

Data Protection Impact Assessment (DPIA) over 'Ondermijning'

Gemeente Leeuwarden/ Dienst Veiligheidsdomein/ Sector Juridische- en Veiligheidszaken

Datum: maart 2019

Versie: 1

Auteurs: Claire de Jong (Beleidsadviseur Openbare Orde en Veiligheid) Anna Posthuma
(Juridisch beleidsmedewerker)

Beschrijving kenmerken gegevensverwerkingen

1. Omschrijving van de verwerking

Er wordt van gemeenten veel verwacht in de aanpak van georganiseerde ondermijnende criminaliteit onder meer binnen het kader van de RIEC-samenwerking alsmede in het kader van de eigen taakuitvoering (niet-faciliteren van criminaliteit). Het gaat bij deze aanpak om personen / netwerken die binnen de gemeente Leeuwarden actief zijn in illegale en of onrechtmatige activiteiten waarbij de overheid de mogelijkheid heeft om de rechtmatige situatie te herstellen / dan wel onrust weg te nemen en/of criminaliteit waarbij de overheid (onbewust) mogelijk faciliteert. Een goede informatiepositie van de gemeente in de voorfase draagt bij in de aanpak van ondermijning. Om die reden worden signalen van ondermijning geregistreerd. Signalen kunnen vervolgens intern worden gedeeld in een signaaloverleg en extern worden gedeeld met de politie in het signaaloverleg. Indien daartoe aanleiding is worden signalen opgeschaald naar het RIEC die de persoonsgegevens verder verwerkt in het kader van de aanpak van ondermijning. In dat geval valt de gegevensverwerking onder het RIEC convenant. Onderhavige DPIA heeft op deze fase uitdrukkelijk geen betrekking. De verwerking vindt alsdan plaats onder RIEC convenant en het tussen deelnemende partijen gesloten privacyprotocol.

2. Persoonsgegevens

De volgende categorieën van persoonsgegevens worden verwerkt in het kader van de verwerking als hierboven omschreven:

Naast 'gewone' persoonsgegevens worden er ook bijzondere persoonsgegevens verwerkt.

Gewone persoonsgegevens

1. Persoonsgegevens zoals naam, adres, beroep, e-mail, telefoonnummer, etc.
2. informatie uit de Kamer van Koophandel
3. Informatie uit het Kadaster
4. Informatie uit Bestemmingsplannen
5. Informatie over erfpacht
6. Informatie afkomstig van het internet.

Afhankelijk van de melding van het signaal en/of relevante casusinformatie kunnen ook de volgende categorieën van persoonsgegevens worden verwerkt:

7. Informatie uit de basisregistratie Adressen en Gebouwen
8. Informatie uit de basisregistratie personen
9. Informatie uit VIS over vergunningen horeca, intrekkingsbesluiten
10. Informatie uit systemen van W&I over uitkeringen, subsidies, andersoortige beschikkingen
11. informatie uit systemen van over uitkeringen, subsidies, andersoortige beschikkingen (gesloten bron)
12. Informatie uit Melddesk
13. informatie uit systemen over subsidies of andersoortige beschikkingen (gesloten bron)
14. informatie uit systemen over andersoortige beschikkingen (bv parkeervergunning, bestuurlijke boetes Drank- en Horecawet) (gesloten bron)
15. gegevens over de financiële of economische situatie van betrokkene;
16. gegevens over overtredingen van wettelijke voorschriften, bestuurlijke maatregelen of sancties;

Bijzondere persoonsgegevens die kunnen worden verwerkt zijn:

17. Ras of etnische afkomst

Daarnaast kunnen in het signaaloverleg strafrechtelijke gegevens – afkomstig uit de politiebronnen – worden verwerkt. Dit kunnen strafrechtelijke veroordelingen betreffende strafbare feiten of daarmee verband houdende veiligheidsmaatregelen zijn. Voorbeelden zijn bestuurlijke rapportages, processen verbaal, strafblad, antecedenten, etc.

