het empirische onderzoek richt zich op de uitvoering van gemeentelijke taken ten behoeve van het veiligheidsdomein[6], mede in relatie tot de samenwerking met ketenpartners en de bijbehorende uitwisseling van vertrouwelijke gegevens.

1.3 Uitvoering onderzoek

In het onderzoek zijn de volgende activiteiten uitgevoerd:

- Het onderzoek is gestart met een documentstudie om zicht te krijgen op het screeningsinstrumentarium dat gemeenten momenteel ter beschikking staat en de bijbehorende randvoorwaarden voor toepassing van het instrumentarium. Daartoe hebben we een documentenstudie gedaan van verschillende handboeken, beleid, wet- en regelgeving, wetenschappelijke artikelen en andere (juridische) publicaties. In bijlage 1 is een lijst van de bestudeerde documenten te vinden.
- Parallel aan deze documentstudie zijn in afstemming met de opdrachtgever aan vier instellingen vragenlijsten verzonden met betrekking tot onder meer de identificatie van risicovolle functies / taken, risico-inventarisatie, risico beperkende maatregelen en beschikbare screeningsmethodieken. Het doel hiervan is om een beeld te kunnen vormen hoe de beschikbaarheid en inzet van screeningsmethodieken en risico's bij gemeenten zich verhoudt tot de beschikbaarheid en inzet van screeningsmethodieken en risico's bij deze instellingen. De

[6] In de praktijk voeren gemeenten diverse taken uit ter bevordering van openbare orde en veiligheid. In enge zin omvat dit de medewerkers van de afdelingen 'openbare orde en veiligheid (OOV)', medewerkers die deelnemen aan samenwerkingsverbanden gericht op OOV (zoals Veiligheidshuizen), en functionarissen met OOV taken waarbij de gemeente opdrachtgever is (met name boa's).

instellingen hebben documenten ten behoeve van het onderzoek beschikbaar gesteld en een vragenlijst ingevuld. Op basis van deze documenten en de vragenlijst is een concepttekst opgesteld en deze is met de contactpersoon van de instelling schriftelijk en/of telefonisch afgestemd. De aan de instellingen gestelde vragen zijn te vinden in bijlage 2.

- Om inzicht te krijgen in de toepassing van het beschikbare screeningsinstrumentarium door gemeenten is in afstemming met opdrachtgever een verkennend onderzoek in de vorm van case studies uitgevoerd bij vijf gemeenten. Bij de selectie van gemeenten is in afstemming met opdrachtgever rekening gehouden met grootte, inschatting van het volwassenheidsniveau op het gebied van integriteit en screening en geografische spreiding. De resultaten van de case studies zijn anoniem verwerkt om vertrouwelijke gemeentelijke informatie te kunnen beschermen.
  - We zijn de case studies begonnen door per gemeente de beschikbare beleidsstukken en overige documentatie op het gebied van integriteit en screening te bestuderen. Daarbij kan gedacht worden aan gedragscodes, sjablonen voor risicoanalyses en resultaten van uitgevoerde risicoanalyses.
  - Vervolgens hebben we interviews afgenomen met medewerkers van de vijf gemeenten. Onder andere is gesproken met gemeentesecretarissen, directeuren veiligheid, medewerkers personeelszaken en medewerkers op het gebied van integriteit/weerbaarheid. Daarbij is gesproken over ‘risicovolle functies’, de inzet van instrumentarium om risico’s te beperken en de behoeften van gemeenten op het gebied van screening. Zie bijlage 3 voor de interviewleidraad die is gehanteerd tijdens de case studies.
  - Na de documentstudie en interviews is de informatie verwerkt in een factsheet die ter feitelijke wederhoor aan de gemeenten is voorgelegd.
- De resultaten van de documentenstudie en case studies zijn geanalyseerd en de bevindingen zijn opgenomen in voorliggende rapportage.

Gedurende het onderzoek heeft periodieke afstemming plaatsgevonden met de begeleidingsgroep en klankbordgroep. Voor een overzicht van de leden van beide groepen zie bijlage 4.

1.4 Leeswijzer

In hoofdstuk 2 wordt een overzicht geboden van het juridische kader dat relevant is voor gemeenten in het kader van screening in het veiligheidsdomein en het instrumentarium dat beschikbaar is om integriteitrisico’s in te perken. In hoofdstuk 3 worden de resultaten van de case studies onder vijf gemeenten en de instellingen gepresenteerd. In hoofdstuk 4 wordt een analyse met bevindingen gemaakt. Ten slotte presenteren we in hoofdstuk 5 onze conclusies.

2. Juridische kaders en instrumenten

2.1 Inleiding

In dit hoofdstuk wordt een overzicht gegeven van het instrumentarium dat gemeenten momenteel ter beschikking staat om als werkgever integriteitsrisico's te beperken bij de uitvoering van gemeentelijke taken ten behoeve van het veiligheidsdomein. Onder 'instrumentarium' vallen diverse instrumenten, waaronder diverse screeningsmethodieken.[7] Voordat deze instrumenten worden toegelicht, wordt eerst op hoofdlijnen stilgestaan bij relevante juridische kaders die van belang zijn bij de inzet van deze instrumenten: de rechtspositie van gemeenteambtenaren, de bescherming van persoonsgegevens, de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de verstrekking van justitiële- en politiegegevens en het instellen van een veiligheidsonderzoek.

2.2 Juridische kaders

2.2.1 Rechtspositie van gemeenteambtenaren

Gemeenten zijn zelf verantwoordelijk voor de eigen informatiebeveiliging en integriteit van de organisatie en diens medewerkers. Om als gemeentelijke werkgever integriteits- en informatiebeveiligingsrisico's bij de uitvoering van gemeentelijke taken binnen het veiligheidsdomein te kunnen beperken, is het van belang om vanuit de rechtspositie van gemeenteambtenaren te bezien welke instrumenten ingezet kunnen worden en welke randvoorwaarden daarbij gelden.

Artikel 125 lid, eerste en tweede lid, van de Ambtenarenwet legt de basis voor de rechtspositie van gemeenteambtenaren. Hierin wordt bepaald dat voorschriften voor gemeenteambtenaren worden vastgesteld over bijvoorbeeld aanstelling, schorsing en ontslag, het onderzoek naar de geschiktheid en de bekwaamheid, bescherming bij de arbeid, overige rechten en verplichtingen en disciplinaire straffen. In een aantal andere bepalingen van de Ambtenarenwet is onder meer vastgelegd dat een (eigen) integriteitsbeleid gevoerd moet worden en een gedragscode voor goed ambtelijk handelen moet worden opgesteld (art. 125quater van de Ambtenarenwet), de verplichting wordt opgelegd om voorschriften te stellen voor het afleggen van een eed of belofte bij aanstelling, en voorschriften gesteld moeten worden ten aanzien van melding, registratie, openbaarmaking en verbieden van nevenwerkzaamheden en melding en registratie van financiële belangen (art.125quinquies, tweede lid, van de Ambtenarenwet) en geheimhouding op te leggen (art.125a lid 3 van de Ambtenarenwet).

Een nadere uitwerking van art. 125 Ambtenarenwet is voor gemeenteambtenaren opgenomen in de rechtspositionele regeling Collectieve Arbeidsvoorwaardenregeling en Uitwerkingsovereenkomst (CARUWO). De CAR omvat de hoofdlijnen van de rechtspositieregelingen voor de gemeenten en is bindend voor alle gemeenten. De arbeidsvoorwaarden in de CAR zijn nader uitgewerkt in de zogenoemde Uitwerkingsovereenkomst (de UWO), waarbij het merendeel van de gemeenten zich

[7] In dit rapport omvat methodiek zowel een methode (zoals gesprek of vragenlijst) als de categorieën van persoonsgegevens waarnaar gevraagd wordt.

heeft aangesloten. Op lokaal niveau kan afgeweken worden van de UWO en/of kunnen er nadere ‘eigen’ gemeentelijke arbeidsvoorwaarden worden vastgesteld, als daarover overeenstemming bestaat in het plaatselijke Georganiseerd Overleg. De G4-gemeenten nemen bijvoorbeeld ten opzichte van de CARUWO een eigen positie in en hebben een eigen regeling.

In het CARUWO wordt bepaald dat de kandidaat kan worden aangenomen na een daartoe door de gemeente gehouden onderzoek waaruit blijkt dat de kandidaat in voldoende mate beschikt over de hoedanigheden tot het verrichten van de hem op te dragen werkzaamheden (art. 2:2 van de CAR). Uit de voorgaande bepaling volgt echter niet op welke wijze een dergelijk onderzoek uitgevoerd moet worden en welke instrumenten hiervoor ingezet kunnen worden. Wel is in art. 2:2 lid 3 CARUWO bepaald dat voor een *aanstelling* als vereiste kan worden gesteld dat de kandidaat in het bezit is van een verklaring omtrent het gedrag (VOG) als bedoeld in de Wet justitiële en strafvorderlijke gegevens (Wjsg). Bij een VOG gaat het om de beoordeling van het gedrag van de kandidaat en het bepalen van het risico voor de samenleving in het geval de kandidaat de taak of de bezigheden gaat verrichten waarvoor de verklaring is gevraagd.

Daarnaast kunnen er op grond van de CAR ‘overige verplichtingen’ aan de ambtenaar worden opgelegd (hoofdstuk 15 CAR). Het gaat hierbij om een aantal ‘overige verplichtingen’, in de vorm van actieve meldingsplichten en gedragsvoorschriften, bijvoorbeeld: de functie nauwgezet en ijverig te vervullen, zich te gedragen als een goed ambtenaar, het melden van nevenwerkzaamheden en financiële belangen en niet persoonlijk gebruik te maken van goederen of diensten van de gemeente.

De mogelijkheid voor gemeentelijke werkgevers om een VOG van medewerkers te verzoeken is per 1 januari 2018 uitgebreid. Aan artikel 2:2 CAR is een nieuw artikellid toegevoegd op grond waarvan de werkgever ook gedurende de aanstelling een recente VOG van medewerkers kan vragen. Ter verduidelijking is opgenomen dat de werkgever in de situaties waarin er sprake is van een functiewijziging, overplaatsing of tewerkstelling van een medewerker om een VOG kan verzoeken.[8]

Op 1 januari 2020 is de invoering van de Wet Normalisatie Rechtspositie Ambtenaren (Wnra) beoogd. Vanaf dat moment wordt op de gemeenteambtenaren het civiele arbeidsovereenkomstenrecht van toepassing (Boek 7, titel 10 van het Burgerlijk Wetboek). In het civiele arbeidsovereenkomstenrecht prevaleert in beginsel de contractsvrijheid tussen partijen. Ook in die situatie geldt echter dat de persoonlijke levenssfeer van de werknemer wordt beschermd, door onder meer art. 10[9] van de Grondwet en art. 8[10] van het Europees Verdrag tot bescherming

[8] Zie de brief van het Landelijk Overleg Gemeentelijke Arbeidsvoorwaarden d.d. 9 oktober 2017: Wijzigingen CAR-UWO artikelen per 1 januari 2018. Ledenbrief nr. 17, CvA/LOGA 17/11.

[9] Art. 10 van de Grondwet: 1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. 2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. 3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

van de rechten van de mens en de fundamentele vrijheden (EVRM). Op grond van art. 8 van het EVRM en art. 10 van de Grondwet is er een expliciete wettelijke grondslag vereist. Dit houdt in dat een verregaandere screening een wettelijke grondslag moet hebben en niet op grond van een overeenkomst kan worden afgedwongen. De Ambtenarenwet 2017 (Stb 2017, 123) voorziet in dezelfde grondslagen als de huidige Ambtenarenwet, zoals hierboven omschreven (paragrafen 2, 3 en 4, van die wet). Als zodanig brengt de normalisatie van de rechtspositie van ambtenaren dan ook geen wezenlijke verandering wat betreft de inzet van instrumenten in het kader van integriteit. De CARUWO als ambtelijke rechtspositieregeling wordt te zijner tijd omgezet in een 'cao gemeenten' met een civielrechtelijk karakter, waarbij de materiële arbeidsvoorwaarden niet of slechts beperkt wijzigen.

2.2.2 Bescherming van persoonsgegevens

Bij de inzet van beschikbare instrumenten door de gemeentelijke werkgever speelt de bescherming van persoonsgegevens als grondrecht van de kandidaat / ambtenaar een belangrijke rol. Dit grondrecht is vastgelegd in art. 8 van het EVRM, art. 8 van het Handvest van de grondrechten van de Europese Unie[11] en is nader ingevuld door richtlijn 95/46/EG ('privacyrichtlijn'). Tot 25 mei 2018 is de Wet bescherming persoonsgegevens(Wbp) van toepassing en na deze datum wordt de bescherming van persoonsgegevens vervangen door de Algemene Verordening gegevensbescherming (AVG).[12]

De doelstellingen en beginselen die aan de privacyrichtlijn ten grondslag lagen, blijven overeind onder de AVG. Het gaat onder meer om: rechtmatigheid van de verwerking, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, integriteit en vertrouwelijkheid en verantwoordingsplicht voor de gemeente. Ook gelden de algemene eisen van noodzaak, proportionaliteit en subsidiariteit van het verwerken van persoonsgegevens. Gedurende de verwerking van persoonsgegevens is de gemeente aan deze (rechts)beginselen gebonden.

De begrippen in de AVG zijn materieel anders omschreven dan in de Wbp en hieronder volgt een korte toelichting op een aantal begrippen.

---

[10] Art. 8 EVRM: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[11] Artikel 8 van het Handvest van de grondrechten van de Europese Unie: 1. Eenieder heeft recht op bescherming van zijn persoonsgegevens. 2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan. 3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd.

[12] Verordening (EU) nr. 2016/679.

Enkele begrippen uit de AVG nader toegelicht

persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan orden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

verwerking: 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.

→Uit bovenstaande beschrijving wordt duidelijk dat het begrip 'verwerking' dus veelomvattend is. Voor elke verwerking is in ieder geval een grondslag in de AVG nodig.

verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; 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: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

→ Indien de gemeente gebruik maakt van een derde partij voor het verwerken van persoonsgegevens, moet de gemeente met deze derde een verwerkersovereenkomst sluiten (art. 28 AVG)

ontvanger: 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 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.

bijzondere categorieën van persoonsgegevens (art. 9 AVG): 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.

→ Op grond van art. 9 van de AVG is het verboden om deze bijzondere gegevens te verwerken, tenzij aan een van de voorwaarden in lid 2 van art. 9 van de AVG is voldaan, bijvoorbeeld dat betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking.

Alvorens persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt dient het voor de betrokkene (de kandidaat) kenbaar en voorzienbaar, dus transparant te zijn dat zijn / haar persoonsgegevens worden verwerkt (art. 8 lid 2 van het EVRM). Voor het rechtmatig verwerken ervan in het kader van een screening door de gemeente moet er een wettelijke grondslag zijn en art.10 van de Grondwet stelt ook deze eis. In artikel 8 van de Wbp en art. 6 van de AVG zijn de grondslagen hiervoor opgesomd. Toestemming is onder de AVG één van die grondslagen net als onder de Wbp, maar de toezichthouder, de Autoriteit Persoonsgegevens (AP), heeft reeds[13] bepaald dat toestemming van de kandidaat voor het verwerken van zijn persoonsgegevens in de 'pre-employment' fase niet als grondslag kan gelden. Er is sprake van een afhankelijkheidspositie van een sollicitant tegenover de beoogd werkgever en van 'vrije toestemming' is dan geen sprake.

Voor het uitvoeren van een screening kan de gemeente op basis van de Wbp een beroep doen op de grond dat de verwerking noodzakelijk is voor de behartiging van de 'gerechtvaardigde belangen' van de gemeente.[14] De AP heeft in een onderzoeksrapport[15] aangegeven dat de gemeente als verantwoordelijke moet voldoen aan de eisen van subsidiariteit en proportionaliteit. Er moet een gerechtvaardigd belang zijn, bijvoorbeeld om het juiste, betrouwbare personeel in dienst te nemen of hebben. Daarnaast moeten de risico's in kaart worden gebracht van de verschillende functiegroepen binnen de organisatie; screenings moeten dus naar aard, inhoud en omvang worden beperkt tot reductie van het risico waarvoor zij worden verricht. Hieronder wordt ook begrepen dat de aard van de gevraagde informatie en de termijn ('terugkijktijd') waarop de screening ziet in verhouding moet staan tot het betreffende risico. Vervolgens moet de gemeente het interne beleid zodanig vormgeven dat risico's worden verkleind of weggenomen door organisatorische maatregelen te nemen. Screening is een sluitstuk op het interne beleid; screening is aanvullend op organisatorische maatregelen. Verder moet de gemeente een afweging maken ('afwegingskader') tussen het gerechtvaardigd belang bij het nastreven van een integere publieke organisatie en het belang van kandidaat op bescherming van de persoonlijke levenssfeer.

Indien de screening voorzienbaar is voor de kandidaat, en deze ook noodzakelijk is voor het bewaken van de integriteit van de organisatie en tot slot met de juiste waarborgen is omkleed, kan

---

[13] Zie bijvoorbeeld p. 36 e.v. in het *Onderzoek naar de verwerking van persoonsgegevens bij pre- en in - employment screening* inzake Hoffmann B.V. van de Autoriteit Persoonsgegevens (23 mei 2016). In dit rapport wordt uitvoerig stilgestaan bij de randvoorwaarden voor de verwerking van diverse (bijzondere) persoonsgegevens.

[14] Art. 8 onder f van de Wbp: de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

[15] Zie het *Onderzoek naar de verwerking van persoonsgegevens bij pre- en in - employment screening* inzake Hoffmann B.V. van de Autoriteit Persoonsgegevens (23 mei 2016).

een inbreuk op het recht op de bescherming van de persoonlijke levenssfeer van de kandidaat worden gerechtvaardigd.[16]

Per 25 mei 2018 kan de gemeente mogelijk geen beroep meer doen op de grondslag 'gerechtvaardigd belang' zoals opgenomen in art. 6 lid 1, onder punt f, van de AVG aangezien aansluitend is bepaald dat deze grond niet geldt ´voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken'.

Gelet op bovenstaande is nu niet met zekerheid aan te geven hoe de juridische interpretatie van 'gerechtvaardigd belang' in het onderzoeksrapport betreffende Hoffmann B.V. voor overheidsinstanties door vertaald kan worden naar het regime van de AVG.

De gemeente zal als verwerkingsverantwoordelijke zelf aannemelijk moeten maken welke grondslag(en) uit de AVG zij geschikt acht voor de verwerking van persoonsgegevens in het kader van screeningsactiviteiten[17]. De gemeente zal zich minimaal op een van de grondslagen in art. 6 van de AVG moeten baseren.

Gemeenten kunnen zich niet beroepen op 'toestemming' omdat dat al eerder is bepaald door de AP. Ook andere grondslagen voor verwerking die in art. 6, lid 1, van de AVG zijn opgenomen, lijken niet voor de hand te liggen in het kader van screening. Het gaat om de gronden:
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen,
c. noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust,
d. noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen.

Het is vervolgens de vraag of de verwerking door gemeenten in het kader van screening binnen de reikwijdte van artikel 6, lid 1, punt e, van de AVG kan vallen.[18] Het lijkt aannemelijk dat gemeenten een grondslag kunnen vinden in artikel 6, lid 1, punt e, en lid 3 van de AVG; de verwerking moet noodzakelijk zijn voor de vervulling van een taak van algemeen belang of van een taak in het kader

---

[16] Zie het *Onderzoek naar de verwerking van persoonsgegevens bij pre- en in - employment screening* inzake Hoffmann B.V. van de Autoriteit Persoonsgegevens (23 mei 2016).

[17] Elke verwerkingsverantwoordelijke is verplicht verantwoording af te leggen ('verantwoordingsplicht') over de gegevensverwerking aan de AP; zie art. 5 lid 2 van de AVG.

[18] De AVG kent open begrippen en normen en deze zullen in de praktijk uitkristalliseren door interventies van toezichthouders en uiteindelijk door uitspraken van rechters. In de AVG (inclusief in de bijbehorende overwegingen) is bijvoorbeeld niet concreet bepaald wat verstaan dient te worden onder 'taak van algemeen belang' of 'uitoefening van het openbaar gezag' (art. 6. lid 1, punt e, van de AVG). De Wbp kent overigens een uitgebreide parlementaire geschiedenis met toelichting op begrippen, waaronder een toelichting met betrekking tot 'publiekrechtelijke taak' (Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3, pagina's 33, 84-86).

van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen, mits deze taak ook in nationale wettelijke regelingen is vastgesteld.