3. Gegevensverwerking

De volgende verwerkingen van gegevens komen voor:

- Verzamelen
- Vastleggen
- Archiveren
- Ordenen
- Structureren
- Opslaan
- Opvragen
- Raadplegen
- Gebruiken
- Verstrekken door middel van doorzending
- Verspreiding
- Combineren
- Afschermen
- Vernietigen

4. Verwerkingsdoeleinden

Binnen het grondgebied van de gemeente Leeuwarden wordt beoogd om door samenwerking en gegevensdeling:

- ondermijnende activiteiten te signaleren en te analyseren;
- voorkomen dat de overheid ondermijnende activiteiten (onbewust) faciliteert;
- vroegtijdig kunnen signaleren en interveniëren middels een bestuurlijke aanpak of opschaling naar de lokale driehoek c.q. RIEC Noord Nederland
- voorkomen van onrechtmatigheden en maatschappelijke bedreigingen veroorzaakt door criminele activiteiten.

5. Betrokken Partijen

Verantwoordelijke

De Burgemeester van de Gemeente Leeuwarden is verwerkingsverantwoordelijke in de zin van de AVG.

Verwerker

De gemeente Leeuwarden verwerkt de verzamelde gegevens fasegewijs overeenkomstig het 'privacyprotocol ondermijning'. Indien professionals of burgers binnen de gemeente Leeuwarden signalen melden die kunnen duiden op verschijningsvormen van ondermijnende criminaliteit, dan wordt dit signaal gemeld bij de gemeentelijke coördinator ondermijning. Daartoe wordt gebruik gemaakt van een vastgesteld formulier. Indien de coördinator ondermijning oordeelt dat er mogelijk sprake is van een ondermijnende activiteit dan volgt een signaalafstemming onder regie van de coördinator ondermijning. In het signaaloverleg zijn afgevaardigden van de desbetreffende gemeentelijke onderdelen vertegenwoordigd alsook de politie. Het signaal wordt daarin gedeeld en indien nodig aangevuld met relevante informatie uit gemeentelijke bronnen en bronnen van de politie. Indien de coördinator ondermijning vaststelt

dat er sprake is van een ondermijnende activiteit wordt in een casusoverleg een plan van aanpak opgesteld waarbij de casus wordt gemonitord op voortgang en wordt afgesloten. Indien de coördinator vaststelt dat er geen sprake is van een ondermijnende activiteit, maar wel van andere onregelmatigheden, dan wordt het signaal doorgestuurd naar de betreffende vakafdeling die de casus onder eigen regie verder oppakt. Als vast komt te staan dat er sprake is van georganiseerde criminaliteit waarop het RIEC convenant van toepassing is, dan wordt het signaal via de lokale driehoek doorgeleid naar het RIEC.

Overige partijen

De politie is in het signaaloverleg betrokken indien een signaal duidt op ondermijnende activiteiten. De politie vult het signaal indien noodzakelijk aan met (strafrechtelijke) gegevens afkomstig uit de bronnen van de politie.

6. Belangen bij gegevensverwerking

- ondermijnende activiteiten signaleren en analyseren;
- voorkomen dat de overheid ondermijnende activiteiten (onbewust) faciliteert;
- vroegtijdig kunnen signaleren en interveniëren middels bestuurlijke aanpak;
- voorkomen van onrechtmatigheden en maatschappelijke bedreigingen veroorzaakt door criminele activiteiten.

7. Verwerkingslocaties

De voorgenomen verwerkingen vinden plaats binnen Nederland en in ieder geval binnen de EU. Dit zorgt voor een zekerheid met betrekking tot het beschermingsniveau op het gebied van privacy.