Op basis van de vorige paragraaf (2.2.1) zou gesteld kunnen worden dat deze grondslag nader wordt ingevuld door art. 125, lid 1, onder b, van de Ambtenarenwet dat stelt: “Voor zover deze onderwerpen niet reeds bij of krachtens de wet zijn geregeld, worden voor de ambtenaren, door of vanwege het rijk aangesteld, bij of krachtens algemene maatregel van bestuur voorschriften vastgesteld betreffende: het onderzoek naar de geschiktheid en de bekwaamheid”. Lid 2 stelt: “Het bevoegd gezag van provincies, gemeenten en waterschappen stelt voor de ambtenaar door of vanwege deze lichamen aangesteld, onder gelijk voorbehoud voorschriften vast omtrent de onderwerpen, genoemd in het eerste lid.” Voor gemeenten geldt dat deze voorschriften (mede) zijn uitgewerkt in de CARUWO.

Hiermee zou de combinatie van art. 6, lid 1, punt e, van de AVG tezamen met art. 125, lid 1, onder b, van de Ambtenarenwet in samenhang met de CARUWO, een wettelijke grondslag kunnen bieden voor screening van (kandidaat) werknemers door gemeenten. Dit laat onverlet dat ook aan de andere vereisten van de AVG, art. 10 van de Grondwet en art. 8 van het EVRM moet worden voldaan, zoals noodzakelijkheid, proportionaliteit en subsidiariteit.

Bijzondere (categorieën van) persoonsgegevens
Bij screening mag de gemeente geen ‘bijzondere (categorieën van) persoonsgegevens’[19] verwerken (art. 16 Wbp en vergelijkbaar art. 9 en 10 AVG). Het opvragen en verwerken van dergelijke gegevens is verboden tenzij er een wettelijke uitzondering is. In de artikelen 17-24 van de Wbp en in art. 9 van de AVG zijn uitzonderingsgronden opgenomen ten behoeve van de verwerking van deze bijzondere (categorieën van) persoonsgegevens.

De gemeente kan in het algemeen dus niet vragen naar deze bijzondere (categorieën van) persoonsgegevens bij een screening. De AP heeft in het hiervoor genoemde onderzoek betreffende Hoffmann B.V. ook aangegeven dat ‘slechts indien niet kan worden volstaan met een VOG in de sollicitatie (en screenings-)procedure strafrechtelijke gegevens kunnen worden verwerkt’. De gemeente moet dus aangeven waarom een VOG niet volstaat en wat de aanleiding is om aanvullend strafrechtelijke gegevens te verwerken.

2.2.3 Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

De in de inleiding geschetste ontwikkelingen vragen in toenemende mate om bescherming van vertrouwelijke overheidsinformatie en persoonsgegevens tegen ongeautoriseerde toegang en misbruik door werknemers en externen.

In 2013 hebben de VNG-leden ingestemd met de resolutie ’Informatieveiligheid, randvoorwaarde voor de professionele gemeente’. De resolutie beschrijft in grote lijnen dat iedere gemeente

[19] Het gaat bijvoorbeeld om ras / etnische afkomst, politieke gezindheid / opvatting, godsdienst / religieuze of levensbeschouwelijke overtuigingen en gezondheid.

informatieveiligheidsbeleid vaststelt aan de hand van een basisnormenkader: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Aan de hand van een stappenplan kan de gemeente een samenhangend informatiebeveiligingsbeleid ontwikkelen en onderhouden, bestaande uit een pakket van maatregelen, ter waarborging van de betrouwbaarheid van het informatievoorzieningsproces.

De BIG bestaat uit drie delen[20]: de Strategische Baseline, de Tactische Baseline en de Operationele baseline. In de BIG wordt ervan uitgegaan dat binnen gemeenten het college van Burgemeester en Wethouders integraal verantwoordelijk is voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Een ander uitgangspunt is dat het basisvertrouwelijkheidniveau is vastgesteld als 'Departementaal Vertrouwelijk'[21], zoals gedefinieerd in het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI).[22] Deze rubricering houdt in dat kennisname van de informatie van gemeenten door niet geautoriseerden schade kan toebrengen aan de gemeentelijke belangen, maar dat de maatschappelijke consequenties als gevolg van ongeautoriseerde kennisname beperkt blijven in tijd en omvang. Voor gemeenten praten we hier over 'Vertrouwelijk'. Het gaat dan bijvoorbeeld om persoonsvertrouwelijke informatie, commercieel vertrouwelijke informatie of gevoelige informatie in het kader van beleidsvorming, zogenaamde beleidsintimiteit. Voor wat betreft de bescherming van bijzondere persoonsgegevens geldt artikel 16 van de Wbp (vanaf 25 mei 2018 is dat artikel 9 van de AVG).

De Strategische Baseline kan gezien worden als de kapstok waaraan de elementen van informatiebeveiliging opgehangen kunnen worden en bevat een hiërarchie in de beschrijving van de informatiebeveiligingseisen. Centraal staan de organisatie en de verantwoording over informatiebeveiliging binnen de gemeente. Bewust en verantwoord gedrag van mensen is hierbij essentieel voor een goede informatiebeveiliging. De Tactische Baseline geeft hiervoor normen en maatregelen - ten behoeve van controle en risicomanagement met betrekking tot bedrijfsvoeringprocessen, onderliggende informatiesystemen en informatie van de gemeente - die voor iedere gemeente noodzakelijk zijn om te implementeren.[23] Bij de implementatie geldt voor de tactische normen en eisen een 'comply or explain beleid'. Gemeenten kunnen er dus ook voor kiezen om bijvoorbeeld het eigen integriteitsprotocol aan te vullen met het aspect informatiebeveiliging.

---

[20] Tekst ontleend aan https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2016/07/Strategische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.02.pdf

[21] De rubricering in het VIRBI gaat van zwaar naar licht: Staatsgeheim ZEER GEHEIM (afgekort Stg.ZG), Staatsgeheim GEHEIM (afgekort Stg.G), Staatsgeheim CONFIDENTIEEL (afgekort Stg.C) en Departementaal VERTROUWELIJK (afgekort Dep.V).

[22] Het VIRBI is niet van toepassing op gemeenten.

[23] De Tactische Baseline volgt dezelfde indeling als de internationale beveiligingsnorm ISO/IEC 27002:2007, de controls / maatregelen die als baseline gelden voor alle gemeenten.

In de Tactische Baseline wordt specifiek in hoofdstuk 8 de doelstelling van ‘screening’ voorafgaand aan het dienstverband beschreven als: ‘Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoort te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's’. Tijdens het dienstverband is de doelstelling: ‘Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen en het risico van een menselijke fout te verminderen’.

Om de invoering van de Strategische en Tactische Baseline te ondersteunen, zijn producten ontwikkeld op operationeel niveau, de Operationele baseline.[24] Een van de relevante producten met betrekking tot screening door gemeenten is de ‘Handleiding screening personeel’ van de Informatiebeveiligingsdienst voor gemeenten (IBD). Het geeft een handleiding over hoe invulling kan worden gegeven aan de verificatie van de achtergrond voor alle kandidaten (werknemers), ingehuurd personeel en externe gebruikers zodat integriteitsrisico’s ingeperkt kunnen worden. Gemeenten wordt perspectief geboden hoe ze kunnen omgaan met functieclassificatie en hoe kwetsbare functies gerelateerd kunnen worden aan risicofactoren en het daarbij benoemen van enkele specifieke functies.

2.2.4 Het verstrekken van justitiële- en politiegegevens en het instellen van een veiligheidsonderzoek

Justitiële gegevens

In art. 23 en verder van het Besluit justitiële en strafvorderlijke gegevens (Bjsg) is bepaald dat justitiële gegevens worden verstrekt met het oog op het bij wettelijk voorschrift geregelde onderzoek naar de betrouwbaarheid en geschiktheid van een persoon die in aanmerking wil komen voor een functie bij een ambtelijke dienst voor zover de functie bijzondere eisen stelt aan de integriteit of verantwoordelijkheid van de betrokkene.

Zonder een wettelijke bepaling is het niet mogelijk om justitiële gegevens te verstrekken. Voor gemeenten is niet voorzien in een wettelijk voorschrift en het verstrekken van justitiële gegevens aan de gemeente ten behoeve van het aannemen van personeel op grond van het Bjsg is niet mogelijk.

[24] Tekst ontleend aan https://www.ibdgemeenten.nl/producten/strategische-en-tactische-big/

Politiegegevens

In het Besluit politiegegevens (Bpg) is in paragraaf 4 de verstrekking van politiegegevens aan derden[25] geregeld voor zover het tevens gegevens betreft die worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde en deze derden de gegevens behoeven voor een goede uitvoering van hun taak. Deze derden worden niet in algemene zin benoemd, maar in relatie tot (het uitvoeren van) specifieke taken. In enkele bepalingen in pararaaf 4 is de verstrekking van politiegegevens gerelateerd aan bijvoorbeeld (her)benoeming / aanstelling en ontslag.

Het gaat hier om zachte gegevens, die binnen de politie worden verwerkt. Het betreft informatie over de mogelijke betrokkenheid van personen bij ernstige strafbare feiten of schendingen van de rechtsorde, ten aanzien waarvan de betrouwbaarheid niet is vastgesteld.[26] Gemeenten zijn in het kader van de uitvoering van hun taken in het veiligheidsdomein niet in dit besluit opgenomen zodat politiegegevens niet aan hen verstrekt kunnen worden.

Het instellen van een veiligheidsonderzoek

Een veiligheidsonderzoek wordt door de Algemene Inlichtingen- en Veiligheidsdienst uitgevoerd en omvat het instellen van een onderzoek naar gegevens die uit het oogpunt van de nationale veiligheid van belang zijn voor de vervulling van de desbetreffende vertrouwensfunctie. Uit de kwalificatie van de vertrouwensfunctie, welke is gebaseerd op de mogelijke schade die de vertrouwensfunctionaris kan aanrichten aan de Nationale Veiligheid, volgt voor welk soort veiligheidsonderzoek de persoon in aanmerking komt: een A, B, of een C onderzoek. Een A onderzoek is het meest diepgaand en wordt slechts ingesteld voor de meest kwetsbare vertrouwensfuncties en een C onderzoek is het minst diepgaande onderzoek. Bij A- en B-veiligheidsonderzoeken kan de partner worden gescreend.[27]

Het veiligheidsonderzoek kan pas worden uitgevoerd als de functie door de betreffende ‘vakminister’ is aangewezen als vertrouwensfunctie.[28] De AIVD voert het onderzoek uit en maakt op

[25] Onder meer worden genoemd: de Immigratie- en Naturalisatiedienst, luchtvaartmaatschappijen, de Minister van Buitenlandse Zaken, het Waarborgfonds Motorverkeer, het college van burgemeesters en wethouders, ten behoeve van de uitvoering van de Jeugdwet, Minister van Veiligheid en Justitie, de Onderzoeksraad voor Veiligheid.

[26] Zie de toelichting op het Besluit van 14 december 2007, houdende bepalingen ter uitvoering van de Wet politiegegevens (Besluit politiegegevens), Staatsblad 2007, 550.

[27] Zie artikel 2 (en toelichting bij art. 2) van de Beleidsregel beoordelingsperiodes en onvoldoende gegevens veiligheidsonderzoeken. Voorgaande wordt binnenkort vervangen door de Beleidsregel veiligheidsonderzoeken waarin geen onderscheid meer wordt gemaakt tussen A-, B- en C-onderzoeken.

[28] De aanwijzing is gebaseerd op de ‘Leidraad aanwijzing vertrouwensfuncties’ en de ‘Kwetsbaarheidsanalyse Spionage’ (KWAS).

grond van art. 7 van de Wet veiligheidsonderzoeken (Wvo) gebruik van de volgende gegevens:
a. justitiële en strafvorderlijke gegevens als bedoeld in de Wet justitiële en strafvorderlijke gegevens en gegevens als bedoeld in de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag BES alsmede van gegevens als bedoeld in de Wet politiegegevens en van gegevens verwerkt in het kader van de uitvoering van de politietaak op Bonaire, Sint Eustatius en Saba;
b. gegevens betreffende deelneming of steunverlening aan activiteiten die de nationale veiligheid kunnen schaden;
c. gegevens betreffende lidmaatschap van of steunverlening aan organisaties die doeleinden nastreven, dan wel ter verwezenlijking van hun doeleinden middelen hanteren, die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde;
d. gegevens betreffende overige persoonlijke gedragingen en omstandigheden, naar aanleiding waarvan betwijfeld mag worden of de betrokkene de uit de vertrouwensfunctie voortvloeiende plichten onder alle omstandigheden getrouwelijk zal volbrengen.

Het resultaat van een vertrouwensonderzoek kan zijn een verklaring dat uit het oogpunt van de nationale veiligheid er geen bezwaar bestaat tegen vervulling van een bepaalde vertrouwensfunctie door een bepaalde persoon, of een weigering van deze verklaring.

Na de aanwijzing als vertrouwensfunctie wordt telkens na vijf jaren nagegaan of de aanwijzing gehandhaafd moet blijven. Voor het instellen van een hernieuwd[29] veiligheidsonderzoek is de instemming van de betrokkene niet vereist.

Er zijn tot op heden geen gemeentelijke functies in het veiligheidsdomein aangewezen[30] als vertrouwensfunctie. Dit neemt niet weg dat mogelijk vertrouwensfuncties binnen gemeenten aangewezen kunnen worden indien de nationale veiligheid in het geding is.

2.3 Instrumentarium

In deze paragraaf beschrijven we het instrumentarium dat gemeenten ter beschikking staat om risico's op het gebied van integriteit te beperken. Dit instrumentarium bestaat uit diverse screeningsmethodieken.

Een noot vooraf bij de inzet van het instrumentarium

Vanuit het oogpunt van de bescherming van persoonsgegevens van de kandidaat is het vanaf 25 mei 2018 aan de gemeente om *vooraf* te toetsen of een beroep kan worden gedaan op een of meerdere grondslagen in de AVG en moet tevens voldaan worden aan de eisen uit artikel 8 van het EVRM. Voor alle te verwerken (persoons)gegevens zal dus vooraf bepaald moeten worden of aan

[29] Bijvoorbeeld op basis van informatie uit de Wet justitiële en strafvorderlijke gegevens en van gegevens als bedoeld in de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag BES alsmede van gegevens als bedoeld in de Wet politiegegevens (art. 9 lid 2 Wvo).

[30] Art. 3 Wvo.

het voorgaande wordt voldaan en gelden er dus grenzen op basis van de AVG. Door een gemeente kan in beginsel niet gevraagd worden naar 'bijzondere persoonsgegevens', tenzij wordt voldaan aan een wettelijke uitzondering. Alvorens persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt, dient het voor de betrokkene (de kandidaat) kenbaar en voorzienbaar, dus transparant te zijn dat zijn / haar persoonsgegevens worden verwerkt (art. 8 lid 2 van het EVRM).

2.3.1 Handreikingen om risicovolle functies in kaart te brengen

Naast de reeds genoemde 'Handleiding screening personeel' uit 2016 van de IBD zijn er ook andere handreikingen waarmee risicovolle functies in kaart gebracht kunnen worden. Het betreft bijvoorbeeld de 'Handreiking kwetsbare functies - van kwetsbaar naar weerbaar' (Bureau Integriteitsbevordering Openbare Sector (BIOS), 2010), de 'Leidraad aanwijzing vertrouwensfuncties' (Algemene Inlichtingen- en Veiligheidsdienst, 2014) en de brochure 'Screening van personeel' (Justis, 2017).

Om de proportionaliteit van de inzet van screeningsmethodieken te kunnen bepalen is inzicht nodig in de risico's van bepaalde functies. Daartoe kunnen gemeenten bijvoorbeeld een risico-inventarisatie uitvoeren waarmee kwetsbare / risicovolle functies in kaart kunnen worden gebracht. In de opgesomde handreikingen worden op hoofdlijnen de volgende risicovolle factoren van een functie genoemd:

- toegang tot vertrouwelijke informatie
- omgaan met geld (bijvoorbeeld betalingen verrichten of het innen van belastingen)
- machtspositie (bijvoorbeeld handhaving en toezicht)
- toekennen rechten/bevoegdheden aan personeel en/of burgers en bedrijven (bijvoorbeeld vergunningen, subsidies, uitkeringen)
- beoordelen en adviseren
- uitbesteden / inkoop (het aanschaffen van goederen en diensten)
- solistisch kunnen handelen.

2.3.2 Het instrumentarium bij pre-employment en in-employment

Bij de inzet van het instrumentarium door gemeenten zijn een tweetal fases te herkennen: de pre-employment- en de in-employment-fase. Binnen deze fases kan een onderverdeling worden gemaakt van minder ingrijpende naar ingrijpende instrumenten waarmee risico's beperkt kunnen worden. Langs deze lijn worden onderstaand de instrumenten beschreven. Indien een gemeente (nog) geen gebruik kan maken van het instrumentarium dan wel dat een andere grondslag vereist is, wordt dat aangegeven.

Pre-employment

Gemeenten hebben de bevoegdheid een onderzoek uit te voeren waaruit moet blijken of de kandidaat in voldoende mate beschikt over de hoedanigheden tot het verrichten van de hem op te dragen werkzaamheden. De algemene grondslag is 125 e.v. van de Ambtenarenwet in samenhang met art. 2:2 van het CARUWO. Over de aard en vorm van een dergelijk onderzoek is niets bepaald.

Het instrumentarium in de fase van pre-employment:

- Het sollicitatiegesprek

De gemeentelijke werkgever hanteert in de praktijk standaard een sollicitatiegesprek. Dit gesprek is veelal gericht op het aannemen van de kandidaat ambtenaar waarbij kennis en kunde (competenties) worden getoetst. De sollicitatieprocedure kan de werkgever echter ook inzetten als instrument om integriteitsrisico's te checken. Tijdens het sollicitatiegesprek kan aandacht worden besteed aan thema's als integriteit, privacy, nevenfuncties en/of -werkzaamheden en informatieveiligheid.

- Bestudering van curriculum vitae (cv)

Het cv bevat een overzicht van het arbeidsverleden en werkervaring van een kandidaat. Bestudering van het cv is net als het sollicitatiegesprek veelal gericht op de kennis en kunde van de kandidaat. Vanuit het oogpunt van risicobeperking kan echter ook gekeken worden naar bijvoorbeeld hiaten, nevenwerkzaamheden, privé-activiteiten of andere informatie die aanknopingspunten biedt om door te vragen op aspecten van integriteit.

- Opvragen van originele diploma's en cijferlijsten / certificaten / getuigschriften

Diploma's, cijferlijsten en certificaten geven aan wat de resultaten / waarderingen zijn van een opleiding / onderwijs, cursus of andere ervaring. De gemeente kan vanuit het oogpunt van risicobeperking de originelen opvragen en daarmee fraude voorkomen.

- Controle van paspoort of identiteitskaart

Een gemeente kan de identiteit van de persoon verifiëren ('identificeren') bijvoorbeeld in het kader van een sollicitatiegesprek.[31]

- Gesprek over integriteit / afnemen van een integriteitstest

Met een gesprek specifiek over integriteit of met een (digitale) integriteitstest als onderdeel van de selectieprocedure kan de gemeente vooraf meer te weten te komen over iemands oordeel over integriteit. Door dilemma's voor te leggen, kan iemand getest worden op regelkennis, alertheid en openheid.

- Het laten invullen van een vragenlijst / eigen verklaring door de kandidaat ambtenaar

Een vragenlijst of eigen verklaring geeft de geschiktheid aan van de kandidaat. Hierin kunnen vragen aan bod komen als: bent u in de afgelopen vijf jaar wel eens ontslagen? Bent u in het verleden getoetst op integriteit of vakbekwaamheid, en zo ja: is er een voorbehoud gemaakt? Ook

[31] Bij de sollicitatieprocedure mag door de gemeente niet zomaar een kopie van het paspoort worden gemaakt en worden verwerkt (in verband met het BSN-nummer op het paspoort of ID-kaart). Het BSN-nummer moet dus zijn afgeschermd.

kan ervoor gekozen worden de kandidaat een verklaring af te laten afleggen over deze onderwerpen en deze te laten ondertekenen.

- Het checken van referenties

Referenten, bijvoorbeeld vorige werkgevers of opdrachtgevers, kunnen bepaalde aspecten uit het (recente) arbeidsverleden van een kandidaat bevestigen. Hierdoor kan bijgedragen worden aan de integriteitstoets van een gemeente. De kandidaat moet zelf referenten hebben opgegeven of moet op de hoogte zijn dat anderen dan opgegeven referenten kunnen worden bevraagd. In het laatste geval moet eerst toestemming van de kandidaat zijn verkregen voor het bevragen van niet-opgegeven referenten aldus de NVP Sollicitatiecode.[32]

- Openbare bronnen / open bronnenonderzoek

Er zijn verschillende openbare registers waarin (persoons)gegevens zijn opgenomen over de (financiële) achtergrond van een kandidaat. Zo zijn er bijvoorbeeld het curateleregister, het centraal insolventieregister, het Handelsregister van de Kamer van Koophandel en het BKR (kredietregistratie).[33] Deze voorbeelden zijn vormen van openbare bronnen die iedereen (soms tegen betaling) kan raadplegen. Voor het BKR geldt dat alleen de kandidaat de aanvraag kan indienen voor een afschrift.