8. Technieken en methoden van de gegevensverwerking

Signalen met betrekking tot ondermijning worden gemeld via een vastgesteld formulier bij de coördinator ondermijning. Indien het signaal wordt gedeeld ten behoeve van het signaaloverleg wordt enkel gebruik gemaakt van een sharepointomgeving zodat de deelnemers aan het signaaloverleg de informatie op een streng beveiligd platform kunnen delen met elkaar. Daarbij worden niet meer persoonsgegevens met elkaar gedeeld dan noodzakelijk voor het doel, namelijk de aanpak van ondermijning. Dit wordt gewaarborgd doordat gebruik wordt gemaakt van een vastgesteld formulier zodat niet onbedoeld meer informatie wordt verstrekt / meer persoonsgegevens worden verstrekt dan noodzakelijk. Omdat de eerste signaalweging door de coördinator ondermijning wordt gedaan, is de verstrekking van de persoonsgegevens beperkt. De coördinator ondermijning beoordeelt of het noodzakelijk is de persoonsgegevens verder te delen met de deelnemers van het signaaloverleg. De coördinator ondermijning bepaalt de samenstelling van de deelnemers van het signaaloverleg. Daarmee blijft de groep van ontvangers van de persoonsgegevens en geautoriseerde gebruikers, beperkt.

9. Grondslag

De grondslag voor de verwerking is dat de gegevensverwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Op basis van de AVG (overweging 45) blijkt dat er wetgeving moet zijn die als basis fungeert voor de gegevensverwerking die noodzakelijk is voor de vervulling van een taak in het kader van de uitoefening van het openbaar gezag. Met andere woorden: er dient voldoende duidelijke wetgeving te zijn. Voor de aanpak van ondermijning betekent dit dat het Nederlandse recht daarvoor een afdoende wettelijke bepaling dient te bevatten waaruit blijkt dat de burgemeester een taak heeft bij de aanpak van ondermijning. Die taakbepalingen zijn opgenomen in verschillende materiewetten. Meer specifiek (maar niet uitsluitend) kunnen genoemd worden de bevoegdheden uit de Gemeentewet:

-Aritkel 151 d (Wet aanpak woonoverlast)

- Artikel 170 lid 3 (bestuurlijke integriteit)
- Artikel 172 (handhaving openbare orde)
- Artikel 172a (gebiedsverboden, groepsverboden, meldplicht bij verstoren openbare orde)
- Artikel 172b (gebiedsverboden 12 minners)
- Artikel 174a (het sluiten van een woning wegens verstoren openbare orde)
- Artikel 174b (aanwijzen veiligheidsrisicogebied)
- Artikel 175 (noodbevel)
- Artikel 176 (noodverordening)
- Artikel 176a (bestuurlijke ophouding)

Daarnaast heeft de burgemeester meer specifieke bevoegdheden op grond van (ondermeer) de volgende wetten:

- Artikel 13b Opiumwet (sluiten woning wegens aantreffen middelen op Lijst I /II Opiumwet)
- Wet tijdelijk huisverbod (opleggen van een huisverbod bij (dreiging van) huiselijk geweld)
- Wet Bibob (integriteitsbeoordeling bij vergunningaanvraag of aangaan overeenkomsten)

10. Bewaartermijnen

Gegevens dienen niet langer bewaard te worden dan noodzakelijk is voor het doel. In het privacyprotocol ondermijning zijn de bewaartermijnen nader gespecificeerd. Een signaal wordt niet langer dan een jaar bewaard. Indien een signaal leidt tot een plan van aanpak, wordt het signaal maximaal 5 jaar bewaard in een niet-actieve omgeving.

11. Informatiebeveiliging

Gemeente: Informatiebeveiliging bij Gemeente vindt plaats volgens Baseline Informatiebeveiliging Nederlandse Gemeenten. Deze is gebaseerd op het ISO 27001 en ISO27002 maatregelenkader.

- Verwerker: Informatiebeveiliging bij verwerker vindt plaats volgens algemeen erkende normen, namelijk de ISO 27001.

12. Incidenten

Van incidenten dient zo spoedig mogelijk (uiterlijk binnen 24 uur) een melding te worden gemaakt via privacy@leeuwarden.nl of telefoonnummer 14058. Er wordt gehandeld conform het protocol datalekken dat is vastgesteld en heeft te gelden binnen de gemeentelijke organisatie.

Beoordeling rechtmatigheid gegevensverwerking

13. Bijzondere persoonsgegevens

Bijzondere persoonsgegevens die kunnen worden verwerkt zijn ras of etnische afkomst van betrokkene. Dit speelt met name een rol als het gaat om de verwerking van persoonsgegevens bij signalen die duiden op mensenhandel.