Naast deze openbare registers kan een gemeente via zoekmachines als bijvoorbeeld Google en wieowie.nl veel te weten komen over (mogelijke integriteitsaspecten en betrouwbaarheid van) kandidaten. Ook zakelijke en persoonlijke gegevens via LinkedIn, Twitter of Facebook, blogs of reacties op internetfora zijn voor handen.

De Europese privacy toezichthouder (de zogenoemde Artikel 29-werkgroep) heeft hierover recentelijk een opinie aangenomen.[34] In de opinie wordt de hoofdregel aangegeven dat een ‘online onderzoek’ niet kan, tenzij een wettelijke grondslag aanwezig is en dat de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit, gelden voor alle gegevensverwerkingen

---

[32] De NVP Sollicitatiecode bevat basisregels die arbeidsorganisaties (bedrijven en instellingen die arbeidsrelaties aangaan) en sollicitanten naar het oordeel van de Nederlandse Vereniging voor Personeelsmanagement & Organisatieontwikkeling (NVP) in acht behoren te nemen bij de werving en selectie ter vervulling van vacatures. Het doel van de code is een norm te bieden voor een transparante en eerlijke werving en selectieprocedure. De code is chronologisch opgebouwd vanaf het ontstaan van de vacature tot de aanstelling.

[33] https://insolventies.rechtspraak.nl/, https://curateleenbewindregister.rechtspraak.nl/, https://www.kvk.nl/zoeken/handelsregister/ en https://www.bkr.nl/

[34] Opinion 2/2017 on data processing at work, 8 juni 2017. Opinies zijn geen wet- of regelgeving, maar zijn wel zeer gezaghebbend in de praktijk.

gedurende de gehele screeningsprocedure.[35] Op basis van de eis van kenbaarheid (ex artikel 8 EVRM) voor de kandidaten moet een betrokkene vooraf en nadien over een voorgenomen open bronnenonderzoek worden geïnformeerd. Verder volgt uit de opinie dat een werkgever verplicht is tot het maken van afwegingen, bijvoorbeeld of de 'online' gegevens een zakelijk dan wel privékarakter hebben, waarbij het bekijken van zakelijke online informatie eerder gerechtvaardigd lijkt te zijn.

Voormalig Minister van SZW Asscher heeft onlangs nog een reactie gegeven op deze opinie. In zijn reactie is opgenomen dat 'de opinie geen directe gevolgen heeft voor de Nederlandse wet- en regelgeving; het gaat hier om een uitleg van bestaande regelgeving door een onafhankelijk adviesorgaan van Europese privacy-toezichthouders. De artikel 29-werkgroep heeft deze opinie uitgebracht om duidelijkheid te scheppen over de balans tussen de belangen van werkgevers en het recht op privacy van (toekomstige) werknemers'. Ten aanzien van de vraag of werkgevers gebruik mogen maken van online profielen die een professioneel doeleinde hebben, zoals een online cv, geeft hij aan: 'Een werkgever mag uitsluitend een inbreuk maken op het recht op bescherming van persoonlijke levenssfeer van de (toekomstige) werknemer indien daarvoor een wettelijke grondslag aanwezig is. Dit geldt ook voor het gebruik maken van online profielen van een sollicitant. In een sollicitatieprocedure zal een werkgever moeten kunnen onderbouwen dat een online check noodzakelijk is voor het behartigen van een gerechtvaardigd belang. Als er sprake is van een profiel dat een professioneel doeleinde dient, zal daar eerder sprake van kunnen zijn dan als het een privé profiel betreft. Van belang is bovendien dat werkgevers vooraf transparant zijn over het feit dat een online screening onderdeel uitmaakt van de procedure, en dat gegevens die tijdens een screening worden verzameld niet langer bewaard worden dan noodzakelijk is'.[36]

De Nederlandse Vereniging voor Personeelsmanagement & Organisatieontwikkeling (NVP) heeft een sollicitatiecode[37] vastgesteld ('zelfregulering') en deze sollicitatiecode is breed geaccepteerd. Het gebruik van 'open bronnen' en/of 'openbare informatie' lijkt in de sollicitatiecode geaccepteerd te worden zolang de bron wordt vermeld. Opgemerkt wordt dat bij het gebruik van deze bronnen aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit voldaan moet worden. Dit is ook conform bovenstaande opinie van de Artikel 29-werkgroep en de reactie van de voormalige minister van SZW.

- Vragen van een verklaring omtrent het gedrag (VOG)

Een VOG is een verklaring op basis van een onderzoek naar justitiële documentatie waaruit blijkt dat het gedrag van de kandidaat in het verleden geen bezwaar vormt voor het vervullen van een specifieke taak of functie (art. 28 Wjsg). In de verklaring worden geen mededelingen gedaan over

---

[35] Vergelijk ook het *Onderzoek naar de verwerking van persoonsgegevens bij pre- en in - employment screening* inzake Hoffmann B.V. van de Autoriteit Persoonsgegevens (23 mei 2016).

[36] 28 september 2017, Tweede Kamer, vergaderjaar 2017–2018, Aanhangsel nr. 74.

[37] Zie de sollicitatiecode van juni 2016 op https://nvp-plaza.nl/download/?id=624

de geregistreerde justitiële gegevens; er wordt uitsluitend vermeld dat niet is gebleken van bezwaren tegen die persoon. Indien de kandidaat geen strafblad heeft, wordt de VOG altijd verleend. Een VOG wordt slechts geweigerd 'indien in de justitiële documentatie met betrekking tot de aanvrager een strafbaar feit is vermeld, dat, indien herhaald, gelet op het risico voor de samenleving en de overige omstandigheden van het geval, aan het doel waarvoor de verklaring omtrent het gedrag wordt gevraagd, in de weg zal staan' (artikel 35 Wjsg).

Er is geen plicht[38] voor een gemeente om een VOG van een kandidaat te vragen. De gemeente kan een VOG verlangen op grond van art. 2:2 lid 3 CARUWO. Vanaf 1 januari 2018 is deze mogelijkheid uitgebreid in situaties van functiewijziging, overplaatsing of tewerkstelling. De gemeente bepaalt, afhankelijk van de taken die kandidaat gaat uitvoeren, waarop wordt gescreend. Op het VOG-aanvraagformulier moet de gemeente als werkgever verplicht aangeven op welke functieaspecten zij de betreffende kandidaat wil laten screenen.[39] Bij deze screening wordt door Justis gekeken naar de relatie tussen het werk dat de kandidaat gaat doen en de delicten op zijn of haar strafblad.

Er bestaan twee soorten screeningsprofielen: een algemeen en een specifiek.[40] Het algemene screeningsprofiel is onderverdeeld in acht risicogebieden (informatie, geld, goederen, diensten, zakelijke transacties, proces, aansturen organisatie en personen).[41] Voor bijvoorbeeld buitengewoon opsporingsambtenaren (boa's) is er een specifiek screeningsprofiel[42] waarbij de juridische grondslag is te vinden in art. 142 lid 2 Wetboek van strafvordering in samenhang met artikel 17 van het Besluit buitengewoon opsporingsambtenaar en paragraaf 3.3 van de Beleidsregels buitengewoon opsporingsambtenaren. Daarnaast is het altijd mogelijk om de betrouwbaarheid tussentijds te toetsen. Mocht bij deze tussentijdse toetsing twijfels bestaan omtrent de betrouwbaarheid of blijken dat de boa niet meer betrouwbaar is, dan kan de bevoegdheid worden opgeschort of ingetrokken. Of de boa nog betrouwbaar is wordt vastgesteld aan de hand van de justitiële documentatie of politiële informatie afkomstig van de toezichthouder en/of de direct toezichthouder. Bij verstrekking van deze informatie kan advies worden gevraagd aan de toezichthouder en/of de direct toezichthouder. Ook feiten die (nog) niet tot strafrechtelijke vervolging

[38] De wetgever heeft voor enkele specifieke beroepen in regelgeving vastgelegd dat een VOG in ieder geval verplicht is, bijvoorbeeld voor leraren en taxichauffeurs.

[39] Het screeningsprofiel is uitsluitend gekoppeld aan het doel waarvoor de betrokkene de VOG aanvraagt, zie Kamerstukken II 2010/11, 32 763, nr. 3, p. 8.

[40] Er zijn een aantal specifieke screeningsprofielen ontwikkeld, speciaal voor bepaalde beroepsgroepen dan wel bepaalde doelen: https://www.justis.nl/binaries/Screeningsprofielen%20met%20ingang%20van%201%20jan%202018-versie%201.3_tcm34-296676.pdf

[41] Er geldt hierbij een standaard terugkijktermijn van vier jaren.

[42] Bij de toets aan dit screeningsprofiel geldt een terugkijktermijn van tien jaren.

hebben geleid worden meegenomen bij het bepalen of de boa nog betrouwbaar kan worden geacht.[43]

In-employment

Bij de in-employment-fase mogen gemeenten onderstaand instrumentarium inzetten met als grondslag art. 125 e.v. van de Ambtenarenwet in samenhang met hoofdstuk 15 van het CARUWO. Ook hier moet aandacht besteed worden aan de bescherming van persoonsgegevens zoals eerder is aangegeven bij de 'pre-employment'-fase.

Het instrumentarium in de fase van 'in-employment':

- Integriteitsbeleid (Gedragscode)

Op grond van art.125 en 125quater van de Ambtenarenwet heeft de gemeente de taak 'een integriteitsbeleid voor goed ambtelijk handelen' op te stellen dat in ieder geval aandacht besteedt aan het bevorderen van integriteitsbewustzijn en aan het voorkomen van misbruik van bevoegdheden, belangenverstrengeling en discriminatie. Het integriteitsbeleid maakt een vast onderdeel uit van het personeelsbeleid door in ieder geval integriteit in functioneringsgesprekken en werkoverleg aan de orde te stellen en door het aanbieden van scholing en vorming op het gebied van integriteit.

- Voeren van een periodiek gesprek (inzake functioneren)

Een gesprek met de ambtenaar kan gaan over diens functie en de uitoefening ervan in relatie tot integriteitsaspecten. Een dergelijk periodiek gesprek is dan gebaseerd op art. 125 van de Ambtenarenwet in samenhang met art. 15:1:15 van het CARUWO. Hierin is bepaald dat het college kan bepalen dat met inachtneming van door het college te stellen regels over de ambtenaar periodiek een beoordeling wordt uitgebracht omtrent de wijze waarop hij zijn functie vervult en omtrent zijn gedragingen tijdens de uitoefening daarvan.

- Gesprek over integriteit / afnemen van een integriteitstest

Met bijvoorbeeld een (digitale) integriteitstest of een gesprek over integriteit kan de gemeente gedurende het dienstverband meer te weten te komen over iemands integriteit. Tijdens een dergelijk gesprek kunnen actuele dilemma's besproken worden of kan de medewerker getest worden op alertheid, openheid en regelkennis op het gebied van integriteit.

- Controle van paspoort of identiteitskaart

Een gemeente is verplicht tot het vaststellen van de identiteit van een werknemer. In artikel 28, eerste lid, onder f, van de Wet op de loonbelasting 1964 is bepaald dat de inhoudingsplichtige gemeente is gehouden van de werknemer die loon uit tegenwoordige dienstbetrekking geniet de

[43] Zie paragraaf 3.3 van de Beleidsregels Buitengewoon Opsporingsambtenaar. Boa's zijn in bezoldigde overheidsdienst, maar hierop kunnen een aantal uitzonderingen van toepassing zijn zoals opgenomen in paragraaf 3.1 van de Beleidsregels Buitengewoon Opsporingsambtenaar.

identiteit vast te stellen aan de hand van een document als bedoeld in de Wet op de identificatieplicht.[44]

- Het afleggen van de eed / belofte

Na indiensttreding dient een ambtenaar de eed of belofte af te leggen. Daarmee belooft de ambtenaar integer te handelen en te hebben gehandeld bij verkrijging van de aanstelling. In art. 125q Ambtenarenwet en 15:1:a CARUWO is vastgelegd dat de ambtenaar verplicht is de eed of belofte af te leggen die bij wet, bij instructie of bij besluit van het college is voorgeschreven.

- VOG aanvragen bij functiewijziging, overplaatsing of tewerkstelling

De gemeente kan een VOG verlangen van de kandidaat op grond van art. 2:2 lid 3 CARUWO. Vanaf 1 januari 2018 is deze mogelijkheid uitgebreid door aan artikel 2:2 CARUWO een vierde lid[45] toe te voegen waardoor een werkgever ook gedurende de aanstelling een VOG kan vragen. Deze mogelijkheid is echter beperkt tot situaties waarin de medewerker andere werkzaamheden gaat doen, namelijk bij functiewijziging, overplaatsing of tewerkstelling.

---

[44] Het betreft een geldig reisdocument, of een Nederlandse identiteitskaart en vervangende Nederlandse identiteitskaart, de documenten waarover een vreemdeling ingevolge de Vreemdelingenwet 2000 moet beschikken ter vaststelling van zijn identiteit, nationaliteit en verblijfsrechtelijke positie en een geldig nationaal, diplomatiek of dienstpaspoort dat is afgegeven door het daartoe bevoegde gezag in een andere lidstaat van de Europese Gemeenschappen of in een andere staat die partij is bij de Overeenkomst betreffende de Europese Economische Ruimte, voor zover de houder de nationaliteit van die andere lidstaat bezit. Een rijbewijs kan hiervoor dus niet gebruikt worden.

[45] Lid 4: Bij een functiewijziging, tewerkstelling of overplaatsing kan als vereiste worden gesteld dat de ambtenaar een recente verklaring omtrent het gedrag als bedoeld in lid 3 overlegt.

3. Case studies

3.1 Verkennend onderzoek bij vijf gemeenten

In deze paragraaf beschrijven we de resultaten van de verkenning van vijf case studies bij gemeenten.[46] Het doel van deze case studies is inzicht te krijgen in hoeverre gemeenten in de praktijk zicht hebben op risicovolle functies bij de beoefening van taken binnen het veiligheidsdomein. Daarnaast is het doel om inzicht te krijgen in hoeverre en op welke wijze door gemeenten gebruik wordt gemaakt van het beschikbare instrumentarium wat betreft screening en overige risico beperkende maatregelen.

In onderstaande paragrafen presenteren we de feitelijke bevindingen per gemeente.[47] Deze bevindingen zijn het resultaat van documentanalyse en verdiepende gesprekken met medewerkers van de respectievelijke gemeenten. We geven de bevindingen zodanig weer dat deze niet naar de gemeenten te herleiden zijn. De gemeenten worden daarom aangeduid met de letters A t/m E. We hanteren per gemeente de volgende indeling:

- Contextschets

Het gaat hierbij om de omvang en ligging van de gemeente, de aard van de gemeentelijke problematiek binnen het veiligheidsdomein en eventuele overige relevante actualiteiten.

- Kwetsbare functies

Dit zijn de functies die door de gemeente als kwetsbaar worden gezien. Primair gaat het hier om functies binnen het veiligheidsdomein. Daarnaast wordt beschreven op welke wijze deze functies zijn geïdentificeerd.

- Inzet instrumentarium

Hierbij gaat het om de inzet van het beschikbare instrumentarium om risico's en kwetsbaarheden in te perken. Daarbij kan het gaan om organisatorische maatregelen en screening.

- Screeningsbehoefte

Hier beschrijven we de eventuele aanvullende behoefte die binnen gemeenten leeft op het gebied van screening.

[46] De case studie is bij vijf gemeenten uitgevoerd. Ondanks het feit dat er rekening is gehouden met grootte, problematiek en geografische ligging, is dit geen volledig representatieve steekproef.

[47] Bij de beschrijving van deze paragrafen is onder meer geput uit de gesprekken, opgestelde factsheets, nadere reacties van de gemeenten op de factsheets en ontvangen documenten.

3.2 Gemeente A

3.2.1 Contextschets

Gemeente A is een 100.000+ gemeente gelegen in het zuiden van het land. De gemeente is bekend met problematiek op het gebied van ondermijning en organiseert interne activiteiten op dit thema. Tevens worden er jaarlijks grote evenementen in de gemeente georganiseerd, waarbij de integriteit van medewerkers op de proef wordt gesteld. Binnen het veiligheidsdomein van de gemeente zijn een aantal voormalig medewerkers van de politie werkzaam. In het kader van de case studie hebben we gesproken met de gemeentesecretaris, corporate controller, specialist veiligheid, strategisch adviseur veiligheid, teammanager Veiligheid, hoofd Juridische Zaken, medeweker HR beleid en P&O manager.

3.2.2 Kwetsbare functies

Door middel van een risicoanalyse zijn kwetsbare functies geïdentificeerd - Binnen gemeente A zijn op basis van een risicoanalyse kwetsbare functies binnen het veiligheidsdomein aangewezen. Deze risicoanalyse is gemaakt op basis van een sjabloon. Dat sjabloon is specifiek opgesteld voor het maken van een risicoanalyse binnen het veiligheidsdomein[48] en gebaseerd op de 'Leidraad aanwijzing vertrouwensfuncties' en de 'Kwetsbaarheidsanalyse Spionage' (KWAS), beide van de AIVD. In beide documenten is het criterium waaraan getoetst is 'toegang tot kwetsbare informatiesystemen'. Binnen gemeente A is een ambtenaar in het veiligheidsdomein verantwoordelijk voor het identificeren van kwetsbare functies. Met ondersteuning van een medewerker van de afdeling personeelszaken heeft de ambtenaar aan de hand van de risicoanalyse kwetsbare functies geïdentificeerd.

Alle functies binnen het veiligheidsdomein worden als risicovol aangemerkt - Een uitkomst van de risicoanalyse is dat alle functies binnen het domein veiligheid (enige mate van) kwetsbaarheid met zich meebrengen. Een groot aantal functies binnen het veiligheidsdomein wordt door de toegang tot bepaalde vertrouwelijke informatie als dusdanig kwetsbaar bestempeld dat verdergaande screening dan op dit moment mogelijk is, gerechtvaardigd zou zijn, aldus gemeente A op basis van hun risicoanalyse. Dit geldt voor de functies: Adviseur OOV, Specialist Veiligheid, Procesregisseur, Informatie coördinator, Informatieanalist, Coördinator BIBOB, Coördinator Ondermijning, Specialist Veiligheid en Coördinator interne weerbaarheid. In gemeente A wordt binnen het domein veiligheid niet expliciet onderscheid gemaakt tussen verschillende risiconiveaus. Dit gebeurt volgens gemeente A wel impliciet door een functiespecifieke VOG aan te vragen.

Naast kwetsbare functies zijn ook kwetsbare processen in kaart gebracht - Een van de kwetsbare processen heeft betrekking op de aanpak van georganiseerde criminaliteit. Bij dit proces

[48] Gemeenten zijn op uiteenlopende wijze georganiseerd en gebruiken uiteenlopende terminologie om de groep personen aan te duiden die zich bezig houden met het thema veiligheid. Vanuit het oogpunt van eenduidigheid noemen wij deze groep mensen in deze rapportage het 'veiligheidsdomein' of 'domein veiligheid'.

zijn verschillende ambtenaren betrokken, ook ambtenaren die niet werkzaam zijn in het veiligheidsdomein. Gemeente A is dan ook van mening dat de risico's in het veiligheidsdomein samenhangen met risico's in andere domeinen (zoals ICT, Sociaal, Ondersteunend en Dienstverlenend) waar met vertrouwelijke of gevoelige informatie wordt omgegaan.

3.2.3 Inzet instrumentarium

Er wordt gebruik gemaakt van beheersmaatregelen om risico's in te perken - Binnen gemeente A worden in het veiligheidsdomein diverse beheersmaatregelen ingezet om risico's te beperken. Deze beheersmaatregelen zijn deels gekoppeld aan de risicoanalyse.

Een maatregel die voor iedereen geldt, onafhankelijk van het risicoprofiel van een bepaalde functie, is dat integriteit deel uitmaakt van het functioneringsgesprek tussen een medewerker en zijn/haar leidinggevende. Verder bestaat er een gemeentelijke gedragscode en dienen medewerkers de ambtseed af te leggen. Tevens gaan medewerkers in sessies 'morele oordeelvorming' met elkaar in gesprek over mogelijke issues op het gebied van integriteit en hoe daarmee om te gaan.