Daarnaast kunnen in het signaaloverleg strafrechtelijke gegevens – afkomstig uit de politiebronnen – worden verwerkt. Dit kunnen strafrechtelijke veroordelingen betreffende strafbare feiten of daarmee verband houdende veiligheidsmaatregelen zijn. Voorbeelden zijn bestuurlijke rapportages, processen verbaal, strafblad, etc. Deze gegevens worden alleen verwerkt indien dit noodzakelijk is om te kunnen beoordelen of betrokkene zich bezig houdt met ondermijnende activiteiten.

Bijzondere persoonsgegevens en strafrechtelijke gegevens worden alleen verwerkt indien dat om redenen van zwaarwegende belangen noodzakelijk wordt geacht. Per casus wordt door de coördinator ondermijning afgewogen of het noodzakelijk is om het signaal aan te vullen met bijzondere dan wel strafrechtelijke gegevens. Indien verstrekking van informatie door de politie op grond van de Wpg noodzakelijk is dan wordt de casus in ieder geval aangevuld met die gegevens van de politie. Ook bij ondermijnende activiteiten met een sterke strafrechtelijke component is ten behoeve van het plan van aanpak aanvulling met strafrechtelijke gegevens noodzakelijk om de ondermijnende activiteiten effectief te kunnen bestrijden (zwaarwegend belang). Dit kan aan de orde zijn bij de aanpak van OMG's, drugshandel en hennepcultuur, mensenhandel, fraude en witwassen.

14. Doelbinding

Ten behoeve van de aanpak van ondermijning worden persoonsgegevens enkel voor dit doel verwerkt. Dit betekent het samenbrengen van signalen met betrekking tot ondermijning, aangevuld met informatie uit openbare bronnen, gemeentelijke bronnen en eventueel strafrechtelijke gegevens in het signaaloverleg c.q. plan van aanpak. Verdere verwerking van de persoonsgegevens is niet toegestaan, behoudens toestemming van betrokkene of indien dit gebaseerd is op een specifiek wettelijk voorschrift dat een noodzakelijke en evenredige maatregel is in een democratische samenleving ter waarborging van en belagrijke doelstelling van algemeen belang, bijvoorbeeld de nationale veiligheid, de openbare veiligheid, etc. Daarnaast wordt verdere verwerking ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden als verenigbaar geacht met de oorspronkelijke doeleinden.

15. Noodzaak en evenredigheid

De inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens staan in evenredige verhouding tot de verwerkingsdoeleinden. De verwerkingsdoeleinden kunnen niet in redelijkheid op een andere, voor de betrokkene minder nadelige wijze, worden verwezenlijkt. De voorgenoemde gegevensverwerking is daarmee noodzakelijk voor het verwezenlijken het doel, te weten de aanpak van ondermijning.

16. Rechten van betrokkenen

De rechten van betrokkenen worden niet beperkt. De betrokkene heeft de volgende rechten:

- Recht op inzage (Art. 15 AVG)
- Recht op rectificatie (Art. 16 AVG)
- Recht op gegevenswissing (Art. 17 AVG)
- Recht op beperking van de verwerking (Art. 18 AVG)
- Recht op overdraagbaarheid van de gegevens (Art. 19 AVG)
- Recht van bezwaar (Art. 21 AVG)

Deze rechten kunnen door betrokkene worden uitgeoefend door middel van een verzoek aan de verantwoordelijke; de burgemeester van de Gemeente Leeuwarden. De rechten die betrokkene heeft worden getoetst aan de weigeringsgronden zoals opgenomen in de AVG en UAVG.

Risico's

17. Risico's verwerkingsverantwoordelijke

Risico's van de gegevensverwerking zijn de volgende:

1. Er is (nog) geen concrete wettelijke grondslag die de aanpak van ondermijning regelt. De gegevensverwerking is derhalve gebaseerd op de algemeen omschreven taken uit de gemeentewet die met name zorgplichten van de burgemeester bevatten. Daarnaast zijn er een aantal specifieke taken in verband met openbare orde en veiligheid zoals nader omschreven onder punt 9. Op dit moment wordt gewerkt aan 'ondermijningswetgeving' die de aanpak moet vestreken, maar ook (intra- en extra gemeentelijke) gegevensuitwisseling in het kader van ondermijning beter mogelijk te maken.¹
2. Het interpreteren van deze samenwerking als noodzakelijk ter uitvoering van een publieke taak is ruim geïnterpreteerd, doch wel algemeen aanvaard (dit blijkt bijvoorbeeld uit de sleutelpositie die gemeenten geacht worden in te nemen in de RIEC samenwerkingsverbanden). Zie ook het standpunt van de Minister in deze.^{2 3}
3. Mogelijk worden er soms meer gegevens verwerkt dan noodzakelijk. De coordinator ondermijning beoordeelt in dat geval of er bovenmatige gegevens die niet noodzakelijk zijn moeten worden verwijderd.
4. Het is meestal niet mogelijk om betrokkene te informeren over de gegevensverwerking in verband met de weigeringsgronden zoals die daaromtrent zijn geformuleerd in de UAVG.
5. In geval van een datalek of beveiligingsincident is er een groot risico voor de verwerkingsverantwoordelijke gezien het lekken van gegevens voor wat betreft een mogelijk lopend opsporingsonderzoek door de politie / handavingsonderzoek door de gemeente.

18. Risico's voor betrokkene

6. Het is een risico voor betrokkene dat er een onjuiste inschatting wordt gemaakt voor wat betreft de afweging dat er sprake is van ondermijnende activiteiten door betrokkene.

¹ TK 2018-2019, 29911, nr 212. Brief van de minister aan de Tweede Kamer waarin wordt geïnformeerd over de voortgang en stand van zaken met betrekking tot de ondermijningswetgeving.

² TK 2018-2019, 29911, nr 212. Brief van de minister aan de Tweede Kamer waarin wordt geïnformeerd over de voortgang en stand van zaken met betrekking tot de ondermijningswetgeving.

³ TK2017-2018, 29 911 nr. 207 Brief van het kabinet aan de Tweede Kamer van 11 juli 2018 over hoe het kabinet de aanpak van ondermijnende criminaliteit de komende jaren wil versterken.

Gedacht kan worden aan stigmatisering, uitsluiting, financiële verliezen, reputatieschade of ander maatschappelijk of economisch nadeel voor betrokkene.

7. In geval van een beveiligingsincident of datalek, kan betrokkene in zijn persoonlijke levenssfeer worden aangetast.
8. Indien bewaartermijnen niet goed worden nageleefd kan een signaal de betrokkene te lang in verband brengen met ondermijnende activiteiten. Een en ander terwijl een signaal mogelijk niet heeft geleid tot een plan van aanpak daar de afweging heeft geleid tot de conclusie dat er geen sprake was van ondermijning. Dit kan leiden tot stigmatisering of uitsluiting van betrokkene.

18. Maatregelen

Bovenstaande risico's zijn geminimaliseerd doordat er duidelijke (werk)afspraken zijn gemaakt in het 'privacyprotocol ondermijning'. Hierin worden de privacy en de rechten en vrijheden van betrokkene zo goed als mogelijk gewaarborgd. Verder worden risico's geminimaliseerd doordat slechts een select aantal personen toegang heeft tot de gegevens die in het kader van de aanpak van ondermijning worden verwerkt. Die toegang wordt verder geoptimaliseerd door het delen van de informatie in een beveiligde sharepoint omgeving waarin de informatie zal worden gedeeld. Middels de fasegewijze verwerking van persoonsgegevens, zoals omschreven in het 'privacyprotocol ondermijning', worden bovendien in iedere fase niet meer gegevens verwerkt dan noodzakelijk, worden de gegevens niet met meer personen gedeeld dan noodzakelijk en worden de gegevens niet langer bewaard dan noodzakelijk. Daarmee zijn de privacyrechten voor betrokkene zoveel als mogelijk gewaarborgd en zijn de risico's aanvaardbaar. Meer specifiek worden tegen de benoemde risico's de volgende maatregelen genomen / waarborgen gesteld:

Ad. 1. Middels het privacyprotocol en deze DPIA is een duiding gegeven aan de grondslag voor de gegevensverwerking en de wetgeving die als basis fungeert voor de gegevensverwerking. De regioburgemeesters en VNG pleiten voor uitbreiding van wetgeving die een effectievere aanpak van ondermijning (door ondermeer gegevensuitwisseling) mogelijk moet maken. Dit kan op termijn leiden tot een meer specifieke wettelijke grondslag en betere duiding van die wettelijke grondslag. Tot op dat moment moet gewaarborgd worden dat de gegevensverwerking gebaseerd wordt op een van de materiewetten zoals benoemd onder punt 9.