Er gelden aanvullende beheersmaatregelen in het veiligheidsdomein - Naast deze meer generieke maatregelen wordt binnen het veiligheidsdomein ook gewerkt met functieroulatie waarmee wordt voorkomen dat medewerkers te lang op een bepaalde positie zitten. Verder wordt, voor bepaalde transacties of handelingen, het vierogenprincipe toegepast waardoor de kans op frauduleus handelen wordt verkleind.

De bestaande maatregelen worden volgens gemeente A nog niet optimaal benut - Gemeente A is van mening dat de beheersmaatregelen nuttig zijn en goed werken, maar er wordt nog niet maximaal gebruik gemaakt van de maatregelen om risico's op het gebied van integriteit te beperken. Zo kan volgens gemeente A zelf beter regie worden gevoerd op het thema weerbaarheid binnen de gemeente en kan er nog harder worden gewerkt aan het structureel onder de aandacht brengen ervan.

Alle medewerkers dienen een VOG te overleggen en binnen het veiligheidsdomein gelden aanvullende eisen - Binnen gemeente A wordt gebruik gemaakt van uiteenlopende screeningsmethodieken. Elke medewerker van de gemeente dient een VOG te overleggen. Het invullen van het werkgeversdeel van de VOG kan door verschillende personen worden gedaan.[49] Om eenduidig te handelen is in een protocol per afdeling en/of taakinhoud aangegeven welke categorieën voor welke nieuwe medewerker moet worden aangekruist.

Daarnaast wordt voor alle nieuwe medewerkers binnen het veiligheidsdomein (ook voor de medewerkers die intern worden overgeplaatst naar de afdeling veiligheid) een VOG aangevraagd met een specifiek screeningsprofiel "(buitengewoon) opsporingsambtenaar".

Verder worden referenties gecheckt van sollicitanten in het veiligheidsdomein. Dit gebeurt met instemming vooraf van betrokkene zelf. Deze referenties worden gecheckt door een medewerker

[49] Dit kan echter niet door de persoon zelf gedaan worden die een VOG aanvraagt.

van het veiligheidsdomein (eventueel) in afstemming met de afdeling personeelszaken. Boa's van Stadstoezicht en medewerkers van het RIEC ondergaan een 'BGO-lang'[50]. Deze screening wordt door de politie uitgevoerd.[51]

Medewerkers worden niet periodiek gescreend. Mogelijk komt daar in de nabije toekomst wel een wijziging in. De screening wordt uitgevoerd door medewerkers van het veiligheidsdomein, met ondersteuning van de afdeling personeelszaken.

3.2.4 Screeningsbehoefte

Gemeente A geeft aan behoefte te hebben aan aanvullende mogelijkheden op het gebied van screening - De behoefte aan extra screening komt voort uit de eigen analyse dat bepaalde kwetsbare functies binnen het veiligheidsdomein kunnen beschikken over dusdanig gevoelige informatie dat bestaande risico beperkende maatregelen en screeningsmethodieken onvoldoende waarborgen bieden om risico's tegen te gaan. Volgens gemeente A kan men met fysieke noch organisatorische maatregelen de risico's op het doorspelen, verkopen, wijzigen dan wel manipuleren van informatie afdoende inperken.

Gemeente A geeft aan dat de gevoelige informatie onder meer betreft persoonsinformatie over het vrijkomen of verloven van gedetineerden en ex-gedetineerden alsmede de reden van detentie (strafrechtelijke informatie), persoonsinformatie over personen binnen de Jeugdzorg (GCOS), persoonsinformatie (persoons- en adresgegevens, overtredingen en huisregelovertredingen) op het gebied van voetbalhooliganisme, huisverboden (persoonsgegevens uit huis geplaatsten, achterblijvers, financiële informatie van het gezin), persoonsgegevens (inclusief medische gegevens) over zedenzaken (zowel dader als slachtoffer) of verwarde personen, mondelinge toelichting van politie en OM op lopende onderzoeken, Basisregistratie Personen – zowel lokaal als landelijk, informatie over personen die in verband worden gebracht met radicalisering of extremisme, informatie over verbanden tussen personen die in beeld zijn bij de inlichtingeneenheden / politie en raakvlakken met de gemeente en informatie over waar hennepruimingen hebben plaatsgevonden en wie als verdachte is aangemerkt.

---

[50] Door gemeenten wordt het 'BGO' zoals dat door de politie wordt uitgevoerd gezien als een screeningsinstrument. Technisch gezien is echter geen sprake van een screeningsinstrument, maar van een verzameling aan methodieken/instrumenten in het kader van de aanstelling als politieambtenaar. In de beschrijvingen van de case studies waar 'BGO' door gemeenten wordt gehanteerd gaat het dus om een screening zoals bij politieambtenaren.

[51] Er is een uitvoeringspraktijk ontstaan waarbij de politie ook gemeentelijke medewerkers screent, daarvoor is nu geen wettelijke bevoegdheid. De Tweede Kamer is hierover geïnformeerd waarbij is aangegeven dat deze tijdelijke oplossing blijft bestaan opdat kan worden bepaald hoe de screening van deze medewerkers geregeld dient te worden. Deze situatie komt in meerdere case studies aan de orde.

Er is behoefte aan uitbreiding van screening binnen het veiligheidsdomein, maar ook naar verbreding tot andere domeinen - Omdat (een deel van de) ambtenaren binnen het veiligheidsdomein de beschikking heeft over eerder genoemde informatie is het volgens gemeente A noodzakelijk de mogelijkheden tot het uitvoeren van screening uit te breiden naar een screening zoals de politie die voor het eigen personeel hanteert. Daarmee wordt tevens de preventie versterkt aldus gemeente A. Naast uitbreiding van de screeningsmogelijkheden bestaat ook de wens screening breder dan het veiligheidsdomein in te zetten (bijvoorbeeld bij ICT of Vastgoed). Daarnaast bestaat de wens screening uit te breiden van alleen instroomvoorwaarde naar een periodieke screening (gedurende het dienstverband).

De behoefte tot extra screening komt niet door druk vanuit externe partijen - Vanuit partijen als de politie en het Openbaar Ministerie wordt geen eis op tafel gelegd dat medewerkers van de gemeente gescreend moeten worden om over de genoemde informatie te mogen beschikken. Deze behoefte aan aanvullende screeningsmogelijkheden komt vanuit de gemeente zelf en in het bijzonder vanuit het veiligheidsdomein.

3.3 Gemeente B

3.3.1 Contextschets

De gemeente is een 100.000+ gemeente gelegen in het noorden van het land. De gemeente heeft te maken met georganiseerde criminaliteit in de regio en maakt zich daarom hard voor bewustwording en awareness met betrekking tot integriteit. Het RIEC heeft onlangs een presentatie gegeven aan het gemeentebestuur over het ondermijningsbeleid en potentiële valkuilen voor bestuurders. In het kader van de case studie hebben we gesproken met de gemeentesecretaris, integriteitcoördinator, teamleider JZ en teamleider Inkoop en adviseur OOV en team Organisatie & Advies, Werving & Selectie.

3.3.2 Kwetsbare functies

Er wordt geen gebruik gemaakt van risicoanalyses en andere tools - Binnen gemeente B wordt geen gebruik gemaakt van risicoanalyses, risico-inventarisaties, risicomatrices en risicoprofielen. Er wordt gesteld dat men hier nooit volledig in kan zijn en dat er een variëteit aan functies is, die tevens verspreid is over de gehele gemeentelijke organisatie en inhoudelijk verschillend zijn. Tevens wordt aangegeven dat omgevingsfactoren mede bepalend zijn, waardoor de meerwaarde en preventieve werking van dergelijke analyses in twijfel wordt getrokken.

Binnen het veiligheidsdomein zijn geen kwetsbare functies geïdentificeerd - Er is geen lijst van risicovolle functies opgesteld of een (recente) risicoanalyse op functies uitgevoerd. Er is een document opgesteld over criteria voor kwetsbare functies, maar dit betreft geen lijst met specifieke functies. Het startpunt hierbij zijn kwetsbare processen. Het document was bedoeld voor de gesprekken met medewerkers in het kader van functioneringsgesprekken, maar het document wordt niet of nauwelijks meer gebruikt. Volgens gemeente B zijn deze criteria voor kwetsbare functies ook van toepassing op het sociaal domein (WMO-functionarissen), het fysieke domein, vastgoeddomein, in contacten met derden en op de communicatieafdeling. De noodzaak voor meer bewustwording

ten aanzien van de risico's die bepaalde functies met zich meebrengen, wordt onderkend, mede gelet op het verschuiven van 'ondermijningsactiviteiten' richting de gemeentegrenzen.

Het creëren van bewustzijn en het voeren van gesprekken over integriteit wordt belangrijker geacht dan identificatie van kwetsbare functies - Binnen gemeente B wordt vooral veel waarde gehecht aan het creëren van bewustzijn bij ambtenaren. Daarnaast is er veel vertrouwen in oprechte gesprekken met medewerkers over integriteit. Het (functionerings)gesprek wordt belangrijker geacht dan, in hun ogen, kwantitatieve tools als een risicoanalyse. Men gaat er vanuit dat deze gesprekken beter bijdragen aan inzicht over integer handelen en mogelijke (persoonlijke) kwetsbaarheden van medewerkers dan dergelijke analyses. Houding, gedrag en het continu creëren van bewustzijn met betrekking tot integriteit worden tevens belangrijker geacht dan het bijhouden van lijsten met kwetsbare functies.

3.3.3 Inzet instrumentarium

Er wordt gebruik gemaakt van diverse risico beperkende maatregelen - Het werken aan bewustwording bij medewerkers staat in gemeente B centraal. Door OOV-medewerkers is een speciaal beveiligde laptop in gebruik vanwege de politie informatie die er op staat. Verder is in 2017 de gemeentelijke gedragscode herzien en het belang hiervan wordt vanuit het gemeentebestuur onderschreven. In de gedragscode is aandacht voor informatieveiligheid, nevenfuncties, het gebruik van openbare bronnen (onder andere sociale media) en het aannemen van geschenken. Er wordt echter geen verbinding gelegd tussen de gedragscode en kwetsbare functies. Het algemene beeld is dat werknemers zich gedragen conform deze gedragscode. Overige organisatorische en fysieke maatregelen die worden getroffen tijdens de employment fase zijn: logging van bepaalde systemen, toegangscontrole, autorisaties, wachtwoordbeheer, cleandesk policy en functiescheiding. De continue aandacht voor integriteit en gemeentelijke integriteitskwesties uit het verleden hebben geleid tot een groot moreel besef binnen de ambtelijke organisatie.

Er wordt beperkt onderscheid gemaakt tussen kwetsbare en reguliere functies bij de screening - Screening wordt in gemeente B voor alle medewerkers op dezelfde manier uitgevoerd (met uitzondering van medewerkers betrokken bij Veiligheidshuizen). De screening van nieuwe medewerkers bestaat uit een sollicitatiegesprek, het aanvragen van een functiespecifieke VOG, het inwinnen van referenties (intern en extern), een controle van diploma's, certificaten, cijferlijsten en curriculum vitae, controle van identiteitsbewijs en controle van ontslagbrieven en getuigschriften.

Gemeentelijke medewerkers worden niet periodiek gescreend en bij een interne functiewijziging wordt niet opnieuw een VOG aangevraagd. Screening vindt zowel centraal als decentraal plaats binnen de gemeente. Screening wordt meestal uitgevoerd door een teamleider, een selectiecommissie of een medewerker van de beoogde afdeling (afhankelijk van de functie) en het wordt gecoördineerd door een HR adviseur. Voor ingehuurde of gedetacheerde medewerkers geldt dat een externe partij de VOG opvraagt en een voorselectie doet. Deze externe partij wordt door interne medewerkers gecontroleerd en heeft geen toegang tot de gemeentelijke systemen.

3.3.4 Screeningsbehoefte

Het effect van screening op risicobeperking wordt betwijfeld - Binnen gemeente B wordt beperking van risico's door zwaardere vormen van screening betwijfeld. Volgens gemeente B draait het vooral om permanente hygiëne van de gemeentelijke organisatie, ook als medewerkers al (vele jaren) in dienst zijn. Handelen op basis van goed vertrouwen is hierbij het fundament voor de meeste functies.

Voor een aantal kwetsbare functies kan de inzet van zwaardere screening volgens gemeente B wel van meerwaarde zijn - Bij zwaardere screening denkt de gemeente bijvoorbeeld aan een BKR check, periodiek aanvragen van een VOG of het checken van informatie uit politiesystemen. Zwaardere screening wordt als gelegitimeerd gezien vanuit het beperken van de risico's met betrekking tot het openbaar bestuur, het onderwerp ondermijning en voor zware (financiële) functies.

De gemeente is indien nodig bereid hier intern het gesprek over aan te gaan met medewerkers. In de interviews is echter naar voren gebracht dat goed moet worden nagedacht over het continuüm tussen paranoia, naïviteit, privacy en welke screeningsmethodieken acceptabel worden geacht, wanneer en voor welke functie.

Gemeente B ervaart geen externe druk om zwaardere screening uit te voeren - Vanuit de ketenpartners of samenwerkingsverbanden komen geen signalen van behoefte aan extra screening van gemeenteambtenaren in het veiligheidsdomein. Ook is er vanuit de partners geen sprake van terughoudendheid bij het delen van informatie; dit wordt op basis van gevestigd goed vertrouwen gedeeld. Op voorhand is niet te zeggen of dit ook het geval zal zijn indien er nieuwe medewerkers van de gemeente betrokken worden bij een ketenoverleg.

3.4 Gemeente C

3.4.1 Contextschets

Gemeente C ligt in de Randstad en heeft een inwoneraantal tussen de 50.000 en 100.000. De gemeente bevindt zich in de nabijheid van een van de grote steden en heeft mede daarom te maken met georganiseerde criminaliteit en grootstedelijke problematiek. In het kader van de case studie hebben we gesproken met de loco gemeentesecretaris, Unithoofd Juridische Zaken en projectleider Ondermijning en de senior P&O manager.

3.4.2 Kwetsbare functies

Binnen het veiligheidsdomein zijn geen specifieke kwetsbare functies geïdentificeerd - Bij gemeente C zijn binnen het veiligheidsdomein geen kwetsbare functies aangewezen. Wel leeft binnen het veiligheidsdomein, en in het bijzonder binnen de afdeling die zich richt op de bestrijding van ondermijning, het besef dat medewerkers kwetsbare functies bekleden. De kwetsbaarheid van de functie zit met name in de beschikking over (mogelijk) gevoelige informatie, in het bijzonder casusinformatie gerelateerd aan ondermijnende activiteiten. Dit maakt, aldus gemeente C, de gemeente kwetsbaar maar ook de medewerkers zelf, doordat medewerkers door derden onder druk gezet kunnen worden om informatie te delen.

Binnen het veiligheidsdomein wordt geen risicoanalyse gemaakt, wel wordt impliciet een onderscheid gemaakt in risiconiveaus - Er wordt geen risicoanalyse gemaakt en er worden geen risicoprofielen gehanteerd. Impliciet worden wel verschillende risiconiveaus onderscheiden. Medewerkers van de afdeling personeelszaken en het project ondermijning zijn alerter op het moment dat een functie door henzelf als kwetsbaar(der) wordt geduid. Leidend daarin is de informatie waarover een ambtenaar kan beschikken. Een analist, projectleider ondermijning, BIBOB-functionaris en projectsecretaris kunnen de meeste informatie inzien (zoals strafdossiers) en worden vanuit het project ondermijning gezien als zeer kwetsbaar. Dit geldt (in mindere mate) ook voor deelprojectleiders binnen het project ondermijning en voor handhavers, omdat zij ook beschikken over informatie op casusniveau. Dit impliciete onderscheid in risiconiveaus is niet door vertaald naar verschillende vormen van aanvullende of zwaardere screening voor verschillende functies.

Ook buiten het veiligheidsdomein worden kwetsbare functies gezien - Kwetsbare functies en processen buiten het veiligheidsdomein betreffen medewerkers die betalingen verrichten bij de afdeling financiën, medewerkers die veel contacten hebben met burgers en bedrijven, medewerkers die betrokken zijn bij vastgoed en medewerkers betrokken bij inkoop / aanbestedingen, subsidies, vergunningen en handhaving.

3.4.3 Inzet instrumentarium

Binnen het veiligheidsdomein worden diverse (aanvullende) maatregelen genomen om risico's in te perken - Gemeente C geeft aan dat ook binnen het veiligheidsdomein de gemeentelijke gedragscode van kracht is. Daarnaast dient door de medewerkers de ambtseed te worden afgelegd. Binnen het project ondermijning gelden daarnaast nog een aantal aanvullende maatregelen. Zo dienen medewerkers die deel uitmaken van het zogenaamde kernteam (onderdeel van het project ondermijning) waarin casuïstiek wordt besproken, een geheimhoudingsverklaring te ondertekenen waarmee ze aangeven informatie uit het overleg niet met derden te delen. Ook wordt binnen het project ondermijning gewerkt met het vierogenprincipe, waarbij de koppels regelmatig wisselen. Ook wordt binnen het eerdergenoemde kernteam regelmatig over integriteit en weerbaarheid gesproken.

Nog niet alle risico beperkende maatregelen worden volgens gemeente C optimaal ingezet - Binnen het project ondermijning wordt gewerkt aan aanvullende maatregelen om risico's op het gebied van integriteit te beperken. Het gaat hierbij om fysieke maatregelen als het afschermen van werkplekken en het inzichtelijk maken van mutaties binnen systemen zodat duidelijk is door wie deze zijn doorgevoerd (logging), maar ook om organisatorische maatregelen als het invoeren van intervisie en dilemmatrainingen voor medewerkers. Het project ondermijning loopt hierin voor op andere afdelingen binnen de gemeente. Aangegeven wordt dat het nog wel een ontdekkingstocht is welke risico's precies spelen en op welke manier deze het beste kunnen worden ingeperkt. Dit houdt tevens in dat nog verbeteringen mogelijk zijn in het optimaal inzetten van risico beperkende maatregelen.

Er wordt beperkt onderscheid gemaakt tussen kwetsbare en reguliere functies bij de screening - Screening wordt bij alle nieuwe medewerkers op dezelfde manier uitgevoerd, de nadruk ligt hierbij op competenties en niet op integriteitsaspecten. In de pre-employmentfase vindt een sollicitatiegesprek plaats en wordt er soms navraag gedaan bij referenten, maar dit aspect is niet opgenomen in beleidsdocumenten of werkprocessen. Een referentencheck wordt volgens betrokkenen eerder gedaan bij kandidaten voor kwetsbare functies, maar hier zijn geen expliciete afspraken over gemaakt. De beoordeling of referenties worden gecheckt voor sollicitanten in het veiligheidsdomein, wordt bepaald door de afdeling zelf in overleg met personeelszaken.

Er wordt beperkt aanvullend onderzoek gedaan voordat een medewerker wordt aangenomen. Dit kan bestaan uit het raadplegen van openbare bronnen, maar dit is niet beleidsmatig vastgelegd. Het credo hierbij is: ‘Zo lang het openbaar is, mag het gebruikt worden in de procedure.’ Er wordt geen bewuste afweging gemaakt met betrekking tot privacyaspecten, maar er worden wel stappen gezet om privacy intern te borgen en onder de aandacht te brengen.

Alle medewerkers dienen bij indiensttreding een VOG te overleggen - De VOG wordt specifiek aangevraagd voor het profiel van de functie van de medewerker. Op het moment dat een medewerker overstapt naar een andere functie hoeft er geen nieuwe VOG te worden aangevraagd, ook niet als dit een kwetsbare functie betreft.

In 2017 is een collegebesluit genomen over het periodiek overleggen van een VOG. Ook ingehuurde medewerkers dienen een VOG te overleggen. Daarnaast dienen werkgeversgegevens (zoals gegevens uit het Handelsregister) van de ingehuurde medewerker te worden ingevoerd in een inkoopsysteem.

3.4.4 Screeningsbehoefte

Meerdere functies worden als dusdanig kwetsbaar bestempeld dat zwaardere screening nodig is, dit geldt voor meerdere afdelingen - De kwetsbaarheid is enerzijds gelegen in de informatie (deels afkomstig van samenwerkingspartijen) waarover medewerkers kunnen beschikken en anderzijds in de kwetsbaarheid van de medewerker zelf in relatie tot druk van buitenaf. Dit vergroot tegelijkertijd de kwetsbaarheid van de gemeente, waardoor extra waarborgen zoals zwaardere screening op zijn plaats zijn. Enkel organisatorische en fysieke maatregelen zijn volgens de gemeente onvoldoende om risico’s in te perken. De behoefte aan zwaardere screening is momenteel actueel bij het project ondermijning. Binnen dit project is sprake van koppeling van informatiesystemen, wat de functies binnen het project extra kwetsbaar maakt. De verwachting is echter dat de behoefte aan zwaardere screening ook speelt, danwel gaat spelen, binnen andere afdelingen; het niveau van bewustwording is echter niet binnen alle afdelingen gelijk.

Er is geen sprake van externe druk met betrekking tot zwaardere screening - De behoefte tot zwaardere screening komt vanuit gemeente C zelf, niet vanuit politie of andere ketenpartners. Volgens gemeente C is het laten uitvoeren van zwaardere screening wel overwogen door het RIEC, maar gezien de beschikbare capaciteit voor deze screening is hiervan afgezien. De uitwisseling van informatie met ketenpartners verloopt goed en er zijn procesmatig afspraken vastgelegd in diverse

convenanten, waarbij een privacy impact assessment (PIA) het uitgangspunt vormde. Er zijn geen nadere afspraken gemaakt over eisen aan screening van gemeentelijke medewerkers.

3.5 Gemeente D

3.5.1 Contextschets

Gemeente D betreft een 100.000+ gemeente in de Randstad. Integriteit en ondermijning zijn belangrijke aandachtspunten binnen deze gemeente. Ook heeft de gemeente op regelmatige basis te maken met georganiseerde criminaliteit, ondermijning, radicalisering en overige stedelijke problematiek. In het kader van de case studie hebben we gesproken met het hoofd Integriteit, directeur en medewerkers OOV en medewerkers P&O.

3.5.2 Kwetsbare functies

Binnen het veiligheidsdomein wordt geen expliciete risicoanalyse gemaakt - Het veiligheidsdomein is zelf verantwoordelijk voor identificatie van kwetsbare functies. Bij gemeente D wordt geen centrale regie gevoerd op de identificatie van kwetsbare functies; deze verantwoordelijkheid is decentraal bij de diverse domeinen zelf belegd. Binnen het veiligheidsdomein wordt niet gewerkt met risicoprofielen of risiconiveaus van bepaalde functies. Wel is sprake van een impliciete risicobeoordeling en -weging van functies omdat wordt nagedacht over de mate waarin een bepaalde functie risico's oplevert bij het aanvragen van een VOG.

Er lopen binnen de gemeente verschillende initiatieven om meer zicht te krijgen op kwetsbare functies – Gemeente D is voornemens om in het kader van de implementatie van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en het daaruit voortvloeiende informatiebeveiligingsplan van CIO en CISO, kwetsbare functies te benoemen in relatie tot gevoelige informatie, gegevens of aspecten als bevoegdheden of externe contacten.

3.5.3 Inzet instrumentarium

Er worden diverse organisatorische en fysieke maatregelen getroffen om risico's in te perken - Gemeentebreed is onlangs een nieuwe gedragscode opgesteld en het is recentelijk mogelijk geworden om maandelijks de ambtseed af te leggen. Het doel van het afleggen van de ambtseed is om medewerkers bewust te maken van de uitgangspunten voor goed ambtelijk handelen. Om deze reden wil de gemeente dat nieuwe werknemers de eed zo snel mogelijk na indiensttreding afleggen. Verder is het HR-systeem zodanig ingericht dat eerst een VOG geüpload dient te worden voordat een nieuw personeelsnummer en inlogaccount aangemaakt kunnen worden. Dit geldt tevens voor stagiairs en externe medewerkers en zij dienen verder een geheimhoudingsverklaring en integriteitsverklaring te ondertekenen omdat zij geen ambtseed afleggen. Met de verklaring wordt een externe medewerker tegelijkertijd een handelingskader geboden.

Binnen het veiligheidsdomein gelden aanvullende risico beperkende maatregelen – Binnen het veiligheidsdomein worden hard controls toegepast door middel van de afscherming van het domein met een fysieke toegangscontrole en een deur met bel. Er is geen sprake van structurele aandacht voor het thema integriteit, maar er wordt wel gewerkt aan bewustwording in gesprekken en dilemmasessies. Ook wordt aan de hand van een programma, gericht op het tegengaan van

fraude, aandacht aan het onderwerp besteed en wordt er in het kader van dit programma de komende tijd geëxperimenteerd met functieroulatie. Integriteitsbesef zit volgens betrokkenen in de haarvaten van het veiligheidsdomein. Medewerkers zijn zich volgens hen zeer bewust van de risico's en kwetsbaarheden van hun werk.

Beleid met betrekking tot screening is decentraal belegd - Omdat er geen gemeentebrede regels zijn over screening, bepalen de domeinen zelf wat en waarvoor zij screenen. Binnen het veiligheidsdomein kan daar invulling aan worden gegeven door referenties te raadplegen of openbaar bronnenonderzoek te verrichten, maar hier is geen kader voor opgesteld.

De aard van de screening hangt doorgaans af van een persoonlijke risico-inschatting van degene die verantwoordelijk is voor het aannemen van de medewerker, eventueel in afstemming met de afdeling personeelszaken. Deze verantwoordelijke is over het algemeen een leidinggevende binnen het veiligheidsdomein zelf.

Alle medewerkers dienen bij indiensttreding een VOG te overleggen - Voor alle nieuwe medewerkers wordt een VOG met functiebeschrijving aangevraagd. Juist over het verplicht overleggen van een VOG is in het afgelopen jaar gemeentebreed discussie geweest. Gemeente D geeft aan dat jongeren die in het verleden een misstap hebben begaan moeilijk aan een baan bij de gemeente zouden kunnen komen.[52]

Er is sprake van zwaardere screening binnen het veiligheidsdomein - Alle medewerkers van de afdeling handhaving en toezicht die een politiegebouw kunnen betreden krijgen een 'BGO', aldus gemeente D. De afdeling handhaving en toezicht neemt het verkrijgen van de 'BGO', net als de VOG, als ontbindende voorwaarde op in de aanstelling van de nieuwe medewerker. Er is binnen de gemeente discussie over de wettelijke grondslag voor uitvoering door de politie van een BGO, omdat het vaak onduidelijk is op welke gronden de politie het advies baseert. Indien de aspirant medewerker geen BGO krijgt, dan staat hem door het ontbreken van een wettelijke basis geen bezwaar- en beroepsprocedure ter beschikking, wel kan hij een 'hoorgesprek' aangaan met de politie. Medewerkers uit het veiligheidsdomein plaatsen de waarde van een VOG enigszins in perspectief, doordat het een momentopname is en beperkte informatie over een persoon geeft.

De gemeente geeft aan dat het goed zou zijn om het thema screening nader uit te werken en onderscheid te maken tussen reguliere checks in een selectieproces (hierbij ziet de gemeente de volgende bronnen als regulier: referentiecheck, diplomacheck, openbaar bronnenonderzoek, aanvraag VOG) en screening in uitgebreidere vorm (zoals een assessment, gesprek met de vorige werkgever en een milieu- en antecedentenonderzoek door politie / AIVD).

3.5.4 Screeningsbehoefte

De behoefte aan zwaardere screening in het veiligheidsdomein is niet eenduidig - Voor gemeente D is het nog niet helder of er behoefte is aan zwaardere vormen van screening binnen

[52] Justis heeft een campagne opgezet over het informeren van jongeren over een VOG. Niet ieder misdrijf zorgt ervoor dat er geen VOG meer verkregen kan worden. Zie ook: https://watdevog.nl/#wat-de-vog

het veiligheidsdomein, de behoefte is nog niet in kaart gebracht en de meningen zijn verdeeld. Het in kaart brengen van deze behoefte begint bij het identificeren van risico's, waarbij de vraag gesteld moet worden of zwaardere vormen van screening een oplossing kunnen bieden bij het tegengaan van deze risico's. Daarnaast speelt ook de praktische haalbaarheid van screening een rol in verband met capaciteitsproblemen bij de politie als die ineens een groot aantal gemeentelijke medewerkers dient te screenen.[53] Een andere stroming binnen de gemeente geeft aan dat voor sommige functies binnen het veiligheidsdomein waar gewerkt wordt met informatie van politie en justitie, zeker diepergaande screening nodig is. Deze screening zou dan kunnen bestaan uit een screening die gelijk is aan die van politieambtenaren. Naast screening dient ook aandacht te zijn voor begeleiding, personele zorg en monitoring van medewerkers in de employmentfase.

Medewerkers binnen het veiligheidsdomein hebben geen toegang tot alle informatie van ketenpartners - Voor de uitwisseling van informatie zijn convenanten afgesloten tussen de gemeente en samenwerkingspartners. Er wordt door gemeente D aangegeven dat medewerkers van het veiligheidsdomein soms niet aanwezig mogen zijn bij bepaalde overleggen met ketenpartners omdat zij onvoldoende gescreend zijn om over bepaalde informatie te mogen beschikken. Enerzijds stellen medewerkers uit het veiligheidsdomein dat dit prima is omdat de gemeente geen eigenaar van de informatie is en ze niet alles hoeven en willen weten. Anderzijds wordt de beperking in informatiedeling en het niet aanwezig mogen zijn bij bepaalde overleggen soms als lastig ervaren omdat de gemeente dan niet kan meebeslissen. Het willen meepraten in overleggen en de versteviging van de gemeentelijke informatiepositie zou daarom een aanleiding kunnen zijn om over te gaan op zwaardere vormen van screening. Het veiligheidsdomein heeft hier echter nog geen standpunt over ingenomen.

3.6 Gemeente E

3.6.1 Contextschets

Gemeente E betreft een 100.000+ gemeente gelegen in de Randstad. De gemeente heeft te maken met onder andere vraagstukken rondom georganiseerde criminaliteit en radicalisering. In het kader van de case studie hebben we gesproken met de beleidsadviseur van de afdeling Openbare Orde en Veiligheid.

3.6.2 Kwetsbare functies

Op basis van een risicoanalyse zijn kwetsbare functies in het veiligheidsdomein in kaart gebracht - De analyse van kwetsbare functies is verricht op basis van de 'Leidraad aanwijzen vertrouwensfuncties' van de AIVD en de folder 'Screening van personeel' van Justis. Uit deze risicoanalyse kwam naar voren dat er vooral een vraagstuk zit bij mensen op posities waar over veel informatie beschikt wordt, in combinatie met een bepaalde bevoegdheid of andere kenmerken (zoals verstrekken van vergunningen of inkoop). De conclusie van de analyse was dat bepaalde

[53] De discussie over zwaardere screening wordt deels gekoppeld aan screening door de politie, waarbij zoals eerder genoemd voor de huidige uitvoeringspraktijk nog naar een permanente oplossing wordt gezocht.

functies binnen het veiligheidsdomein overeenkomen met de vereisten die gesteld worden aan een vertrouwensfunctie. De bijbehorende functies zijn in afstemming met politie en RIEC als dusdanig risicovol aangemerkt dat extra screening (een 'BGO-lang') wordt uitgevoerd: leidinggevenden veiligheidsdomein, medewerkers ondermijning, medewerkers RIEC, adviseur driehoek en adviseur BIBOB. De screening van deze medewerkers wordt al enige jaren uitgevoerd door de politie.[54]

3.6.3 Inzet instrumentarium

Er worden diverse organisatorische en fysieke maatregelen getroffen om risico's in te perken - Binnen de gemeente is een gedragscode van kracht. Daarnaast dienen nieuwe medewerkers de ambtseed af te leggen en volgen zij introductiedagen na indiensttreding. Tijdens deze dagen wordt uitgebreid stilgestaan bij integriteit en de relatie tot de afgelegde ambtseed. Verder maakt integriteit deel uit van de gesprekscycli met medewerkers en wordt er om de zoveel tijd een campagne gestart over integriteit. Overige risico beperkende maatregelen bestaan uit het dragen van pasjes en fysieke beveiliging van de verschillende afdelingen. Daarnaast wordt gewerkt met het vierogenprincipe bij bepaalde kritische bedrijfsprocessen of rollen / functies. Deze maatregelen zijn volgens gemeente E echter niet voldoende om de risico's in te perken.

Alle medewerkers dienen bij indiensttreding een VOG te overleggen - Naast het overleggen van een VOG heeft de gemeente naar verschillende methodieken gekeken om de veiligheid beter te garanderen (zoals het checken van referenties, openbare bronnen en cv). De controles hierop worden decentraal uitgevoerd; er is geen centrale dienst of afdeling die dit controleert. In vacatures wordt aangegeven dat er onderzoek in openbare bronnen wordt gedaan; de gemeente is zich er van bewust dat voor het verrichten van openbaar bronnenonderzoek mogelijk geen juridische basis is.

Vanaf 2018 wordt een periodieke VOG verplicht gesteld door gemeente E - Vanaf 1 januari 2018 wordt een periodieke VOG die om de vijf jaar moet worden aangevraagd voor alle medewerkers van de gemeente verplicht. Ook moet voor iedere interne overplaatsing een nieuwe VOG worden aangevraagd als het risicoprofiel van de oude en nieuwe functie van elkaar afwijken.

Voor alle externe krachten (uitzendkrachten, gedetacheerden en stagiairs) wordt een getekende geheimhoudingsverklaring en vanaf 1 januari 2018 een VOG verplicht gesteld.

Er is sprake van zwaardere screening binnen het veiligheidsdomein - Het Management van het veiligheidsdomein heeft in samenspraak met de politie en het RIEC gekozen om voor de functies die vitale informatie onder ogen kunnen krijgen een 'BGO' uit te laten voeren door de politie. Enkel een VOG verschaft geen inzicht in zaken die nog niet tot een veroordeling hebben geleid en een 'BGO' mogelijk wel, aldus gemeente E. Hierbij zijn de gevoeligheid, de samenhang van de informatie en de positie van personen in de organisatie van belang. Het screeningsvraagstuk is in het veiligheidsdomein eerder op de radar gekomen doordat een aantal medewerkers een politieachtergrond heeft.

---

[54] Zie de eerdere opmerkingen over de huidige uitvoeringspraktijk van screening door de politie in voetnoot 53.

De beoordeling van welke vorm van screening relevant is zou volgens gemeente E moeten afhangen van de inhoud van de functie en het soort informatie waar de functionaris over kan beschikken. Op dit moment wordt dit decentraal door de domeinen zelf bepaald, waardoor bepaalde functies niet aan zware screening onderworpen worden terwijl ze wel toegang hebben tot gevoelige informatie. Wellicht moet hier gemeentebreed beleid op gevormd worden aldus gemeente E.

3.6.4 Screeningsbehoefte

Er is behoefte aan uitbreiding van screening en landelijke standaarden - Er vindt nu reeds extra screening plaats maar dit kent geen wettelijke basis. De ratio achter deze behoefte is dat medewerkers op bepaalde functies over dusdanig gevoelige informatie kunnen beschikken dat extra screening geboden is. Deze functies beperken zich niet tot het veiligheidsdomein. Volgens gemeente E zou ten aanzien van een aantal functies (zoals MT-leden en medewerkers in het veiligheidsdomein) een generieke landelijke standaard ontwikkeld kunnen worden ten aanzien van screening, mits er wel ruimte voor maatwerk blijft. Daarnaast dient sprake te zijn van een continue heroverweging van screeningsmogelijkheden. Er zijn namelijk thema's die gaan spelen en weer gaan liggen.

Er is sprake van externe druk met betrekking tot zwaardere screening - De behoefte van gemeente E aan zwaardere screening komt tevens voort uit eisen van samenwerkingspartners. De politie heeft de eis[55] gesteld om in bepaalde veiligheidsdomeinkaders en bij verwerking van bepaalde gegevens in samenwerkingsverband dat medewerkers van de gemeente die aan tafel zitten een screening ondergaan die vergelijkbaar is met die van de politieambtenaren, aldus gemeente E.

3.7 Instellingen

In het kader van dit onderzoek is bij een viertal niet-gemeentelijke instellingen gevraagd naar de huidige wijze van screening: de Politie, de Belastingdienst, de inspectie SZW en het Uitvoeringsinstituut Werknemersverzekeringen (UWV). De reden om deze instellingen in dit onderzoek mee te nemen, is dat aan de eerste drie instellingen justitiële gegevens worden verstrekt op grond van het Bjsg en het UWV vanuit haar wettelijke taken veel bijzondere (medische) persoonsgegevens verwerkt.

Onderstaand is een beschrijving opgenomen per instelling van identificatie van risicovolle functies / taken, risico-inventarisatie, risico beperkende maatregelen, onderbouwing en grondslag van screening. De beschrijvingen zijn gebaseerd op de huidige situatie van wet- en regelgeving en geven het beeld vanuit de instellingen weer.

[55] De politie heeft deze eis laten vallen omdat de eis niet was gebaseerd op wet- en regelgeving.

Politie

Uit de informatie die de Politie heeft aangeleverd, blijkt dat deze het belangrijk vindt dat de politieorganisatie bestaat uit betrouwbare en integere medewerkers. In een organisatie die de wet handhaaft, is geen plaats voor mensen die het zelf niet zo nauw nemen met de wet of een risico kunnen vormen. De politieorganisatie heeft een cruciale rol in de samenleving als het gaat om handhaving, opsporing en hulpverlening. De Politie beschikt over gevoelige informatie en zeer veel informatie die voor zeer veel partijen, waaronder criminelen, interessant is. Om de belangen van de organisatie te beschermen, is het belangrijk om bij het aannemen van nieuwe medewerkers grondig te screenen. Ook in sommige gevallen waar sprake is van inhuur en toegang tot gevoelige informatie danwel een positie die de belangen kan beschadigen, screent de politie eveneens.

Screening bij de politie gebeurt minimaal door middel van een VOG. Bij de aanstelling als politieambtenaar wordt gescreend door middel van een onderzoek naar de betrouwbaarheid en geschiktheid (BGO) op grond van art. 8a van het Besluit algemene rechtspositie politie (Barp). De kandidaat wordt vooraf medegedeeld dat, nadat diens geschiktheid en bekwaamheid voor de desbetreffende functie (vooralsnog) is vastgesteld, een BGO zal worden ingesteld. Er kan opnieuw een onderzoek worden gedaan indien bijvoorbeeld sprake is van wijziging van werkzaamheden, bij aanstelling in een andere functie en bij de vervulling van een functie gedurende ten minste vijf dienstjaren.

Het onderzoek wordt uitgevoerd op basis van het Barp en het Protocol Betrouwbaarheids- en geschiktheidsonderzoek politie 2014. Hierin is opgenomen dat een BGO bestaat uit persoonsgegevens uit de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens, raadpleging van vrij toegankelijke informatiebronnen, navraag bij referenten en een gesprek met betrokkene. De onderzoeken worden uitgevoerd door de afdelingen Veiligheid, Integriteit en Klachten (VIK), door speciaal opgeleide medewerkers. Mede afhankelijk van het risico op schade aan de taakuitoefening of het imago van de politie, de duur van de werkzaamheden en/of de vertrouwelijkheid van de werkomgeving wordt er een BGO-kort[56] of een BGO-lang[57] uitgevoerd. De gegevens worden verwerkt in een omgeving die technisch gescheiden is van de operationele politiesystemen.

Voor de vervulling van een vertrouwensfunctie bij de politie is een VGB vereist. Onder mandaat van de AIVD voert de politie, de afdeling VIK, zelf een deel van de veiligheidsonderzoeken uit die zijn toegespitst op kwetsbaarheden in de betreffende vertrouwensfuncties binnen de politie, de

[56] Een BGO-kort bestaat uit: invullen formulier opgave persoonlijke gegevens (opg) en raadpleging van persoonsgegevens zoals bedoeld in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens en raadpleging van gegevens uit vrij toegankelijke informatiebronnen

[57] Een BGO-lang bestaat uit: a. invullen formulier opgave persoonlijke gegevens (opg); b. opvragen overzicht Bureau Krediet Registratie (BKR); c. raadpleging van persoonsgegevens zoals bedoeld in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens en raadpleging van gegevens uit vrij toegankelijke informatiebronnen; d. navraag bij referenten; e. gesprek met de onderzoeker.

zogenaamde P-onderzoeken (het betreft een variant van een B veiligheidsonderzoek).
Het veiligheidsonderzoek omvat het instellen van een onderzoek naar gegevens die uit het oogpunt van de nationale veiligheid van belang zijn voor de vervulling van de desbetreffende vertrouwensfunctie. Hierbij wordt uitsluitend gelet op de gegevens die in art. 7 van de Wvo worden genoemd, bijvoorbeeld gegevens uit de Wjsg, Wet politiegegevens, gegevens die de nationale veiligheid kunnen schaden. Met betrekking tot de partner van de betrokkene (indien van toepassing), worden in beginsel de gegevens over een periode van vijf jaar direct voorafgaande aan de aanmelding voor een veiligheidsonderzoek beoordeeld.[58]

Voor medewerkers die een aanstelling krijgen, intern doorstromen naar een nieuwe functie, of aspiranten die de politieopleiding gaan volgen, wordt de screening aangevraagd door HRM. Doorstroom vereist volgen de Politie geen screening, het kan wel maar is geen vereiste. Wel kan een veiligheidsonderzoek vereist zijn als men doorstroomt naar een vertrouwensfunctie. Bij inhuur wordt gekeken naar de werkzaamheden en soms kan worden volstaan met een VOG, soms een BGO-kort en soms een BGO-lang. Voor personen die worden ingehuurd is de dienst Facility Management de opdrachtgever voor de screening.

Van leveranciers wordt standaard een VOG gevraagd, maar in bijzondere gevallen kan bij een aanbesteding van een bepaalde dienstverlening ook wel worden gevraagd om medewerkers die beschikken over een VGB van een bepaald niveau. Denk bijvoorbeeld aan het aanbesteden van de uitvoering van penetratietesten.[59]

Inspectie SZW

Volgens de Inspectie SZW komt het beleid ten aanzien van screening voort uit het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI 2013) en de Baseline Informatiebeveiliging Rijksdienst (BIR). Bijzondere informatie wordt op grond van de VIRBI 2013 zodanig beveiligd dat alleen personen die daartoe zijn geautoriseerd deze kunnen behandelen of inzien voor zover dit noodzakelijk is voor een goede uitoefening van hun taak en dat inbreuken op de beveiliging worden gedetecteerd en gedegen onderzoek naar (mogelijke) inbreuken mogelijk is. De beveiliging is ingericht op basis van risicomanagement.

Alle interne en externe medewerkers dienen te worden gescreend voorafgaand aan indiensttreding of bij functiewijziging. De grondslag voor screening ligt in de Ambtenarenwet en het Algemeen Rijksambtenarenreglement. Er wordt gebruik gemaakt van risicoprofielen conform de Leidraad aanwijzen vertrouwensfuncties (2014) en het VIRBI. Deze risicoprofielen zijn onderbouwingen in verband met de data waarmee bepaalde mensen in aanraking komen. Ook binnen alle data is er

[58] Zie art. 2 van de Beleidsregel beoordelingsperiodes en onvoldoende gegevens veiligheidsonderzoeken. Voorgaande wordt binnenkort vervangen door de Beleidsregel veiligheidsonderzoeken waarin geen onderscheid meer wordt gemaakt tussen A-, B- en C-onderzoeken.

[59] Het doel van penetratietesten is het verkrijgen van inzicht in de status en effectiviteit van de ICT beveiligingsmaatregelen.

nog een onderscheid van classificaties waarop deze risicoprofielen/onderbouwingen betrekkingen hebben. Niet iedereen mag dus overal bij (het need-to-know principe). Reguliere medewerkers (intern en extern) van de Inspectie SZW moeten een VOG overleggen omdat zij allen tenminste structurele toegang hebben tot Departementaal Vertrouwelijke informatie, denk hierbij aan ARBO onderzoeken, of onderzoeken naar frauduleuze handelingen. Voor vertrouwensfuncties wordt een Verklaring van geen bezwaar gevraagd (VGB) aan de AIVD conform de zwaarte van het functieprofiel.

Voor inspecteurs binnen Toezicht met een Bijzondere Opsporingsbevoegdheid, geldt eveneens dat een VOG noodzakelijk is voor het verkrijgen van het certificaat (het certificaat is een AOA pas waarmee algemene opsporingsbevoegdheid wordt verkregen). Zij dienen voor het verkrijgen van hun certificaat (en het vernieuwen ervan) voor hun algemene opsporingsbevoegdheid eveneens een VOG te overhandigen. Dit is dus naast de VGB die zij al hebben. Alle medewerkers die in aanraking komen met staatsgeheime informatie dienen een VGB van de AIVD te krijgen.

Voor de aanwijzing van vertrouwensfuncties voor personen die toegang hebben tot Bijzondere Informatie (structurele toegang tot of omgang met staatsgeheime informatie en/of politiegegevens) wordt gebruik gemaakt van de Leidraad aanwijzen vertrouwensfuncties (2014).

De lijst wordt vastgesteld door de secretaris generaal van het Ministerie van SZW. De lijnmanager is verantwoordelijk voor het (laten) uitvoeren door de AIVD van de screenings voor vertrouwensfuncties bij aanstelling of functiewijziging en het uitvoeren van de herhaalonderzoeken binnen de gestelde termijn. De Beveiligingsambtenaar (BVA, zie Beveiligingsvoorschrift Rijk 2013) bewaakt dit proces. In enkele gevallen wordt er vanwege de samenwerking binnen Europees verband (bijvoorbeeld Europol) een Europees screeningsonderzoek uitgevoerd. Indien er sprake is van een vertrouwensfunctie wordt een veiligheidsonderzoek uitgevoerd. Gegevens voor veiligheidsonderzoeken van de AIVD worden in een gesloten envelop ingestuurd. De verklaringen (of de mededeling over het niet afgeven daarvan) komen bij de Beveiligingsambtenaar binnen.

Naast voorgaande mogelijkheden vinden er controles plaats op diploma's en certificaten. Tevens dient de identiteit te worden vastgesteld en zijn de medewerkers verplicht nevenfuncties te melden of zaken die de integriteit kunnen beïnvloeden. De lijnmanager is verantwoordelijk voor de screening. De HR-ondersteuner bewaakt het proces. Het staat ter afweging van de manager zelf of navraag wordt gedaan bij referenten. Een VOG wordt door de medewerker zelf bij de gemeente ingediend, een afschrift wordt toegevoegd in het personeelsdossier (hiertoe hebben enkel gemachtigden toegang).

Voor extern personeel geldt dat zij een VOG moeten afgeven en een geheimhoudingsverklaring dienen te ondertekenen.

Uitvoeringsinstituut Werknemersverzekeringen (UWV)

De reden van het UWV voor het screenen is enerzijds om medewerkers bewust te maken van de risico's en met name de gevoeligheid van de gegevens waar ze mee omgaan. Anderzijds heeft het UWV de maatschappelijke plicht om met de vertrouwelijke gegevens van de burger zeer zorgvuldig om te gaan. Voor het UWV geldt er geen wettelijke verplichting om personeel bij indiensttreding of

op andere relevante momenten te screenen. Het UWV heeft de Baseline Informatiebeveiliging Rijksdienst geadopteerd en daarin staat beschreven dat bij indiensttreding alle medewerkers (intern en extern) een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag overleggen. De maatschappelijke plicht om 'als goed huisvader' met onder meer de gegevens van derden zorgvuldig om te gaan, is te vinden in de Wet structuur uitvoeringsorganisatie werk en inkomen waarin is opgenomen dat het UWV verwerker is in de zin van de Wbp (bijvoorbeeld bij het verwerken van werknemergegevens over arbeidsverhouding en uitkeringsverhouding) en dat het UWV op de voet van de ter zake voor de Rijksdienst geldende voorschriften zorgt voor de nodige technische en organisatorische voorzieningen ter beveiliging van hun gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens.

Sinds 1 januari 2017 zijn twee niveaus van screening vastgesteld. Met betrekking tot niveau 1 worden screenings voor eigen personeel door de manager of afdeling HRM uitgevoerd. Op basis van een risico-inventarisatie wordt beoordeeld welke functies in aanmerking komen voor het tweede of derde niveau van screening. Voor het tweede niveau is een functierisicobeoordelingsmatrix[60] opgesteld. Het derde niveau is, in afwachting van goedkeuring door de OR, vooralsnog van toepassing voor een beperkte groep medewerkers (functies binnen de data-analyse) waarvoor een beslisboom is opgesteld. Aanvullende screeningsinstrumenten voor niveau 3 kunnen ingezet worden als de kandidaat data-analyses kan maken op basis van de databronnen, dat er een mogelijkheid is om databronnen te combineren of databestanden samen te stellen, en als alle in redelijkheid te nemen fysieke en organisatorische maatregelen om misbruik te voorkomen zijn genomen. In andere gevallen wordt het inzetten van aanvullende screeningsinstrumenten niet vereist omdat deze een te grote inbreuk op de persoonlijke levenssfeer van de medewerker zijn of omdat de zwaarte van de aanvullende screeningsinstrumenten niet opweegt tegen het risico dat het UWV loopt. Voor het derde niveau van screening gaat gebruik gemaakt worden van een externe partij vanwege de objectiviteit en professionaliteit van de screening. De opdrachtgever voor de externe partij wordt het Bureau Integriteit van het UWV. Dit bureau beoordeelt of de informatie uit de screening tot mogelijke risico's leidt waarna met de betreffende manager wordt besproken op welke wijze hiermee omgegaan wordt.

Alle nieuwe medewerkers van het UWV dienen te beschikken over een VOG. Iedereen wordt standaard gecheckt op de sollicitatiebrief en cv, diploma's, certificaten, cijferlijsten, nevenfuncties en het identiteitsbewijs. Geheimhouding is onderdeel van de cao afspraken, tevens staat dit expliciet benoemd in het arbeidscontract.[61]
Bij managementfuncties is in de regel sprake van een grotere impact op de interne organisatie en op de verhouding met externen. Daarom is voor managementfuncties altijd het tweede niveau van

[60] Aspecten van de risicobeoordelingsmatrix zijn: vertrouwelijke informatie, omgaan met geld, machts- en monopoliepositie, toekennen van rechten of bevoegdheden, beoordelen en/of adviseren, aanschaffen goederen en/of opdrachtverlening, handhaven, solistisch handelen en werken onder de invloedsfeer van derden.

[61] Medewerkers in dienst van het UWV hebben een arbeidscontract en vallen onder de Cao UWV.

screening van toepassing. Tevens kunnen directies op basis van de functierisicobeoordelingsmatrix andere functies aanwijzen waarop het tweede screeningsniveau van toepassing is. Voor deze kandidaten worden alle voorgaande methodieken toegepast inclusief referentie check / getuigschrift, raadpleging digitale bronnen en social media en/of personeelsdossier / personeels-informatiesysteem, na schriftelijke toestemming/informeren van de sollicitant. Ook aan interne kandidaten wordt op basis van een interne regeling voor dergelijke functies gevraagd om een VOG aan te leveren. Als er geen VOG kan worden overlegd, wordt de kandidaat niet op de functie benoemd. De werving en selectie van managers die rechtstreeks aan de Raad van Bestuur rapporteren en van de managementlaag direct daaronder, wordt door HRM-concern Performance & Development op concernniveau uitgevoerd.

Het management kan ook een VOG vragen bij verlenging van een aanstelling van tijdelijke medewerkers al dan niet met omzetting naar een vast dienstverband, waarvoor bij eerdere benoeming een VOG nog niet aan de orde was.[62]

Bij uitzendkrachten en externe medewerkers komt het UWV met de instantie die uitzendt/uitleent nadrukkelijk overeen dat die instantie verantwoordelijk is voor de integriteit van de medewerker. Zowel voor uitzendkrachten als voor zelfstandigen geldt dat zij een VOG moeten aanleveren. Ook voor trainees maakt de VOG onderdeel uit van de screeningsprocedure.

Bij het verwerken van persoonsgegevens neemt het UWV de privacy wet- en regelgeving in acht. Ook de door het UWV aangezochte externe partijen dienen volledig conform deze wet- en regelgeving te werken. De gegevens worden alleen gebruikt voor de selectieprocedure en voor zover relevant opgeslagen in het personeelsdossier. De toegang tot het personeelsdossier is beperkt tot HRM medewerkers en de directe manager. Voor het derde niveau van screening, wat uitgevoerd zal worden door een externe partij, is het UWV voornemens om de gegevens zoveel mogelijk te beperken.

Belastingdienst

Volgens de belastingdienst worden alle medewerkers, kandidaten en externen (inhuur / detachering) gescreend op basis van vastgesteld beleid. De reden voor de screening is onder meer de bescherming van eigen gegevens, het invullen van goed werkgeverschap, het voldoen aan wettelijke verplichtingen en om te voldoen aan eisen van externe partijen die hun gegevens beschermen.

De belastingdienst (personeelszaken) checkt van alle sollicitanten de cv, referenties en diploma's en vereist van alle nieuwe medewerkers een VOG. Er wordt bij de toepassing van de checks geen onderscheid gemaakt tussen functies, behalve bij de Douane en de FIOD waar wel gebruik wordt gemaakt van een risicoprofiel. De afdeling personeelszaken controleert bijvoorbeeld de diploma's, certificaten en dergelijke waarnaar de sollicitant zelf verwijst in zijn sollicitatiebrief. De betreffende

[62] Overigens geldt ook hier dat het gehele instrumentarium van het tweede niveau van screening van toepassing is.

vakafdeling voert de referentencheck uit. In het kader van de bescherming van persoonsgegevens wordt gebruik gemaakt van procedures met gesloten enveloppen. Voor sommige categorieën medewerkers is een opleiding voorzien die als integriteitsassessment kan worden beschouwd.

Bij de belastingdienst zijn vertrouwensfuncties aangewezen conform de Leidraad aanwijzing vertrouwensfuncties. Indien een betrokkene een vertrouwensfunctie bij de belastingdienst wil vervullen, is een VGB vereist.

De AIVD stelt daartoe een veiligheidsonderzoek in naar de betrokkenen die of politiegegevens, of staatsgeheime gegevens kunnen inzien, alsook medewerkers die op luchthavens werkzaam zijn (juridische grondslag is hiervoor de Luchtverkeerswet).

De MIVD treedt in de plaats van de AIVD indien het een functie bij de Belastingdienst betreft die als vertrouwensfunctie moet worden aangemerkt in verband met de daarmee samenhangende noodzaak om toegang te hebben tot militaire installaties. Het veiligheidsonderzoek omvat het instellen van een onderzoek naar gegevens die uit het oogpunt van de nationale veiligheid van belang zijn voor de vervulling van de desbetreffende vertrouwensfunctie.

Medewerkers van de belastingdienst die extra risico's lopen met betrekking tot financiële belangenverstrengeling krijgen beperkingen en een meldingsplicht ter zake van financiële belangen, effectenbezit en effectentransacties opgelegd op basis van de Insiderregeling Financiën 2017. De aanwijzing als insider[63] gebeurt op voordracht van de betrokken directeur, door de compliance-officer en hij is, samen met de directeuren, belast met de uitvoering van de Insiderregeling Financiën en het actieve toezicht op de naleving van deze regeling. Op basis van deze Insiderregeling stuurt de compliance-officer de insider bij zijn aanwijzing als insider een Algemene verklaring Insiderregeling toe waarmee de desbetreffende medewerker verklaart zich te houden aan de regeling. De compliance-officer moet zich bij de uitoefening van zijn taak aan het bepaalde in de Wet bescherming persoonsgegevens houden.

[63] De aangewezen ambtenaar die werkzaamheden verricht waaraan in het bijzonder het risico van financiële belangenverstrengeling of het risico van oneigenlijk gebruik van koersgevoelige informatie verbonden is.

4. Analyse en bevindingen

4.1 Inleiding

In dit hoofdstuk analyseren we of het reeds beschikbare instrumentarium voor het uitvoeren van screening binnen het veiligheidsdomein voldoende mogelijkheden biedt voor de gemeentelijke werkgever om de eigen verantwoordelijkheden waar te maken en onder welke (rand)voorwaarden deze instrumenten ingezet kunnen worden.

In deze analyse wordt eerst aandacht besteed aan de risicovolle functies bij gemeenten in het veiligheidsdomein en hoe deze functies in beeld worden gekregen. Vervolgens komt aan bod of het bestaande screeningsinstrumentarium dat in hoofdstuk twee is beschreven door gemeenten ten volle wordt benut. Daarna wordt ingegaan op de wijze waarop de case studie gemeenten de uitvoering van screening hebben georganiseerd en of zij voldoende mogelijkheden hebben om met het beschikbare instrumentarium van risicoanalyses en screening de eigen verantwoordelijkheden waar te kunnen maken. Ten slotte wordt aangegeven welke mogelijkheden er zijn om te komen tot een optimale beperking van de veiligheidsrisico's voor gemeenten.

4.2 Zicht op risicovolle functies

De risicovolle functies die door de case studie gemeenten genoemd worden zijn onder meer: adviseur/coördinator/functionaris BIBOB, adviseur driehoek, analist team ondermijning, coördinator/medewerkers ondermijning, coördinator interne weerbaarheid, handhavers, leden van het MT en DT, medewerkers RIEC, adviseur/specialist Veiligheid, procesregisseur, projectleider ondermijning, projectsecretaris, informatie coördinator, informatieanalist, veiligheidsregisseur, teamleider veiligheidsdomein. De opsomming van risicovolle functies betreft een gevarieerde verzameling van titels / functies die per case studie gemeente een andere taakinvulling kennen, organisatorisch anders zijn ingedeeld of een andere aansturing kennen vanuit de gemeentelijke organisatie (bijvoorbeeld een aparte afdeling Veiligheidsdomein met afdelingshoofd of medewerkers die direct verantwoording afleggen aan de gemeentesecretaris).

Uit de vijf case studies blijkt dat er uiteenlopende redenen zijn om functies als risicovol aan te wijzen. Het (kunnen) beschikken over gevoelige / vertrouwelijke informatie wordt door alle case studie gemeenten genoemd als hoofdkenmerk van een risicovolle functie, in combinatie met de uitvoering van een bepaalde taak of het hebben van een bevoegdheid (bijvoorbeeld vergunningverlening, inkoop, contacten met externen, handhaving). Ook wordt aangegeven dat medewerkers in deze functies kwetsbaar worden omdat zij onder druk gezet kunnen worden om deze informatie te delen met derden.

Bij gemeente A, D en E wordt voor bepaalde functies (onder meer boa's, medewerkers RIEC, Afdeling Handhaving en Toezicht en, teamleiders veiligheidsdomein, medewerkers team ondermijning et cetera) in het veiligheidsdomein een screening uitgevoerd zoals bij

politieambtenaren[64] en dit geeft aan dat deze functies als risicovol worden gezien. Dit heeft dus niet alleen te maken met het kunnen beschikken over bepaalde informatie maar ook over het bekleden van bijvoorbeeld een positie als leidinggevende of een functie op het gebied van handhaving.

Uit de case studies komt verder naar voren dat de onderzochte gemeenten in meer of mindere mate zicht hebben op risicovolle functies binnen het veiligheidsdomein. Gemeenten B, C en D hebben geen risicovolle functies in beeld gebracht en hebben dus ook niet expliciet de eerdergenoemde kenmerken van risicovolle functies toegepast. Gemeente B hanteert geen lijst van risicovolle functies en is van mening dat houding, gedrag en het continu creëren van bewustzijn met betrekking tot integriteit belangrijker is dan een lijst bijhouden met risicovolle functies. Ook geeft zij aan dat een dergelijke lijst nooit volledig kan zijn en dat er variëteit in functies zit. Gemeente C heeft ook geen specifieke risicovolle functies geïdentificeerd en bij gemeente D wordt geen centrale regie gevoerd op de identificatie van risicovolle functies en is het veiligheidsdomein zelf verantwoordelijk voor de identificatie ervan. Gemeente D is wel van plan om op basis van de BIG kwetsbare functies te gaan benoemen.

De drie gemeenten die niet inzichtelijk hebben gemaakt welke functies risicovol zijn, hebben geen gebruik gemaakt van instrumenten waarmee risicovolle functies in beeld kunnen worden gebracht. Gemeente B gebruikt geen risicoanalyse, risico-inventarisatie, risicomatrices of risicoprofielen. Gemeente C en D hebben geen expliciete risicoanalyse uitgevoerd, geen risicoprofiel of risiconiveaus bepaald. Gemeente D geeft wel aan dat zij impliciet risiconiveaus onderscheidt en impliciet een risicobeoordeling uitvoert omdat er een functiespecifieke VOG wordt aangevraagd.

Gemeenten A en E hebben beiden wel risicovolle functies inzichtelijk gemaakt. Beide gemeenten hebben risicovolle functies in beeld gebracht door een risicoanalyse uit te voeren die is toegespitst op risico's in de uitvoering van gemeentelijke taken in het veiligheidsdomein. Gemeente A maakt hierbij niet expliciet een onderscheid tussen verschillende risiconiveaus. Uit de door gemeente E uitgevoerde risicoanalyse volgde dat bepaalde functies in het veiligheidsdomein volgens de gemeente qua vereisten overeenkwamen met die van een vertrouwensfunctie.

Met betrekking tot de risicovolle functies heeft alleen gemeente A risico's en risiconiveaus gedefinieerd. Bij gemeente A zijn afdelingshoofden betrokken geweest bij het in kaart brengen van kwetsbare processen en functies. Op basis van een aantal criteria: onder meer de omgang met vertrouwelijke informatie, beoordelen / adviseren / machtspositie, budget- en beslissingsbevoegdheid en contact met burgers en bedrijven. Bij de risicovolle functies zijn de risico's en kwetsbaarheden, risico-verhogende factoren en beheersmaatregelen in de lijst opgenomen. Daarnaast wordt in het zelf opgestelde 'sjabloon risicovolle functies' met enkele kleuren aangegeven of directe actie nodig is of niet.

---

[64] Het gaat hier zoals eerder beschreven om een uitvoeringspraktijk waarbij de politie ook gemeentelijke medewerkers screent; daarvoor is nu geen wettelijke bevoegdheid. De Tweede Kamer is hierover geïnformeerd waarbij is aangegeven dat deze tijdelijke oplossing blijft bestaan opdat kan worden bepaald hoe de screening van deze medewerkers geregeld dient te worden.

Door gemeente E zijn risicovolle functies inzichtelijk gemaakt aan de hand van de ‘Leidraad aanwijzenvertrouwensfuncties’ van de AIVD en de brochure ‘Screening van personeel’ van Justis. Gemeente E heeft geen onderscheid gemaakt tussen verschillende risico’s en risiconiveaus op basis van een door het college van burgemeester en wethouders vastgesteld beleidskader integriteit. In dit document zijn een aantal functieaspecten opgesteld die moeten worden afgewogen (bijvoorbeeld de beschikking hebben over vertrouwelijke/strategische informatie, het omgaan met geld) en daarbij is een afweging voorgeschreven waarbij ingegaan moet worden op de kans op integriteitschendingen en wat de impact daarvan is.

Uit de case studies blijkt dat gemeenten eveneens andere domeinen buiten het veiligheidsdomein kunnen aanduiden die risicovolle functies kennen. Het gaat om functies bij de domeinen Vastgoed, Sociaal, Fysiek, Vergunningverlening Toezicht en Handhaving (VTH), Financiën en ICT. Gemeenten A, B en C geven bijvoorbeeld aan dat de risico’s in het veiligheidsdomein samenhangen met risico’s in andere domeinen waar met vertrouwelijke of gevoelige informatie wordt omgegaan of waarbij er sprake is van kwetsbare processen als inkoop, het doen van betalingen, aanbestedingen en verlenen van vergunningen.

Uit de case studies blijkt verder dat alle vijf gemeenten ook andere maatregelen inzetten om de risico’s omtrent risicovolle functies te beperken voordat wordt ingezet op screening. Gemeente A geeft als enige aan haar maatregelen deels te hebben gekoppeld aan de uitgevoerde risicoanalyse. De onderzochte gemeenten maken gebruik van het laten afleggen van de ambtseed en hebben een vastgestelde gedragscode. Daarnaast wordt een diversiteit aan maatregelen ingezet door de gemeenten. Het gaat om organisatorische maatregelen (bijvoorbeeld het toepassen van het vierogenprincipe, periodieke functieroulatie), fysieke maatregelen (bijvoorbeeld toegangspasjes voor bepaalde afdelingen, clean desk policy, beveiligde laptops) en andere maatregelen (bijvoorbeeld bewustwordingssessies over weerbaarheid en integriteit). In de meerderheid van de gevallen betreft het algemene maatregelen die ook toepassing vinden binnen het veiligheidsdomein.

Met betrekking tot het effect van de inzet van deze maatregelen geeft gemeente A bijvoorbeeld aan dat zij het inzetten van risico beperkende maatregelen nuttig vindt, maar dat deze maatregelen onvoldoende de integriteit kunnen borgen. Gemeente B en D geven aan dat het integriteitsbesef/bewustzijn van medewerkers binnen het veiligheidsdomein, ook los van deze maatregelen, hoog is. Uit twee case studies blijkt verder dat regie op bevordering van de integriteit en structurele aandacht ervoor binnen het veiligheidsdomein meer geborgd kunnen worden.

4.3 Benutting van het bestaande screeningsinstrumentarium door gemeenten

De vijf gemeenten zetten diverse screeningsinstrumenten in die in hoofdstuk 2 van dit onderzoek zijn beschreven.

Bij alle onderzochte gemeenten wordt de VOG verplicht gesteld en bij drie van de vijf onderzochte gemeenten wordt een referentencheck uitgevoerd. De inzet van de verschillende screeningsmethodieken is bij vier gemeenten ter beoordeling van medewerkers binnen het veiligheidsdomein zelf, eventueel in overleg met en centrale aansturing of afstemming vanuit de afdeling personeelszaken.

Dit zou ruimte kunnen bieden voor maatwerk in het veiligheidsdomein, maar de inzet van screeningsmethodieken bij drie onderzochte gemeenten is niet structureel en expliciet gekoppeld aan bijvoorbeeld een voorafgaande risicoanalyse en/of indeling van functies in risicocategorieën in het veiligheidsdomein. Door onderzoekers wordt verder vastgesteld dat geen van de vijf onderzochte gemeenten het gehele palet aan instrumenten gebruikt. Gemeente C geeft bijvoorbeeld te kennen dat bij het aannemen van personeel maar beperkt aandacht geschonken wordt aan aspecten van integriteit tijdens de sollicitatieprocedure zelf.

Het raadplegen van openbare bronnen wordt door drie van de vijf gemeenten ingezet als instrument. Twee daarvan geven expliciet aan dat zij juridische vraagtekens hebben met betrekking tot het uitvoeren van openbaar bronnenonderzoek c.q. dat er geen bewuste afweging wordt gemaakt met de privacyaspecten en de derde gemeente heeft geen kaders gesteld aan het gebruik van openbare bronnen. Gelet op de juridische randvoorwaarden en verschillende beelden die in hoofdstuk 2 van dit rapport zijn beschreven met betrekking tot openbare bronnen zouden gemeenten geholpen zijn met een handreiking of leidraad waarin een handelingsperspectief wordt geboden.

Bij externen / ingehuurde medewerkers lijkt wel steeds sprake te zijn van alertheid en aandacht voor integriteitsaspecten. Er worden echter geen andere eisen gesteld dan aan die van kandidaten of gemeenteambtenaren die reeds in dienst zijn. Er zijn veelal duidelijke procesafspraken en ondertekening van een geheimhoudingsverklaring en/of het overleggen van een VOG is voor externen een vereiste.

Bij de toepassing van de screeningsinstrumenten hebben wij alleen bij gemeente A geconstateerd dat zij rekening houdt met de bepaalde risico’s en risiconiveaus. Bij de andere vier gemeenten zijn er zoals hiervoor aangegeven formeel geen risico’s en risiconiveaus bepaald, maar wordt bij de toepassing van de screeningsinstrumenten soms wel onderscheid gemaakt. Eerder is bijvoorbeeld weergegeven dat bij drie gemeenten een screening wordt uitgevoerd zoals bij de politie. Bij gemeente C moet als extra vereiste een geheimhoudingsverklaring worden ondertekend als medewerkers meedoen aan het project ondermijning. Gemeente B en C gaven aan dat voor alle medewerkers screening op dezelfde wijze wordt uitgevoerd.

4.4 De uitvoering van screening door gemeenten

De wijze waarop gemeenten de uitvoering van screening organiseren, levert een divers beeld op. Drie van de vijf gemeenten stemmen de screening af met de afdeling personeelszaken of zij worden door hen daarbij ondersteund. Bij de andere twee gemeenten is er sprake van dat (de betreffende afdeling in) het veiligheidsdomein de screening zelf uitvoert zonder centrale controle of centraal opgelegde regels en gelden er geen gemeentebrede regels of toezicht hierop. Zij bepalen dus zelf hoe de screening wordt uitgevoerd en welke screeningsinstrumenten worden toegepast. Gemeente E geeft als enige in de vacaturetekst aan dat onderzoek in openbare bronnen wordt gedaan.

Verder blijkt dat de case studie gemeenten de screening niet door een externe partij (bijvoorbeeld werving- en selectiebureau, recherchebureau) laat uitvoeren. Bij drie van de vijf gemeenten wordt bij een aantal gemeenteambtenaren in het veiligheidsdomein een screening uitgevoerd die gelijk is aan

die van politieambtenaren door de politie. Uit de case studies is niet duidelijk geworden wat de impact is van het zelf uitvoeren van de screening en het is niet mogelijk geweest om een vergelijking te maken met bijvoorbeeld een screening die door een extern bureau is uitgevoerd.

Bij de onderzochte gemeenten is door onderzoekers een divers beeld waargenomen met betrekking tot de inzet van screeningsinstrumenten om de integriteit te bewaken van externen. Bij externen / gedetacheerde medewerkers wordt een VOG vereist bij de onderzochte gemeenten. Bij gemeente E is het voor internen en externen zonder een VOG niet mogelijk een inlogaccount bij de gemeente aan te maken. Gemeente B maakt gebruik van bijvoorbeeld een externe partij die de inhuur regelt en deze externe partij regelt de VOG en doet de voorselectie, vraagt werkgeversgegevens op (bijvoorbeeld gegevens uit het Handelsregister) die in het inkoopsysteem van de gemeente worden ingevoerd. Andere gemeenten verplichten externen tot het ondertekenen van een geheimhoudingsverklaring en/of integriteitsverklaring.

4.5 Mogelijkheden voor gemeenten om de eigen verantwoordelijkheden waar te maken door het beschikbare instrumentarium van risicoanalyses en screening

Hierboven is aangegeven dat de vijf case studie gemeenten deels gebruik maken van het totale palet aan instrumenten. Nu deze instrumenten maar deels worden gebruikt, is er nog ruimte voor de gemeentelijke werkgever om de eigen verantwoordelijkheden waar te maken.

In hoofdstuk 1 is een schets van de context beschreven van gemeenten die opereren in het veiligheidsdomein. Gemeenten hebben een steeds grotere taak gekregen bij de aanpak van criminaliteit. Ook hebben zij te maken met nieuwe uitdagingen zoals ondermijning en radicalisering. Om deze uitdagingen het hoofd te kunnen bieden werken gemeenteambtenaren samen met partners in het brede veiligheidsdomein, bijvoorbeeld het RIEC en de politie. In deze samenwerking wordt het delen van informatie van groot belang geacht, maar deze informatiepositie brengt voor gemeenten een aantal uitdagingen met zich mee, zoals de bescherming van vertrouwelijke overheidsinformatie en persoonsgegevens, veiligheid en integriteit van gemeenteambtenaren in risicovolle functies en weerbaarheid van de gemeentelijke organisatie. Het verkennende onderzoek reikte niet zo ver dat duidelijk naar voren is gekomen in hoeverre de informatie die door de samenwerkingspartners van gemeenten wel of niet wordt gedeeld vereist is voor het uitvoeren van de gemeentelijke taken binnen het veiligheidsdomein. Eén gemeente heeft expliciet aangegeven bepaalde informatie van samenwerkingspartners niet te willen ontvangen en dat medewerkers niet aanwezig mogen zijn bij overleggen met ketenpartners omdat zij onvoldoende zijn gescreend. Een andere gemeente ontvangt gevoelige informatie van samenwerkingspartners zonder een zwaardere vorm van screening uit te voeren.

Uit de beschrijving van instrumenten waarover de (niet-gemeentelijke) instellingen, die in hoofdstuk drie zijn opgenomen, kunnen beschikken, komt verder naar voren dat deze organisaties dezelfde instrumenten inzetten als de case studie gemeenten (zoals een VOG, cv check, controle identiteit, geheimhoudingsverklaring). Als men vervolgens de inzet van het beschikbare instrumentarium vergelijkt van de gemeenten en de instellingen komt naar voren dat zowel gemeenten als de instellingen een VOG eisen bij de aanstelling en dat de instellingen ook (een deel van) de andere instrumenten inzetten die gemeenten tot hun beschikking hebben. Vanuit dit perspectief kan niet

gezegd worden dat gemeenten over onvoldoende mogelijkheden beschikken om risico's in te perken omdat de instellingen ook deze instrumenten (deels) inzetten. Onze bevinding is wel dat gemeenten een minder vergaand instrumentarium tot hun beschikking hebben dan de genoemde instellingen. Uit de vergelijking komt namelijk duidelijk naar voren dat de instellingen, behalve het UWV, in de betreffende wet- en regelgeving zoals het Bjsg en/of het Bpg worden genoemd als instellingen die bijvoorbeeld justitiële en/of politiegegevens mogen ontvangen. In art. 23 van het Bjsg wordt er bijvoorbeeld vanuit gegaan dat aan de functies bij deze instellingen bijzondere eisen worden gesteld aan integriteit of verantwoordelijkheid of dat de gegevens benodigd zijn voor een goede uitvoering van hun specifieke taak. Daarnaast kunnen de politie, inspectie SZW en belastingdienst ook een VGB opvragen van de betrokkene. De politie kan daarnaast ook een onderzoek naar de betrouwbaarheid en geschiktheid uitvoeren bij het aannemen van politieambtenaren en zelf onder mandaat een zogenaamd P-onderzoek uitvoeren. De belastingdienst kent nog een Insiderregeling Financiën om de schijn van financiële belangenverstrengeling en het risico van oneigenlijk gebruik van koersgevoelige informatie te voorkomen.
Mede vanuit de hierboven beschreven informatiepositie bezien - dus tot welke informatie is de beschikking en over welke informatie kan worden beschikt - is onze constatering dat een aantal gemeenten zeer veel gevoelige informatie heeft of toegang er toe krijgt en deze positie lijkt vergelijkbaar met die van de instellingen. Vanuit deze optiek hebben we begrip voor de roep van een aantal case studiegemeenten om verregaandere screeningsmogelijkheden, maar dat vergt volgens ons nader onderzoek omdat de huidige verkenning onvoldoende basis biedt om hierover onderbouwde uitspraken te kunnen doen. Daarbij komt nog dat organisaties dus niet zomaar in het Besluit politiegegevens kunnen worden opgenomen.[65]

Voorts heeft binnen dit verkennende onderzoek slechts één gemeente risico's en risiconiveaus inzichtelijk gemaakt waardoor het vergelijken ervan met de risico's van de instellingen niet tot een betrouwbare vergelijking kan leiden.

Als een gemeenteambtenaar vooraf is gescreend op basis van een VOG en daarna is aangenomen voor een functie in het veiligheidsdomein bij een gemeente, is onze bevinding uit de case studies dat er aandacht is voor integriteitsaspecten in bijvoorbeeld functioneringsgesprekken, gedragscodes en fysieke maatregelen. Er is ook een wijziging per 1 januari 2018 dat een VOG ook 'periodiek' kan worden ingezet bij een functiewijziging, overplaatsing of tewerkstelling, maar dat staat in contrast met een aantal instellingen die al mogelijkheden hebben om herhaaldelijk een screeningsinstrument in te zetten (bijvoorbeeld om de vijf jaren hernieuwd veiligheidsonderzoek of onderzoek naar de betrouwbaarheid en geschiktheid). Zij ontvangen daarbij justitiële gegevens op grond van het Bjsg

[65] Zie artikel 18 Wet politiegegevens: Bij of krachtens algemene maatregel van bestuur kunnen personen en instanties worden aangewezen aan wie of waaraan, met het oog op een zwaarwegend algemeen belang, politiegegevens worden of kunnen worden verstrekt ter uitvoering van de bij of krachtens die algemene maatregel van bestuur aan te geven taak.

en het Bpg, terwijl gemeenten bij een VOG geen inzage hebben in de geregistreerde justitiële gegevens.

4.6 Mogelijkheden om te komen tot een optimale beperking van de veiligheidsrisico's door middel van de inzet van risicoanalyses en screening

Uit de case studies blijkt dat gemeenten deels gebruik maken van de beschikbare mogelijkheden van screening en de inzet van bijvoorbeeld risicoanalyses. Onze bevinding is dat er nog ruimte is om deze mogelijkheden in te zetten in het veiligheidsdomein. Volgens onderzoekers zijn er ook nog mogelijkheden om alvorens tot screening over te gaan onder meer organisatorische en fysieke maatregelen in te zetten zoals eerder is beschreven.

Zoals in hoofdstuk 2 is beschreven is voor elke verwerking door de gemeente als verwerkingsverantwoordelijke een grondslag nodig. Dit betekent dat de gemeente als ontvanger van bijvoorbeeld strafrechtelijke / justitiële gegevens en politiegegevens ook een grondslag aannemelijk moet maken dat zij deze gegevens mag verwerken. Indien de gemeente geen beroep kan doen op een geschikte grondslag, mag zij deze gegevens ook niet verwerken. Belangrijk punt om hierbij te noemen, is dat de AP heeft aangegeven dat slechts in incidentele gevallen, indien niet kan worden volstaan met een VOG in de sollicitatie (en screenings-)procedure, strafrechtelijke gegevens kunnen worden verwerkt. De gemeente moet volgens de AP ook aangeven waarom een VOG niet volstaat en wat de aanleiding is om aanvullend strafrechtelijke gegevens te verwerken. Dit zijn volgens onderzoekers zware bewijslasten die door de AP aan gemeenten gesteld worden. Daarnaast geeft de toelichting op art. 23 van het Bjsg bijvoorbeeld aan dat het gaat om bijzondere, wettelijke eisen die worden gesteld aan de verantwoordelijkheid en integriteit van degene die de functie gaat invullen. De bevinding van onderzoekers is dat de eisen die gesteld worden aan het mogen ontvangen van justitiële gegevens en politiegegevens hoog zijn. In de case studies is, zoals hiervoor eerder beschreven, maar in beperkte zin naar boven gekomen (alleen bij gemeente A) welke risico's er zijn met betrekking tot risicovolle functies in het gemeentelijke veiligheidsdomein. Het vergelijken van de verhouding tussen de risico's van de functies die in het Bjsg en het Bpg zijn opgenomen met de risico's op basis van slechts één gemeente ('n=1') is volgens onderzoekers een te kleine steekproef om een onderbouwde conclusie te kunnen trekken.

Uit de case studies is wel naar voren gekomen dat bij een aantal specifieke functies in het veiligheidsdomein (bijvoorbeeld boa's, medewerkers RIEC, afdeling Handhaving en Toezicht) een screening wordt uitgevoerd zoals bij de politie. Ook hier geldt de beperking dat slechts één gemeente de risico's in kaart heeft gebracht.

In de 'pre-employment-fase' geldt de algemene grondslag van art. 125 Ambtenarenwet en art. 2:2 van het CARUWO en in de 'in-employment-fase' kunnen gemeenten op de grondslag van art. 125 van de Ambtenarenwet en hoofdstuk 15 van het CARUWO diverse instrumenten inzetten. Ook moet de bescherming van de persoonlijke levenssfeer van de betrokken kandidaat of ambtenaar afgewogen worden tegen subsidiariteit en proportionaliteit van het in te zetten instrumentarium. Een onderzoek naar bekwaamheid en geschiktheid' zoals bedoeld in art.2:2 CARUWO kan niet gezien worden als basis voor een verregaandere onderzoeksmethodiek waarbij gebruik gemaakt wordt van justitiële gegevens en politiegegevens; dit vergt aanpassing van in ieder geval de Aw, het

Bjsg en het Bpg. De inbreuk die op de persoonlijke levenssfeer van betrokkene wordt gemaakt, gaat zodanig ver dat een dergelijke screening mede gelet op art. 8 van het EVRM, artikel 8 van het Handvest van de grondrechten van de Europese Unie en art. 10 Grondwet een duidelijke grondslag in wetgeving vereist. Het CARUWO biedt gemeentelijke werkgevers per 1 januari 2018 wel ruimte om op lokaal niveau in de situaties waarin er sprake is van een functiewijziging, overplaatsing of tewerkstelling van een medewerker een recente VOG te verzoeken. Ook kunnen gemeenten, zoals is beschreven in hoofdstuk 2, op basis van het verplicht vast te stellen integriteitsbeleid aandacht besteden aan het bevorderen van integriteitsbewustzijn en integriteit in functioneringsgesprekken en werkoverleg aan de orde stellen.

Het zou volgens onderzoekers aannemelijk moeten zijn dat binnen het veiligheidsdomein de organisatorische inbedding van uitvoering van risicoanalyses en screening op een goede manier is geregeld, mede gelet op het feit dat de gemeenten de functies in het veiligheidsdomein zelf als risicovol aanduiden. Hierboven is reeds aangegeven dat maar twee van de vijf gemeenten een risicoanalyse hebben opgesteld met behulp van de daartoe beschikbare instrumenten en dat daarvan slechts één gemeente (gemeente A) risico's en risiconiveaus heeft opgesteld en hiernaar handelt. Uit de case studies is tevens gebleken dat gemeenten screenings en het instrumentarium om risicovolle functies in beeld te krijgen deels inzetten binnen het veiligheidsdomein, maar dat het nog niet ten volle wordt benut. Uit de case studies blijkt ook dat de meerderheid van de case studie gemeenten bij de wijze van uitvoering van screening samenwerken met de afdeling personeelszaken, maar dat de medewerkers in het veiligheidsdomein een behoorlijke mate van vrijheid hebben bij het zelf uitvoeren van de screening; er gelden geen centrale of gemeentebrede regels en de medewerkers bepalen zelf hoe zij de screening uitvoeren en welke screeningsinstrumenten worden ingezet.

Meer aandacht voor de organisatorische inbedding van de uitvoering van risicoanalyses en screening bij gemeenten biedt volgens onderzoekers een kans om het binnen het veiligheidsdomein goed te kunnen regelen. De wijze waarop gemeente A het heeft geregeld zou bijvoorbeeld een opmaat voor een handelingsperspectief kunnen bieden.

5. Conclusies

5.1 Inleiding

In opdracht van het Ministerie van Binnenlandse zaken heeft Berenschot een verkennend onderzoek gedaan naar de screening van gemeenteambtenaren. In dit hoofdstuk presenteren wij onze conclusies.

5.2 Conclusies

Op basis van het verkennende onderzoek komen wij tot de volgende conclusies:

- De gemeentelijke werkgever kan beschikken over de in paragraaf 2.3 opgesomde screeningsinstrumenten. De (rand)voorwaarden bij toepassing van de instrumenten worden met name bepaald door de Wbp (vanaf 25 mei 2018 de AVG), het EVRM, de Ambtenarenwet en het CARUWO.
- De onderzochte gemeenten hebben in meer of mindere mate zicht op risicovolle functies binnen het veiligheidsdomein. Kenmerkende criteria van risicovolle functies binnen het gemeentelijke veiligheidsdomein zijn met name het kunnen beschikken over (gevoelige / vertrouwelijke) informatie in combinatie met het bekleden van een bepaalde functie of uitvoeren van een specifieke taak.
- De meerderheid van case studie gemeenten hebben geen risicovolle functies in beeld gebracht. Zij hebben dus geen gebruik gemaakt van instrumenten waarmee risicovolle functies in beeld kunnen worden gebracht.
- Uit de case studies blijkt dat gemeenten eveneens andere domeinen (bijvoorbeeld Vastgoed, Sociaal, Fysiek, Vergunningverlening Toezicht en Handhaving, Financiën en ICT) en processen (bijvoorbeeld inkoop, het doen van betalingen, aanbestedingen en verlenen van vergunningen) buiten het veiligheidsdomein kunnen aanduiden die risicovolle functies kennen.
- Twee gemeenten hebben risicovolle functies inzichtelijk gemaakt en hierbij een risicoanalyse uitgevoerd die is toegespitst op risico's in de uitvoering van gemeentelijke taken in het veiligheidsdomein. Met betrekking tot de risicovolle functies heeft slecht één van deze gemeenten risico's en risiconiveaus gedefinieerd met behulp van de daartoe beschikbare instrumenten. Bij de overige gemeenten wordt bij de toepassing van de screeningsinstrumenten soms wel impliciet onderscheid gemaakt. Uit de case studies concluderen wij dat gemeenten deels gebruik maken van de inzet van bijvoorbeeld risicoanalyses, aanduiding van risico's en risiconiveaus. Er is nog ruimte om deze mogelijkheden in te zetten in het veiligheidsdomein.
- Uit de case studies blijkt dat de door de gemeente genoemde functies in paragraaf 4.2 als risicovolle functies worden gezien. Bij drie gemeenten wordt voor bepaalde functies in het

veiligheidsdomein een screening uitgevoerd zoals bij politieambtenaren en dit geeft aan dat deze functies als risicovol worden gezien.

- Uit het onderzoek is niet duidelijk geworden in hoeverre de informatie die door de samenwerkingspartners van gemeenten wel of niet wordt gedeeld, vereist is voor het uitvoeren van de gemeentelijke taken binnen het veiligheidsdomein. Een nader onderzoek zou hier meer inzicht in kunnen geven.
- De case studie gemeenten zetten diverse screeningsinstrumenten in die in hoofdstuk twee van dit onderzoek zijn beschreven. Bij alle onderzochte gemeenten wordt de VOG verplicht gesteld. Uit de case studies concluderen wij dat gemeenten de beschikbare screeningsinstrumenten maar deels inzetten en er is dus nog ruimte voor de gemeentelijke werkgever om de eigen verantwoordelijkheden waar te maken.
- Uit de vergelijking met de instellingen concluderen wij dat de gemeenten een minder vergaand instrumentarium tot hun beschikking hebben dan de instellingen. De meerderheid van de instellingen mogen justitiële en/of politiegegevens ontvangen op basis van het Bjsg en het Bpg.
- De inzet van de verschillende screeningsmethodieken is bij de meerderheid van de gemeenten ter beoordeling van medewerkers binnen het veiligheidsdomein zelf en is niet structureel en expliciet gekoppeld aan bijvoorbeeld een voorafgaande risicoanalyse en/of indeling van functies in risicocategorieën in het veiligheidsdomein.
- Het raadplegen van openbare bronnen wordt door de meerderheid van gemeenten ingezet als instrument. Gelet op de juridische randvoorwaarden zoals die in hoofdstuk 2 van dit rapport zijn beschreven, in het bijzonder met betrekking tot de‘online screening’, en de vragen van gemeenten hieromtrent, concluderen wij dat gemeenten geholpen kunnen worden met een handreiking of leidraad waarin een handelingsperspectief wordt geboden hoe met openbare bronnen kan worden omgegaan bij screening.
- Voor zover een gemeente al strafrechtelijke gegevens zou mogen verwerken of ontvangen, concluderen wij dat er een hoge bewijslast is voor gemeenten in het kader van de bescherming van persoonsgegevens. Aangegeven moet worden waarom een VOG niet volstaat en wat de aanleiding is om aanvullend strafrechtelijke gegevens te ontvangen.
- Uit de case studies blijkt dat alle gemeenten ook andere maatregelen inzetten om de risico’s omtrent risicovolle functies te beperken voordat wordt ingezet op screening. Het gaat bijvoorbeeld om organisatorische maatregelen en fysieke maatregelen. Gemeenten zetten tevens diverse integriteit bevorderende maatregelen in als een medewerker eenmaal in dienst is getreden bij de gemeente, bijvoorbeeld functioneringsgesprekken en het opstellen van gedragscodes.
- De wijze waarop gemeenten de uitvoering van screening organiseren levert een divers beeld op. De conclusie is dat bij de wijze van uitvoering van screening de meerderheid van de case studie gemeenten samenwerken met de afdeling personeelszaken, maar dat de

medewerkers in het veiligheidsdomein een behoorlijke mate van vrijheid hebben bij het zelf uitvoeren van de screening. Ook met betrekking tot de inzet van screeningsinstrumenten om de integriteit te bewaken van externen is een divers beeld waar te nemen.

- Uit de case studies blijkt dat de gemeenten de screening niet door een externe partij (bijvoorbeeld werving- en selectiebureau, recherchebureau) laat uitvoeren. Uit de case studies is niet duidelijk geworden wat de impact is van het zelf uitvoeren van de screening in vergelijking met een screening die door een extern bureau is uitgevoerd.
- Een onderzoek naar bekwaamheid en geschiktheid' zoals bedoeld in art.2:2 CARUWO kan niet gezien worden als basis voor een verregaandere onderzoeksmethodiek waarbij gebruik gemaakt wordt van justitiële gegevens en politiegegevens; dit vergt aanpassing van in ieder geval de Aw, het Bjsg en het Bpg.
- Op basis van de case studies concluderen wij dat in het algemeen niet aan te geven is wat voor een gemeente een goede organisatorische inbedding is van uitvoering van risicoanalyses en screening. De wijze waarop gemeente A de organisatorische inbedding heeft georganiseerd zou als voorbeeld kunnen dienen voor andere gemeenten, zij het dat maatwerk mogelijk moet blijven gelet op de context van de gemeente en ontwikkelingen in het veiligheidsdomein.
- Wij concluderen ten slotte dat de gemeentelijke werkgever integriteitsrisico's bij de uitvoering van gemeentelijke taken ten behoeve van het veiligheidsdomein optimaal kan beperken door:
    - gebruik te maken van meer screeningsinstrumenten dan die thans worden ingezet,
    - de inzet van het instrumentarium structureel te borgen in de gemeentelijke organisatie en daarbij als uitgangspunt te nemen dat risicovolle functies in het veiligheidsdomein expliciet inzichtelijk worden gemaakt,
    - de risico's en risiconiveaus van deze risicovolle functies te bepalen en dat deze specifiek worden gekoppeld aan de inzet van de beschikbare screeningsmethodiek(en),
    - meer gebruik te maken van organisatorische en/of fysieke maatregelen alvorens wordt overgegaan tot screening.

Berenschot

Bijlage 1: Documentenlijst

- Autoriteit Persoonsgegevens (2016). Onderzoeksrapport Hoffmann B.V.: Onderzoek naar de verwerking van persoonsgegevens bij pre-en-in-employment screening
- Bureau Regioburgemeesters 5 juni 2017. Wetsvoorstel tot wijziging van de Wet justitiële en strafvorderlijke gegevens
- Bureau Regioburgemeesters. Behoeftestelling regioburgemeesters ten aanzien van screening
- Gemeenteblad Amsterdam (2017). Instemmen met het initiatiefvoorstel “Geef jongeren een nieuwe kans” van de raadsleden Verheul, Boutkan en Blom en kennisnemen van de bestuurlijke reactie (2017, nr. 100/241)
- Justis, Ministerie van Veiligheid en Justitie (2017). Screening van personeel
- Justis. Ministerie van Veiligheid en Justitie (2016). Maatwerk bij de VOG-screening
- KING (2017). Factsheet Informatie BeveiligingsDienst
- KING (2016). Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten
- KING (2016). Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten
- KING (2013). Handleiding Screening Personeel. Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- Laaper, S. (2016). Inventarisatie samenwerkingsverbanden
- Laaper, S. (2016). Overzicht gemeentelijke taken en bevoegdheden/ groslijst
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties – Algemene inlichtingen- en Veiligheidsdienst (2014). Leidraad aanwijzing vertrouwensfuncties. Nadere uitwerking van de Wet veiligheidsonderzoeken
- Politie. Betrouwbaarheids- en geschiktheidsonderzoek
- Politie. Betrouwbaarheids- en geschiktheidsonderzoek sollicitant
- Politie (2014). Protocol Betrouwbaarheids- en geschiktheidsonderzoek
- Pro Facto (2017). Criminele beïnvloeding van het lokale openbaar bestuur
- PwC (2016). Evaluatie aanbevelingen commissie Gunning. Successen behaald in verbetering van veiligheid en kwaliteit in de kinderopvang na de Amsterdamse zedenzaak.
- Staatscourant - 17 januari 2012. Beleidsregel beoordelingsperiodes en onvoldoende gegevens veiligheidsonderzoeken
- Telegraaf (2017). Corruptie uit beeld

- Tweede Kamer der Staten-Generaal (2015-2016). 28 844 - Integriteitsbeleid openbaar bestuur en politie. Nr. 101
- Tweede Kamer der Staten-Generaal (2012-2013). 33 673 - Wijziging van de Wet veiligheidsonderzoeken in verband met het opnemen van een grondslag voor het doorberekenen van kosten verbonden aan het uitvoeren van veiligheidsonderzoeken alsmede enkele andere wijzigingen. Nr. 3
- Tweede Kamer der Staten-Generaal (2015-2016). 34300 VI - Vaststelling van de begrotingsstaten van het Ministerie van Veiligheid en Justitie (VI) voor het jaar 2016. Nr. 78
- Tweede Kamer der Staten-Generaal (1994-1995). 24023 - Regelen inzake het verrichten van veiligheidsonderzoeken (Wet veiligheidsonderzoeken). Nr. 3
- Verheul, A., Boutkan. D. en Blom, S. (2016). NRC Handelsblad: Reken jongeren niet af op één stommiteit
- VNG (2017). Handreiking voor gemeenten. Kernbeleid Veiligheid 2017
- VNG (2015). De rol van gemeenten in de aanpak van radicalisering
- Zouridis, S. & Van der Vorm, B. (2013). Omwille van geloofwaardigheid. Een verkennend onderzoek naar knelpunten en oplossingen bij integriteitsonderzoek in Nederland

Verslagen, nota's en formulieren

- Aanvraagformulier Verklaring Omtrent het Gedrag Natuurlijke Personen (VOG NP)
- Deel van conceptverslag AO strafrechtelijke onderwerpen
- Kort verslag hoofdenoverleg OOV – VNG 19 juni 2017
- Nota VenJ en BZK (2016). Lopende trajecten binnen VenJ en BZK aangaande de screening/integriteit van (gemeente)ambtenaren in het veiligheidsdomein
- Nota Landelijk Overleg Veiligheid en Politie (2016). Stand van zaken werkgroep screening
- Nota Landelijk Overleg Veiligheid en Politie (2017). Stand van zaken screening samenwerkingspartners door politie
- Nota Landelijk Overleg Veiligheid en Politie (2017). Screening van samenwerkingspartners door politie. Bijlage 1: Notitie met stand van zaken van de werkgroep

Wet- en regelgeving en wetsvoorstellen

- Beleidsregels VOG-NP-RP 2013
- Besluit justitiële en strafvorderlijke gegevens.
- Regeling betrouwbaarheids- en geschiktheidsonderzoek politie

- 7 maart 2017: Wetsvoorstel tot wijziging van de Wet justitiële en strafvorderlijke gegevens in verband met het mogelijk maken van het in bepaalde gevallen weigeren van afgifte van een verklaring omtrent het gedrag op basis van politiegegevens
- Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag BES
- Wet politiegegevens
- Wet veiligheidsonderzoeken
- Wet op de inlichtingen- en veiligheidsdiensten 2002
- Wet justitiële en strafvorderlijke gegevens

Berenschot

Bijlage 2: Vragenlijst instellingen

Vragenlijst instellingen screening*

1. Heeft u beleid ten aanzien van de screening van uw medewerkers? (Gaarne uw beleidsstuk meesturen indien aanwezig)
2. Welke medewerkers / functionarissen worden binnen uw organisatie gescreend en wie is opdrachtgever van de screening?
3. Van welke screeningsmethodiek(en)* maakt u gebruik voor welke medewerkers / functionarissen? En welke informatie wordt hierbij gebruikt?
4. Wat is de reden om een screening uit te (laten) voeren?
5. Op welke juridische grondslag baseert u de screening van deze medewerkers / functionarissen?
6. Vindt screening plaats op basis van een risico-inventarisatie en/of wordt er onderscheid gemaakt naar functies? (Zo ja, graag (procedure van) de risico-inventarisatie meesturen)
7. Wordt bij deze risico-inventarisatie gebruik gemaakt van risicoprofielen? (Zo ja, graag de risicoprofielen meesturen)
8. Wijkt de procedure van screening in het geval van gedetacheerde / ingehuurde medewerkers af van de reguliere procedure die u hanteert? Zo ja, op welke wijze?
9. Door wie / welke instantie worden de (verschillende) screenings uitgevoerd?
10. Hoe wordt in geval van screening de privacy van de gescreende medewerker geborgd?

***Screening(smethodieken)**

Screening is het door of in opdracht van de werkgever vergaren van informatie over een sollicitant of werknemer om zo een inschatting te maken van zijn of haar integriteit. Methoden van screening zijn onder andere:

- Aanvragen Verklaring Omtrent Gedrag (VOG)
- Betrouwbaarheids- en geschiktheidsonderzoek (BGO*)*
- Veiligheidsonderzoek AIVD
- Omgevingsonderzoek
- Interne integriteitstoets (o.a. gesprek, checken identiteit, etc.)
- Openbare bronnenonderzoek (Handelsregister, google-search, social media, LexisNexis, etc.)
- Opvragen informatie (bijvoorbeeld BKR-registratie)
- Navraag bij referenten

Berenschot

Bijlage 3: Vragenlijst gemeenten

Vragenlijst screening gemeenten binnen OOV-domein

Documentatie

Graag ontvangen wij van u, indien aanwezig, de volgende documentatie:

- Beleid integriteit en screening
- Beleid integriteit en screening bij werving en selectie
- Beschrijving risicoanalyse (stappenplan / protocol)
- Risicoprofielen

Enkele vragen vooraf

Graag stellen wij u ter voorbereiding op het aanstaande interview een aantal vragen. Mocht u hierover aanvullende documentatie hebben dan ontvangen wij die graag.

- Uit welke functies bestaat bij u het veiligheidsdomein?
  - Zijn de personen die deze functies bekleden actief in samenwerkingsverbanden?
  - Met welke vertrouwelijke/risicovolle informatie krijgen de personen die deze functies bekleden te maken?
- Van welk instrumentarium (risicoanalyses, risicoprofielen, anders) wordt gebruik gemaakt om risicovolle functies binnen het veiligheidsdomein in beeld te brengen?
  - Door wie wordt dit instrumentarium binnen de gemeente gehanteerd?
- Worden screeningsmethodieken ingezet binnen het veiligheidsdomein?
  - Welke screeningsmethodieken*?
  - Door wie wordt deze screening uitgevoerd? Intern of extern?

***Screeningsmethodieken**

Screening is het door of in opdracht van de werkgever vergaren van informatie over een sollicitant of werknemer om zo een inschatting te maken van zijn of haar integriteit. Methoden van screening zijn onder andere:

- Aanvragen Verklaring Omtrent Gedrag (VOG)
- Betrouwbaarheids- en geschiktheidsonderzoek (BGO*)*
- Veiligheidsonderzoek AIVD
- Omgevingsonderzoek
- Interne integriteitstoets (o.a. gesprek, checken identiteit, etc.)
- Openbare bronnenonderzoek (Handelsregister, google-search, social media, LexisNexis, etc.)
- Opvragen informatie (bijvoorbeeld BKR-registratie)
- Navraag bij referenten

Interviewleidraad

Tijdens het interview zelf gaan we dieper in op de door u verstrekte informatie. Hierin komen onder andere de volgende vragen aan bod (let op: deze vragen hoeft u nu nog niet te beantwoorden!):

Risicoanalyse

- Zijn binnen de gemeentelijke organisatie functies (binnen het veiligheidsdomein) aangemerkt als risicovol?
  - Om welke functies gaat het? (binnen en buiten het veiligheidsdomein)
  - Door wie worden deze functies als risicovol aangemerkt?
  - Hoe wordt dit vastgelegd?
- Wordt binnen de gemeente onderscheid gemaakt tussen verschillende risico's en risiconiveaus?
  - Zo ja, welke niveaus worden gehanteerd?
- Is de risicoanalyse van algemene aard of specifiek toegespitst op het veiligheidsdomein?
- Wat is de reden voor de inzet van risicoanalyses?
- Heeft u voldoende zicht op de risico's die de functies binnen het veiligheidsdomein met zich meebrengen?
- Welke maatregelen worden ingezet om gesignaleerde risico's tegen te gaan (beheersmaatregelen)?

Inzet van screeningsmethodieken

- Onder welke voorwaarden wordt tot inzet van (bepaalde) screeningsmethodieken van medewerkers overgegaan?

- Wordt bij de inzet van screeningsmethodieken onderscheid gemaakt tussen medewerkers binnen het veiligheidsdomein en andere medewerkers?
- Is het al dan niet inzetten van screening van medewerkers binnen het veiligheidsdomein gebaseerd op de uitkomsten van een risicoanalyse?
- Hoe wordt in geval van screening de privacy van de gescreende medewerker geborgd?
- Wijkt de procedure van screening in het geval van gedetacheerde / ingehuurde medewerkers binnen het veiligheidsdomein af van de reguliere procedure? Zo ja, op welke wijze?
- Bieden de mogelijkheden tot screening u voldoende ruimte om integriteitsrisico's binnen het veiligheidsdomein door middel van screening in te perken?
- Heeft u behoefte aan aanvullende mogelijkheden op het gebied van screening?

Berenschot

Bijlage 4: Opdrachtgever en klankbordgroep

Naam	Organisatie	Rol
Terry Lamboo	Ministerie van BZK	Opdrachtgever
Ruthy Reinders	Ministerie van BZK	Opdrachtgever
Hella van de Velde	Ministerie van BZK	Opdrachtgever
Marcel Marra	Vereniging Nederlandse Gemeenten	Klankbordgroep
Ilona Kalksma	Bureau Regioburgemeesters	Klankbordgroep
Niels Romijn	Ministerie van J&V	Klankbordgroep
Niels Aangeenbrug	Ministerie van J&V	Klankbordgroep
Arjan Guijt	Unie van Waterschappen	Klankbordgroep
Rianne Becht	Interprovinciaal Overleg	Klankbordgroep
Eugene van de Poel	Vereniging Nederlandse Gemeenten	Klankbordgroep
Johan Hoffman	Ministerie van Financiën	Klankbordgroep
Maril Gelauff	Ministerie van J&V	Klankbordgroep