Ad. 2. Uit diverse Kamerstukken⁴ blijkt dat de aanpak van ondermijning niet meer alleen een taak is van justitie en politie. De aanpak van georganiseerde criminaliteit is dan ook onderdeel van het lokale veiligheidsbeleid van de gemeente.

Ad. 3. Om te voorkomen dat meer gegevens worden verwerkt dan noodzakelijk, is een formulier vastgesteld waarop signalen met betrekking tot ondermijning kunnen worden vermeld. Middels invulvelden wordt bewerkstelligd dat enkel ter zake doende informatie wordt verwerkt. Het signaalformulier wordt in eerste instantie alleen ter beschikking gesteld aan de coördinator ondermijning die een eerste weging maakt. Indien de casus zich leent voor het signaaloverleg wordt een tweede weging gemaakt door de deelnemers van het signaaloverleg. Dit kan al dan niet leiden tot een plan van aanpak. Zo wordt zoveel mogelijk voorkomen dat er bovenmatig persoonsgegevens worden verwerkt

Ad. 4. De gegevensverwerking zal veelal vallen onder de uitzonderingsgronden zoals benoemd in de UAVG. Daardoor kan betrokkene (meestal) niet worden geïnformeerd over de

⁴ TK 2018-2019, 29911, nr 212. Brief van de minister aan de Tweede Kamer waarin wordt geïnformeerd over de voortgang en stand van zaken met betrekking tot de ondermijningswetgeving;

TK2017-2018, 29 911 nr. 207 Brief van het kabinet aan de Tweede Kamer van 11 juli 2018 over hoe het kabinet de aanpak van ondermijnende criminaliteit de komende jaren wil versterken.

gegevensverwerking. De coördinator ondermijning en deelnemers aan het signaaloverleg dienen per betrokkene daarin specifiek een afweging te maken. Indien een betrokkene niet kan worden geïnformeerd in verband met de uitzonderingsgronden uit de UAVG verdient het aanbeveling dit vast te leggen / te registreren. Een en ander is verder nader uitgewerkt in het Privacyprotocol.

Ad. 5. Door te werken in een beveiligde omgeving met beperkte autorisaties vindt de verwerking op een zo gering mogelijke aantal locaties plaats. Op die wijze wordt zoveel mogelijk voorkomen dat persoonsgegevens (onbedoeld) worden gedeeld met anderen. Er zijn bovendien in het privacyprotocol duidelijke afspraken gemaakt over bewaartermijn, zodat persoonsgegevens niet langer worden bewaard dan noodzakelijk. Doordat de gemeente Leeuwarden een helder protocol datalekken heeft, worden beveiligingsincidenten doorgaans zeer vlot opgepakt waarbij zo spoedig mogelijk organisatorische en technische maatregelen worden genomen om eventuele (verdere) schade als gevolg van het beveiligingsincident te voorkomen.

Ad. 6. Door de in het privacyprotocol afgesproken bewaartermijnen goed na te leven wordt voorkomen dat betrokkene (te) lang geconfronteerd blijft met eventuele onterechte ondermijningssignalen jegens hem. Verder dient er vanuit te worden gegaan dat de coördinator ondermijning en de deelnemers van het signaaloverleg voldoende expertise hebben om te beoordelen of een signaal terecht is en dat de weging juist plaats vindt.

Ad. 7. Zie onder ad. 5.

Ad. 8. Zie onder ad. 6.

Akkoord van de FG

Naam Functionaris Gegevensbescherming: P.B.A. Bruin

Datum: 29-03-2019

Handtekening:

