



Gegevensbeschermings- effectbeoordeling (PIA)

[Ministerie/Onderdeel/Afdeling/Proces]

[Directie]

[Plaats/Datum]

Maatregelen
nemen
Privacybewustwording
PIA
Doelbinding
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier

Naam ministerie - Naam directie

Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum

Naam: Typ naam/functie

Advies functionaris voor gegevensbescherming: Selecteer/typ datum

Naam: Typ naam/functie

Advies CIO: Selecteer/typ datum

Naam: Typ naam/functie

Gegevensbeschermings- effectbeoordeling (PIA)

Naam ministerie

Naam directie

Contact:

Ministerie xxx, directie xxx

xxx

xxx

xxx

x

x

x

x

Versie: 1.0 December 2017

Inhoudsopgave

Inleiding	3
A. Beschrijving kenmerken gegevensverwerkingen	3
1. Voorstel	3
2. Persoonsgegevens	3
3. Gegevensverwerkingen	3
4. Verwerkingsdoeleinden	3
5. Betrokken partijen	3
6. Belangen bij de gegevensverwerking	3
7. Verwerkingslocaties	3
8. Techniek en methode van gegevensverwerking	3
9. Juridisch en beleidsmatig kader	3
10. Bewaartermijnen	3
B. Beoordeling rechtmatigheid gegevensverwerkingen	3
11. Rechtsgrond	3
12. Bijzondere persoonsgegevens	3
13. Doelbinding	3
14. Noodzaak en evenredigheid	3
15. Rechten van de betrokkene	3
C. Beschrijving en beoordeling risico's voor de betrokkenen.....	3
16. Risico's	3
D. Beschrijving voorgenomen maatregelen.....	3
17. Maatregelen	3

Inleiding

Voeg hier wanneer gewenst een openingsalinea of inleiding toe. Denk bijvoorbeeld aan:

- Verwijzing naar het privacybeleid of motivatie achter de uitvoering van deze PIA
- Informatie over de manier van opstellen.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel



Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

Het voorstel van wet persoonsgerichte aanpak en meldingen over radicalisering en terroristische activiteiten strekt tot het verstevigen van de wettelijke basis onder de inspanningen van het lokaal bestuur ter bestrijding van radicalisering en terroristische activiteiten. Het wetsvoorstel is opgesteld om een aantal knelpunten weg te nemen met betrekking tot de verwerking van persoonsgegevens in het kader van het casusoverleg radicalisering. Deze nieuwe voorgestelde regeling van de verwerking van persoonsgegevens kan echter niet los worden gezien van de huidige regeling, die grotendeels wordt ingevuld door het modelconvenant. Vandaar dat in deze PIA op verschillende plekken naar het convenant wordt verwezen.

Meer in het bijzonder introduceert het wetsvoorstel een wettelijke taak en een wettelijke mogelijkheid voor het college van burgemeester en wethouders: Het organiseren van casusoverleggen waarin de aanpak van radicaliserende of geradicaliseerde personen kan worden besproken en de mogelijkheid om meldingen inzake radicalisering door te geven aan andere deelnemers van de casusoverleggen, ook voor zover het gaat om bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard.

In aansluiting hierop voorziet het wetsvoorstel in een grondslag voor gegevensdeling door de aan de genoemde casusoverleggen deelnemende partijen ten behoeve van de afstemming van maatregelen. In de op dit moment functionerende casusoverleggen vindt deze gegevensdeling plaats op grond van de op de deelnemers toepasselijke regels voor gegevensdeling. Om buiten twijfel te stellen dat ten behoeve van de afstemming van maatregelen gegevensdeling altijd mogelijk is, is in het voorstel een daarop toegespitste grondslag voor gegevensdeling opgenomen.

2. Persoonsgegevens



Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

De te verwerken categorieën van persoonsgegevens worden in het wetsvoorstel niet verplicht voorgeschreven. Deze categorieën kunnen verschillen per individuele casus: per casus dient te worden afgewogen welke (categorieën) persoonsgegevens noodzakelijk en evenredig zijn. Het wetsvoorstel voorziet in een grondslag om deze gegevens uit te wisselen (gewoon, bijzonder, strafrechtelijk en wettelijk identificerend), maar schrijft niet voor en bepaalt niet welke gegevens dit zijn.

Het modelconvenant bevat enkele bepalingen over welke gegevens respectievelijk ten behoeve van de weegploeg (art. 8) en het casusoverleg (art. 10) worden vastgelegd in een digitaal bestand.

Gelet op het doel van dit wetsvoorstel, de doelen van de samenwerkingsverbanden en de hiervoor genoemde artikelen uit het modelconvenant, zouden bijvoorbeeld de volgende categorieën persoonsgegevens kunnen worden verwerkt:

Wettelijk identificerend:

- BSN

Gewoon

- Leeftijd
- gegevens over uitkeringen, maatschappelijke ondersteuning etc.
- NAW-gegevens
- Paspoortnummer – nodig om uitvoering te kunnen geven aan de paspoortmaatregel (artikelen 23 en 23b Paspoortwet). De rapportages daarover, waar het paspoortnummer in voorkomt, moeten gedeeld kunnen worden binnen het casusoverleg ten behoeve van de (mogelijke) uitvoering van paspoortmaatregelen.)

Bijzonder

- Etniciteit
- Geloofsovertuiging
- Gezondheid (dat iemand bij een GGZ-instelling onder behandeling is),

Strafrechtelijk

- Gegevens over strafrechtelijke antecedenten en lopende strafrechtelijke onderzoeken, justitiële contacten.

Op grond van artikel 2, tweede en vierde lid, worden, indien dat noodzakelijk is voor de bevordering van de afstemming van de maatregelen, tevens persoonsgegevens verwerkt van personen die in zeer nauw verband staan tot de in het eerste lid bedoelde personen. Dat is allereerst noodzakelijk om in te kunnen schatten of er sprake is van een netwerk; met wie betrokkene omgaat kan immers bepalend zijn om de eventuele mate van radicalisering te duiden. Voorts is dit noodzakelijk om de ideologische beïnvloeding door de betrokkene te kunnen beperken ter preventie van verdere radicalisering. Tot slot kan de directe omgeving van belang zijn als interventiemogelijkheid.

Ook kan het gaan om persoonsgegevens (naam en werkadres) van degenen die een rol kunnen spelen in de aanpak van de radicalisering, wanneer dat niet (alleen) een instantie zou zijn maar een natuurlijk persoon.

3. Gegevensverwerkingen



Geef alle voorgenumen gegevensverwerkingen weer.

Melding:

Gemeenten ontvangen in hun dagelijkse praktijk op verschillende manieren signalen van radicalisering. Deze signalen ontvangen zij van lokale partners uit het zorg- en/of veiligheidsdomein of van ongeruste burgers. Om deze signalen op een juiste manier door te geleiden naar de meest geschikte partij of een casusoverleg, en om hulp te bieden aan de persoon die het betreft hebben veel gemeenten een zogenaamd 'meldpunt radicalisering' ingericht. Het wetsvoorstel regelt dat gemeenten –als zij signalen ontvangen over radicaliserende of reeds geradicaliseerde personen – deze meldingen kunnen doorgeven aan andere deelnemers van casusoverleggen, ook voor zover het gaat om bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard. Deze signaleringen kunnen bijvoorbeeld het startpunt vormen van een proces waarin politie, Openbaar Ministerie en gemeente gezamenlijk signalen analyseren en beoordelen ten aanzien van een persoon die kunnen duiden op radicalisering of extremisme.

Casusoverleg:

Na de beoordeling van het signaal worden benodigde vervolgactiviteiten bepaald, waaronder de noodzaak voor een casusoverleg en opstellen van een plan van aanpak en uitvoeren van maatregelen. Van gemeenten wordt verwacht dat zij in dit verband als een 'spin in het web' optreden, omdat het nodig en gewenst is dat gemeenten partijen bijeenbrengen die ieder voor zich slechts een deelverantwoordelijkheid hebben bij de persoonsgerichte, integrale aanpak. Gemeenten bevinden zich in een unieke centrale positie tussen veiligheidspartners en zorgpartijen. De overbrugging tussen deze werkgebieden is niet belegd bij een enkele organisatie. Zowel op lokaal- als rijksniveau bestaat de verwachting dat gemeenten dit 'gat' opvullen, door hun zogenoemde 'regiefunctie' te vervullen.

Deelnemers aan het casusoverleg wisselen persoonsgegevens uit voor zover dat noodzakelijk is met het oog op de bevordering van de afstemming van maatregelen ten aanzien van een persoon die in de gemeente heeft verbleven, verblijft of zal verblijven en die in verband kan worden gebracht met radicalisering of terroristische activiteiten. Daarbij is het van essentieel belang dat de deelnemende instanties zo vroeg mogelijk relevante informatie over een individu met elkaar delen. Alleen zo kan een integrale en adequate inschatting worden gemaakt van de risico's die van dit individu uitgaan. Voor de persoonsgerichte aanpak moeten deelnemende organisaties informatie met elkaar delen om gezamenlijk een casus te kunnen duiden. De gegevensuitwisseling is ook nodig om een integraal plan van aanpak op te kunnen stellen en vervolgens uit te voeren. Zowel voor de totstandkoming als de uitvoering van dat plan van aanpak is het noodzakelijk en onvermijdelijk dat partners relevante gegevens, waaronder ook persoonsgegevens, verwerken. Ook worden hierbij bijzondere categorieën persoonsgegevens en persoonsgegevens van strafrechtelijke aard verwerkt. Bij het verwerken van de persoonsgegevens moeten de deelnemende instanties zich houden aan de Algemene verordening gegevensbescherming (hierna: AVG), de Uitvoeringswet AVG, de Wet justitiële en strafvorderlijke gegevens en de Wet politiegegevens.

In bovengenoemde voorbeelden is gebruik gemaakt van de bij het modelconvenant behorende handleiding, waarin de wijze van samenwerking nader is omschreven.

4. Verwerkingsdoeleinden



Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Het doel van de afstemming over de mogelijke maatregelen is het bereiken van een effectieve persoonsgerichte, integrale aanpak om radicalisering te voorkomen of de-radicalisering te bevorderen. Daarbij worden criminogene en beschermende factoren geïdentificeerd. Dit vormt een startpunt voor gerichte interventies.

Dit sluit aan bij het doel van het samenwerkingsverband zoals verwoord in artikel 3 van het modelconvenant: het reduceren van de risico's voor de samenleving die uitgaan van radicalisering, extremisme, uitreizen, of terugkeer en het bieden van zorg aan subjecten en/of het reduceren van risico's voor de ontwikkeling van minderjarigen door radicalisering, extremisme, uitreizen of terugkeer.

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

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

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

Met persoonsgerichte, integrale aanpak wordt bedoeld op een combinatie van interventies.

Hierbij kan bijvoorbeeld worden gedacht aan de volgende interventies:

- Voor wat betreft politie en OM: strafrechtelijke sancties en maatregelen die speciaal gericht zijn op het voorkomen van de voorbereiding van terroristische aanslagen.
- Voor wat betreft de Minister van JenV: bestuursrechtelijke maatregelen, bijvoorbeeld op grond van de Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding, de Vreemdelingenwet 2000 en de Rijkswet op het Nederlanderschap. Ook kan worden gedacht aan de bevroeringsmaatregel, waarmee financiële tegoeden worden bevroren waardoor de betrokkene er geen toegang meer tot heeft;
- Voor wat betreft reclasseringsinstellingen: de inzet van reclasseringsinstellingen, onder meer door toezicht en controle;
- Voor wat betreft de Raad voor de Kinderbescherming: kinderschermingsmaatregelen;
- Voor wat betreft de gemeente: een veelvoud aan mogelijke interventies, waaronder het aangaan van een gesprek, het ontwikkelen of aanbieden van trainingen, maatregelen op grond van de Wet aanpak woonoverlast, etc.

Op grond van artikel 2, vierde lid, worden, indien dat noodzakelijk is voor de bevordering van de afstemming van de maatregelen, tevens persoonsgegevens verwerkt van personen die in zeer nauw verband staan tot de personen die in verband kunnen worden gebracht met radicalisering. Ook kan het gaan om persoonsgegevens (naam, bereikbaarheidsgegevens en werkadres) van degenen die een rol kunnen spelen in de aanpak van de radicalisering, wanneer dat niet (alleen) een instantie zou zijn maar een natuurlijk persoon.

5. Betrokken partijen



Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Per gemeente of regio kan het casusoverleg verschillend worden ingericht. In het wetsvoorstel is limitatief opgenomen welke partijen deel kunnen uitmaken van het casusoverleg. Dit sluit in hoofdlijnen aan bij de werkwijze zoals omschreven in de handleiding bij het modelconvenant. Gemeente, politie en OM vormen de kernpartijen van het casusoverleg. In het modelconvenant wordt ervan uitgegaan dat deze partijen gezamenlijk verwerkingsverantwoordelijke binnen het casusoverleg zijn. Voor de (dagelijkse) uitvoering van werkzaamheden kunnen de kernpartijen een uitvoerder aanstellen. In de praktijk is dit bijvoorbeeld een gemeente of een veiligheidshuis. De uitvoerder heeft onder meer tot taak alle voorbereidende werkzaamheden ten behoeve van de weging van signalen en het casusoverleg te verrichten, het informatiesysteem en het verwerkingsregister bij te houden en overige op verzoek van de kernpartijen te verrichten werkzaamheden. Het gaat bij alle betrokken partijen om de afdeling of de functionaris die de aanpak radicalisering en extremisme vormgeeft; soms afdelingen die specifiek bij bepaalde casus betrokken zijn. Zoals onder 8 benoemd, zullen autorisaties zo gericht mogelijk worden verstrekt.

- De gemeente

De rol van de gemeente is een regierol ten aanzien van het proces. Gemeenten hebben in deze multidisciplinaire aanpak geleidelijk aan een belangrijke, centrale rol gekregen. Daarnaast heeft de gemeente tot taak de handhaving van de openbare orde op grond van artikel 172 Gemeentewet en wettelijke taken op het terrein van het toegankelijk maken en aanbieden van voorzieningen op het terrein van jeugdzorg, werk en inkomen, scholing, uitkeringen en schuldsaneringen;

- Politie en OM

De politie heeft tot taak de daadwerkelijke handhaving van de rechtsorde en de verlening van hulp aan hen die deze behoeven op grond van artikel 3 van de Politiewet; Het Openbaar Ministerie heeft tot taak de strafrechtelijke handhaving van de rechtsorde op grond van artikel 124 Wet op de rechterlijke organisatie; Hun deelname aan het casusoverleg wordt gerechtvaardigd door de mogelijkheden van strafrechtelijke sancties en maatregelen die speciaal gericht zijn op het voorkomen van de voorbereiding van terroristische aanslagen.

- Minister van JenV

De minister van Justitie en Veiligheid bezit bevoegdheden op grond van de Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding, de Vreemdelingenwet 2000, de Rijkswet op het Nederlanderschap en de Beginselenwet justitiële jeugdinrichtingen. Ook kan worden gedacht aan de bevroeringsmaatregel, waarmee financiële tegoeden worden bevroren.

- Reclasseringsinstellingen

De reclasseringsinstellingen hebben op basis van de Reclasseringsregeling 1995 tot taak bij te dragen aan de veiligheid van de samenleving door het beheersen van risico's en veroordeelden of verdachten te stimuleren zijn of haar gedrag te veranderen. Op die manier werken zij aan het voorkomen van criminaliteit en het terugdringen van recidive. De reclasseringsinstellingen begeleiden de uitvoering van straffen en maatregelen en ander beslissingen van justitiële instanties.

- Raad voor de Kinderbescherming

De Raad voor de Kinderbescherming heeft tot taak om te komen tot een onbedreigd ontwikkelingsperspectief voor het kind (volgens uit artikel 238, tweede lid, van het Burgerlijk Wetboek Boek 1). In het bijzonder gaat het om het beschermen van minderjarigen tegen ernstige bedreigingen in hun ontwikkeling en gezondheid, het optreden ten behoeve van minderjarigen en het op verzoek of uit eigen beweging autoriteiten en instellingen van advies voorzien.

6. Belangen bij de gegevensverwerking



Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

Zoals onder 4 vermeld is het doel van de afstemming over de mogelijke maatregelen het bereiken van een effectieve persoonsgerichte, integrale aanpak om radicalisering te voorkomen of de-radicalisering te bevorderen.

Een dergelijke persoonsgerichte, integrale aanpak is nodig omdat er geen standaard aanpak mogelijk is gebleken ten aanzien van personen die gevoelig zijn voor radicalisering. Uit wetenschappelijk onderzoek naar radicalisering en uit de ervaringspraktijk blijkt dat er geen eenduidig profiel van 'de jihadist' of 'de terrorist' bestaat. Dat betekent dat telkens, in elke casus, zorgvuldig gekeken moet worden naar de achterliggende oorzaken van risicogedrag. Vanuit dat inzicht in achterliggende oorzaken zal vervolgens, in iedere casus, bezien moeten worden welke aanpak en interventies nodig zijn. Dat vergt een persoonsgerichte, integrale aanpak en vereist nauwe samenwerking en inzet van verschillende instanties en disciplines: van veiligheid tot specialistische zorg. Op basis van de specifieke omstandigheden van het geval wordt per casus op grond van een referentiekader met objectieve criteria beoordeeld of een persoonsgerichte, integrale benadering van het subject noodzakelijk is. Indien dit het geval is, wordt voor elke casus beoordeeld welke organen of instanties een taak hebben en betrokken dienen te worden bij de aanpak, en door welk organen of instanties derhalve relevante gegevens, waaronder ook persoonsgegevens, verwerkt moeten worden.

7. Verwerkingslocaties



Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

Nederland

8. Techniek en methode van gegevensverwerking



Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

De wijze waarop de gegevens worden verwerkt binnen een casusoverleg is niet wettelijk voorgeschreven. Dit kan dan ook per gemeente of regio verschillen. Van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen is in beginsel geen sprake.

Binnen veel veiligheidshuizen wordt gebruik gemaakt van het Generiek Casusoverleg Ondersteunend Systeem (GCOS) of een vergelijkbaar systeem, waarin de onder 2 genoemde gegevens toegankelijk zijn. Binnen dergelijke systemen is mogelijk om heel gericht deelnemers voor het overleg te autoriseren. Op die manier hebben alleen geautoriseerde personen toegang tot het overleg en toegang tot de informatie die daarvoor wordt gedeeld. Wanneer een casus wordt behandeld, kunnen de ketenpartners personen toevoegen of autorisaties intrekken. Doordat de ketenpartners alleen noodzakelijke informatie in GCOS delen met elkaar en deze informatie alleen toegankelijk is via gerichte autorisaties, worden persoonsgegevens op een verantwoorde en legitieme manier gedeeld.

9. Juridisch en beleidsmatig kader



Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

Naast de AVG, is voor de verwerkingen van gegevens die zijn verzameld in het kader van opsporing en vervolging, de Wpg en de Wjsg relevant. De grondslag voor gegevensverwerking is voor een belangrijk deel in sectorale wetgeving te vinden (zie hierna onder 11).

Het beleidsmatig kader van de verwerkingen wordt gevormd door het Actieprogramma Integrale Aanpak Jihadisme van de NCTV uit 2014.

10. Bewaartermijnen



Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

De bewaartermijnen van de binnen het casusoverleg gebruikte gegevens zijn niet voorgeschreven in het wetsvoorstel en kunnen per gemeente of regio verschillen. Binnen elk casusoverleg zal de bewaartermijn zelf bepaald en gemotiveerd moeten worden. In het modelconvenant is ervoor gekozen om aan te sluiten bij de termijnen die gelden voor politiegegevens, zijnde 5 jaar. Artikel 13 van het modelconvenant bevat ook afspraken over bewaartermijnen en afscherming.

B. Beoordeling rechtmatigheid gegevensverwerkingen

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

Categorie	Ingang	Termijn	Motivatie	Verantwoordelijkheid
Persoonsgegevens	bewaartermijn	van bewaring	bewaring	voor verwijdering
Naam	Vanaf moment dat	36 ¹ als de	Deze	Functioneel beheerder

11. Rechtsgrond



Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Grondslagen voor verwerking

Gemeente:

In het kader van de aanpak van radicalisering en terroristische activiteiten:

- de handhaving van de openbare orde op grond van artikel 172 Gemeentewet en zijn wettelijke taken op het terrein van het toegankelijk maken en aanbieden van voorzieningen op het terrein van jeugdzorg, werk en inkomen, scholing, uitkeringen en schuldsaneringen. De rechtsgrond voor de verwerking van persoonsgegevens van de gemeente ten behoeve van deze taak is als gevolg hiervan gelegen in art. 6 lid 1 sub e AVG (taak van algemeen belang / openbaar gezag).
- Met voorliggend wetsvoorstel heeft de gemeente er een taak en mogelijkheid bijgekregen: Het organiseren van casusoverleggen waarin de aanpak van radicaliserende of geradicaliseerde personen kan worden besproken en de mogelijkheid om meldingen inzake radicalisering door te geven aan andere deelnemers van de casusoverleggen, ook voor zover het gaat om bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard. Op grond van artikel 6, eerste lid, onder e van de AVG mag de gemeente persoonsgegevens verwerken indien de verwerking 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 (zie daarvoor de in artikel 2 van het convenant en de in het vorige punt genoemde taken);

Met betrekking tot de verstrekking van persoonsgegevens ten behoeve van de afstemming van maatregelen zoals bedoeld in art. 2 lid 1 Wetsvoorstel casusoverleg en meldingen radicalisering:

- Deelnemende instanties zijn verplicht om elkaar persoonsgegevens te verstrekken voor zover dat noodzakelijk is met het oog op de bevordering van de afstemming van maatregelen. Het gaat hierbij om een lidstaatrechtelijke bepaling in de zin van artikel 6, vierde lid, aanhef, AVG die onverenigbare verdere verwerkingen mogelijk maakt ter waarborging van een belangrijke doelstelling van algemeen belang.

Politie

In het kader van de aanpak van radicalisering en terroristische activiteiten:

- de daadwerkelijke handhaving van de rechtsorde en de verlening van hulp aan hen die deze behoeven op grond van artikel 3 van de Politiewet. De rechtsgrond voor de verwerking van persoonsgegevens van de politie ten behoeve van deze taak is als gevolg hiervan gelegen in de Wet politiegegevens, waaronder artikel 8 daarvan.

Met betrekking tot de verstrekking van persoonsgegevens ten behoeve van de afstemming van maatregelen zoals bedoeld in art. 2 lid 1 Wetsvoorstel casusoverleg en meldingen radicalisering: De politie is bevoegd (zowel in de huidige praktijk als in de voorgestelde situatie) om politiegegevens te verstrekken aan:

- leden van het openbaar ministerie op grond van artikel 16 Wpg, voor zover zij deze behoeven in verband met hun gezag of zeggenschap over de politie en voor de uitvoering van andere hun bij of krachtens de wet opgedragen taken;
- de burgemeester voor zover hij deze behoeft in verband met zijn gezag en zeggenschap over de politie en in het kader van de handhaving van de openbare orde (artikel 16 Wpg);
- de deelnemende instanties van het casusoverleg persoonsgerichte aanpak radicalisering, op grond van het bestaande artikel 20 Wpg, de grondslag voor verstrekking aan samenwerkingsverbanden. Volgens artikel 4:5, eerste lid, Besluit politiegegevens gaat het daarbij in beginsel alleen om politiegegevens die oorspronkelijk werden verwerkt op grond van artikel 8 Wpg (gegevensverwerking in kader van de dagelijkse politietaak) en artikel 13 Wpg (gegevensverwerking in kader van ondersteunende taken). Sinds 1 januari 2019 kan het op grond van artikel 4:5, tweede lid, Besluit politiegegevens onder

voorwaarden¹ tevens gaan om politiegegevens die oorspronkelijk werden verwerkt op grond van artikel 9 Wpg (onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval) en artikel 10, eerste lid onder a en c, Wpg (onderzoek in verband met bepaalde ernstige bedreigingen van de rechtsorde). Overigens is in verband met laatstgenoemde categorieën politiegegevens in 2017 een Wpg-machtigingsbesluit² vastgesteld. Met het oog op het beperken en keren van de bedreiging van de democratische rechtsorde als gevolg van terrorisme en extremisme is het noodzakelijk om in de analyse en beoordeling ook de laatstgenoemde categorieën politiegegevens te betrekken.

- *In het wetsvoorstel wordt buiten twijfel gesteld dat de politie bevoegd is om in het casusoverleg politiegegevens in te brengen op grond van het voorgestelde artikel 20, derde lid, Wpg. Momenteel is dit mogelijk op grond van het bestaande artikel 20 Wpg. Voor het casusoverleg relevante doeleinden uit dit artikel zijn met name het voorkomen en opsporen van strafbare feiten, het handhaven van de openbare orde en het uitoefenen van toezicht op het naleven van regelgeving. Deze criteria zijn niet in alle gevallen toegesneden op de gegevensverstrekking die noodzakelijk is voor de casusoverleggen radicalisering.*

Openbaar Ministerie:

In het kader van de aanpak van radicalisering en terroristische activiteiten:

- de strafrechtelijke handhaving van de rechtsorde op grond van artikel 124 Wet op de rechterlijke organisatie. De rechtsgrond voor de verwerking van persoonsgegevens van het OM ten behoeve van deze taak is als gevolg hiervan gelegen in de Wjsg, in het bijzonder artikel 2.

Met betrekking tot de verstrekking van persoonsgegevens ten behoeve van de afstemming van maatregelen zoals bedoeld in art. 2 lid 1 Wetsvoorstel casusoverleg en meldingen radicalisering:

- Wanneer het OM in een casusoverleg strafvorderlijke gegevens inbrengt, is het vanwege de geheimhoudingsplicht uit de Wet justitiële en strafvorderlijke gegevens (artikel 52 Wjsg) noodzakelijk dat hier een uitzondering op van toepassing is. Het OM is op dit moment reeds bevoegd – en blijft dat in de voorgestelde situatie – om binnen de kaders van artikel 39f, eerste lid, Wjsg strafvorderlijke gegevens te verstrekken, onder meer voor het voorkomen en opsporen van strafbare feiten, het nemen van een bestuursrechtelijke beslissing, het handhaven van de orde en veiligheid of het uitoefenen van toezicht op het naleven van regelgeving. Het OM kan deze gegevens delen met partijen indien, kort gesteld, een zwaarwegend belang aan de orde is en één van de in artikel 39f, eerste lid, limitatief opgesomde doeleinden. Het moet dan gaan om partijen die vanuit hun wettelijke taak bemoeienis met een casus zouden moeten hebben. Zo kan het OM bijvoorbeeld gegevens delen met de burgemeester indien er sprake is van een zwaarwegend belang dat raakt aan de handhaving van de openbare orde.
- *In het wetsvoorstel wordt buiten twijfel gesteld dat het OM bevoegd is om in het casusoverleg justitiële of strafvorderlijke gegevens in te brengen op grond van de voorgestelde artikelen 8b en 39fa Wjsg. Momenteel is gegevensverstrekking mogelijk op grond van artikelen 8a en 39f Wjsg. Het zwaarwegend algemeen belang is hierbij gelegen in de bestrijding van radicalisering en terroristische activiteiten, ten behoeve waarvan afstemming tussen deelnemende organisaties van cruciaal belang is. Voor het casusoverleg relevante doeleinden uit artikel 39f jo. 8a Wjsg³ zijn met name het*

¹ Die voorwaarden zijn een beslissing van verwerkingsverantwoordelijke, een strikte noodzaak voor het doel van de verstrekking, en overleg met – kort gezegd – de leider van het onderzoek of zijn plaatsvervanger.

² Stcrt. 2017, 41324. De grondslag hiervoor is artikel 18, tweede lid, Wpg.

³ Artikel 8a Wjsg is genoemd omdat hieruit volgt dat het OM in de gevallen waarin het op grond van artikel 39f Wjsg strafvorderlijke gegevens mag verstrekken, tevens bevoegd is justitiële

voorkomen en opsporen van strafbare feiten, het handhaven van de openbare orde en het uitoefenen van toezicht op het naleven van regelgeving. Deze criteria zijn niet in alle gevallen toegesneden op de gegevensverstrekking die noodzakelijk is voor de casusoverleggen radicalisering.

Raad van de Kinderbescherming:

In het kader van de aanpak van radicalisering en terroristische activiteiten:

- de taken en bevoegdheden volgend uit artikel 238, tweede lid, van het Burgerlijk Wetboek Boek 1, in het bijzonder het beschermen van minderjarigen tegen ernstige bedreigingen in hun ontwikkeling en gezondheid, het optreden ten behoeve van minderjarigen en het op verzoek of uit eigen beweging autoriteiten en instellingen van advies voorzien; De rechtsgrond voor de verwerking van persoonsgegevens van de gemeente ten behoeve van deze taak is als gevolg hiervan gelegen in art. 6 lid 1 sub e AVG (taak van algemeen belang).

Met betrekking tot de verstrekking van persoonsgegevens ten behoeve van de afstemming van maatregelen zoals bedoeld in art. 2 lid 1 Wetsvoorstel casusoverleg en meldingen radicalisering:

- Deelnemende instanties zijn verplicht om elkaar persoonsgegevens te verstrekken voor zover dat noodzakelijk is met het oog op de bevordering van de afstemming van maatregelen. Het gaat hierbij om een lidstaatrechtelijke bepaling in de zin van artikel 6, vierde lid, aanhef, AVG die onverenigbare verdere verwerkingen mogelijk maakt ter waarborging van een belangrijke doelstelling van algemeen belang.

Reclasseringsinstellingen

In het kader van de aanpak van radicalisering en terroristische activiteiten:

- het op basis van de Reclasseringsregeling 1995 bijdragen aan de veiligheid van de samenleving door het beheersen van risico's, en veroordeelden of verdachten te stimuleren zijn of haar gedrag te veranderen. Op die manier werken zij aan het voorkomen van criminaliteit en het terugdringen van recidive. De reclasseringsinstellingen begeleiden de uitvoering van taakstraffen en houden toezicht op maatregelen en andere beslissingen van justitiële instanties. Haar taken bij geradicaliseerde personen worden verricht door een specialistisch landelijk georganiseerd team. Dit team is toegerust om de specifieke signalen van radicalisering te herkennen en daarop te acteren. Op grond van artikel 8 Reclasseringsregeling 1995 juncto artikel 6, eerste lid, onder e van de AVG mogen persoonsgegevens door de Reclassering worden verstrekt indien de verstrekking noodzakelijk is voor de uitvoering van reclasseringswerkzaamheden:
 - I. het houden van toezicht op en het begeleiden van personen die worden verdacht van of die zijn veroordeeld wegens een strafbaar feit;
 - II. het geven van voorlichting en advies aan justitiële instanties;
 - III. het voorbereiden en begeleiden van de uitvoering van de taakstraffen.

Met betrekking tot de verstrekking van persoonsgegevens ten behoeve van de afstemming van maatregelen zoals bedoeld in art. 2 lid 1 Wetsvoorstel casusoverleg en meldingen radicalisering:

- Deelnemende instanties zijn verplicht om elkaar persoonsgegevens te verstrekken voor zover dat noodzakelijk is met het oog op de bevordering van de afstemming van maatregelen. Het gaat hierbij om een lidstaatrechtelijke bepaling in de zin van artikel 6, vierde lid, aanhef, AVG die onverenigbare verdere verwerkingen mogelijk maakt ter waarborging van een belangrijke doelstelling van algemeen belang.

Onze Minister van JenV

gegevens te verstrekken voor zover dat noodzakelijk is met het oog op een zwaarwegend algemeen belang.

Met betrekking tot de verstrekking van persoonsgegevens ten behoeve van de afstemming van maatregelen zoals bedoeld in art. 2 lid 1 Wetsvoorstel casusoverleg en meldingen radicalisering:

- Deelnemende instanties zijn verplicht om elkaar persoonsgegevens te verstrekken voor zover dat noodzakelijk is met het oog op de bevordering van de afstemming van maatregelen. Het gaat hierbij om een lidstaatrechtelijke bepaling in de zin van artikel 6, vierde lid, aanhef, AVG die onverenigbare verdere verwerkingen mogelijk maakt ter waarborging van een belangrijke doelstelling van algemeen belang.

12. Bijzondere persoonsgegevens



Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

Wettelijke identificatienummers

BSN - Gebruik door overheidsorganen toegestaan op grond van artikel 46 UAVG jo de artikelen 10 en 11 van de Wet algemene bepalingen burgerservicenummer.

Bijzondere persoonsgegevens

Etniciteit, geloofsovertuiging en gegevens die zien op de (mentale) gezondheid van een persoon; dezelfde gegevens van partners en kinderen – Gerechtvaardigd op grond van artikel 9, tweede lid, onderdeel g, van de AVG. Dat zwaarwegend algemeen belang is gelegen in de bestrijding van radicalisering en terroristische activiteiten, ten behoeve waarvan afstemming tussen deelnemende organisaties van cruciaal belang is. Daarom biedt het voorstel in artikel 3 een wettelijke grondslag voor de verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen kan blijken, alsmede gegevens betreffende gezondheid, en persoonsgegevens van strafrechtelijke aard, voor zover dat noodzakelijk is voor de uitvoering van de in artikel 2, eerste lid, geregelde taak. Daarmee wordt gebruikt gemaakt van de mogelijkheid om op grond van artikel 9, tweede lid, onder g, AVG een uitzondering te maken op het verwerkingsverbod.

Strafrechtelijke gegevens

Het betreft gegevens over strafrechtelijke antecedenten en lopende strafrechtelijke onderzoeken en justitiële contacten. Bovenstaande geldt ook voor persoonsgegevens van strafrechtelijke aard. Zo moeten de deelnemers aan de weegploeg voor een goede analyse en beoordeling ook persoonsgegevens van strafrechtelijke aard kunnen verwerken. Iedere verwerking van bijzondere categorieën persoonsgegevens en persoonsgegevens van strafrechtelijke aard in de zin van de AVG brengt op grond van bestaand recht verplichtingen met zich mee ten aanzien van onder meer bewaartermijnen, zorgvuldige verwerking en voldoende beveiliging. Op grond van artikel 3, derde lid, kunnen hierover nadere regels bij algemene maatregel van bestuur worden gesteld.

13. Doelbinding



Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Telkens spelen diverse (sociale, economische, culturele) factoren op meerdere niveaus een rol in processen van radicalisering. Dat betekent dat telkens, in elke casus, zorgvuldig gekeken moet worden naar de achterliggende oorzaken van risicogedrag. Vanuit dat inzicht in achterliggende oorzaken zal vervolgens, in iedere casus, bezien moeten worden welke aanpak en interventies nodig zijn. Dat vergt een persoonsgerichte, integrale aanpak en vereist nauwe samenwerking en inzet van verschillende instanties en disciplines: van veiligheid tot specialistische zorg. Op basis van de specifieke omstandigheden van het geval wordt per casus op grond van een referentiekader met objectieve criteria beoordeeld of een persoonsgerichte, integrale benadering van het subject noodzakelijk is. Indien dit het geval is, wordt voor elke casus beoordeeld welke organen of instanties een taak hebben en betrokken dienen te worden bij de aanpak, en door welk organen of instanties derhalve relevante gegevens, waaronder ook persoonsgegevens, verwerkt moeten worden. Als een deelnemer aan het casusoverleg persoonsgegevens verstrekt ten behoeve van de taak van een of meerdere andere deelnemers, is echter niet sprake van een "gewone" verwerking van persoonsgegevens, maar van een "verdere verwerking" in de zin van artikel 6, vierde lid, AVG. Dat betekent dat bij de onderlinge verstrekking tussen de deelnemers tevens moet zijn voldaan aan artikel 6, vierde lid, AVG.

Het voorgestelde artikel 2, tweede lid, van dit wetsvoorstel beoogt aan de onduidelijkheid over toelaatbaarheid van verdere verwerking een einde te maken door een duidelijke grondslag te bieden: deelnemende instanties zijn verplicht om elkaar persoonsgegevens te verstrekken voor zover dat noodzakelijk is met het oog op de bevordering van de afstemming van maatregelen. Het gaat hierbij om een lidstaatrechtelijke bepaling in de zin van artikel 6, vierde lid, aanhef, AVG die onverenigbare verdere verwerkingen mogelijk maakt ter waarborging van een belangrijke doelstelling van algemeen belang, zoals benoemd in artikel 23, eerste lid van de AVG, in dit geval de nationale veiligheid.

Artikel 2, derde lid, van het wetsvoorstel bepaalt dat de deelnemende instanties verplicht zijn tot geheimhouding van persoonsgegevens waarvan zij kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

14. Noodzaak en evenredigheid



Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

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

Meldingen:

Artikel 5, eerste lid, van het wetsvoorstel bepaalt dat het college van burgemeester en wethouders een melding ontvangt ter zake van radicalisering, het college de ontvangen gegevens alleen ter beschikking kan stellen van deelnemende instanties voor zover dat noodzakelijk is met het oog op hun taakuitoefening. Daarmee is de proportionaliteit op het niveau van de wet vastgelegd. Alle meldingen worden door het college opgeslagen voor het beoordelen van toekomstige meldingen. Deze beoordeling heeft geen ander doel dan te bepalen of doorzending naar een bepaalde instantie aangewezen is.

Regiefunctie gemeente:

Als het college de conclusies van het casusoverleg ten aanzien van een bepaald subject vastlegt ten behoeve van een eventueel volgend overleg over deze persoon, dan dient de gegevensverwerking door het college in het kader van deze taak daartoe beperkt te blijven. Het is nadrukkelijk niet de taak van het college om ten aanzien van personen die worden besproken in het casusoverleg een dossier aan te leggen waarin alle door de verschillende deelnemende partijen ingebrachte gegevens worden samengevoegd. Dat is immers niet strikt noodzakelijk voor het uitvoeren van deze taak, het bevorderen van afstemming tussen deelnemende instanties. Per casus wordt beoordeeld welke organen of instanties een taak hebben en betrokken dienen te worden bij de aanpak en door welke organen of instanties derhalve relevante gegevens, waaronder ook persoonsgegevens, verwerkt moeten worden.

Casusoverleg:

Er is geen standaard aanpak mogelijk gebleken ten aanzien van personen die gevoelig zijn voor extremistisch gedachtengoed. Uit wetenschappelijk onderzoek naar radicalisering en uit de ervaringspraktijk blijkt dat er geen eenduidig profiel van "de jihadist" of "de terrorist" bestaat. Dit betekent dat van geval tot geval beoordeeld zal moeten worden welke maatregel het meest geschikt is. Een dergelijke maatwerkaanpak maakt het mogelijk om per geval ook te beoordelen welke persoonsgegevens daarvoor verwerkt moeten worden.

In artikel 10 van het modelconvenant is vastgelegd welke gegevens worden vastgelegd ten behoeve van het casusoverleg. Ook via die weg wordt de proportionaliteit gewaarborgd.

15. Rechten van de betrokkene



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

De betrokkene (of zijn wettelijk vertegenwoordiger), kan op grond van de AVG, de Wjsg of de Wpg aan de verwerkingsverantwoordelijke een verzoek indienen waarbij hij een beroep doet op een van zijn rechten als betrokkenen. Wanneer een dergelijk verzoek wordt ontvangen dient de uitvoerder allereerst te beoordelen aan wie het verzoek gericht is, onder welke wettelijke regime het verzoek valt en welke spelregels daarvoor gelden. Hierbij is het van belang dat er onderscheid wordt gemaakt in verzoeken die gericht zijn aan het samenwerkingsverband en verzoeken die rechtstreeks gericht zijn aan een van de deelnemende partijen van het samenwerkingsverband. Dit maakt namelijk wat uit voor de toepasselijkheid van de wettelijke kaders (AVG of Wpg/Wjsg). De betrokkene heeft ook het recht om bij de Autoriteit Persoonsgegevens een klacht in te dienen over de verwerking van zijn persoonsgegevens.

Op basis van artikel 41 UAVG kunnen de rechten van betrokkenen beperkt worden. Uitgangspunt bij het informeren van betrokkene is "informeren, tenzij...". Het casusoverleg overlegt of een van de uitzonderingen genoemd in artikel 41 UAVG van toepassing is, waardoor het informeren van betrokkene dat hem/haar aangaande informatie wordt verwerkt nog niet mogelijk is, bijvoorbeeld vanwege de bescherming van anderen of de betrokkene zelf. Daarnaast is bijvoorbeeld de uitzonderingen uit bijvoorbeeld artikel 14, vijfde lid, onder c, AVG relevant. De verplichting om betrokkenen te informeren over hen betreffende verwerkingen van persoonsgegevens die niet van hen zijn verkregen, is niet van toepassing indien de gegevensverstrekking verplicht is, zoals bijvoorbeeld het geval is bij verwerking op grond van artikel 2, tweede lid, van het wetsvoorstel.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's



Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;**
- b. de oorsprong van deze gevolgen;**
- c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;**
- d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.**

- a. In algemene zin bestaat het risico dat binnen samenwerkingsverband meer gegevens worden uitgewisseld dan noodzakelijk en dat deze gegevens voor andere doeleinden worden gebruikt dan waarvoor ze bedoeld waren. Meer specifiek bestaat het risico dat betrokkene ten onrechte gelabeld wordt bij gemeentelijke instanties en politie. Dat kan bijvoorbeeld leiden tot regelmatige controles, huisbezoeken.
- b. bespreking in het casusoverleg.
- c. is casusafhankelijk: door een zorgvuldige afweging te maken ten aanzien van de noodzaak van bespreking in een casusoverleg en daarbij noodzakelijk aanwezige partijen worden de risico's van de gegevens verwerking zoveel mogelijk beperkt.
- d. is ook casusafhankelijk: als er ernstige zorgen bestaan, is de inmenging groter en is ook de kans groter dat gegevens met meer partijen gedeeld worden. Dat kan leiden tot geregelde en diepgaande inmenging in de persoonlijke levenssfeer, bijvoorbeeld door bezoek van een wijkagent.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen



Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Signalen worden van geval tot geval gewogen, met behulp van een wegingskader. Van geval tot geval wordt bepaald welke partners deelnemen aan het casusoverleg: op grond van de gezamenlijke analyse bepaalt het casusoverleg of deelname van nader te bepalen partners aan het casusoverleg in dit geval noodzakelijk is.

Hier kunt u aanvullende punten toevoegen: selecteer de tab *Invoegen*, kies *Snelonderdelen*, *Aanvullend punt*

Voeg hier wanneer gewenst een afsluitende alinea toe. Denk bijvoorbeeld aan:

- Lessen uit deze PIA
- Volgende stappen etc.



Maatregelen
nemen

Privacybewustwording

Doelbinding

Noodzaak

Effecten in kaart

PIA

Bescherming van
persoonsgegevens

Risico's

minimaliseren

Richtinggevend

Rechtsgrond

Met open vizier



Gegevensbeschermings- effectbeoordeling (PIA)

Wetsvoorstel gegevensverwerking door
samenwerkingsverbanden (WGS), Kapstok

Ministerie van Justitie en Veiligheid

Directoraat-Generaal Rechtspleging en Rechtshandhaving (DGRR)

Maatregelen
nemen
Privacybewustwording
PIA
Doelbinding
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond.
Met open vizier

Vaststelling verwerkersverantwoordelijke: Selecteer/typ datum

Naam: Minister van Justitie en Veiligheid

Advies functionaris voor gegevensbescherming: Selecteer/typ datum

Naam:

Advies CIO: Selecteer/typ datum

Naam: nvt

Gegevensbeschermings- effectbeoordeling (PIA)

Ministerie van Justitie en Veiligheid
Directoraat-Generaal Rechtspleging en Rechtshandhaving (DGRR)

Contact:

Ministerie van Justitie en Veiligheid, Directoraat-Generaal Rechtspleging en Rechtshandhaving

Inhoudsopgave

Inleiding	5
A. Beschrijving kenmerken gegevensverwerkingen	6
1. Voorstel	6
2. Persoonsgegevens	7
3. Gegevensverwerkingen	7
4. Verwerkingsdoeleinden	8
5. Betrokken partijen	9
6. Belangen bij de gegevensverwerking	9
7. Verwerkingslocaties	10
8. Techniek en methode van gegevensverwerking	10
9. Juridisch en beleidsmatig kader	10
10. Bewaartermijnen	10
B. Beoordeling rechtmatigheid gegevensverwerkingen.....	11
11. Rechtsgrond	11
12. Bijzondere persoonsgegevens	12
13. Doelbinding	12
14. Noodzaak en evenredigheid	13
15. Rechten van de betrokkene	13
C. Beschrijving en beoordeling risico's voor de betrokkenen	14
16. Risico's	14
D. Beschrijving voorgenomen maatregelen	14
17. Maatregelen	14

Inleiding

Het wetsvoorstel Regels omtrent gegevensverwerking door samenwerkingsverbanden (Wet gegevensverwerking door samenwerkingsverbanden) strekt er in de eerste plaats toe de verwerking van persoonsgegevens (...) van een adequate juridische basis te voorzien¹. Het dient slechts om te voorzien in grondslagen voor de verwerking van gegevens door samenwerkingsverbanden.² In het wetsvoorstel betreft het vier concrete bestaande samenwerkingsverbanden, te weten:

- a. het Financieel Expertisecentrum (FEC),
- b. de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV),
- c. de Regionale Informatie- en Expertisecentra (RIEC's) en
- d. de Zorg- en Veiligheidshuizen (ZVH's).

In de tweede plaats maakt het wetsvoorstel het mogelijk om andere samenwerkingsverbanden aan te wijzen, die gebracht worden onder reikwijdte van de WGS zonder dat daarvoor direct een nieuwe formeelwettelijke grondslag gecreëerd moet worden. Deze aanwijzing kan namelijk gebeuren bij amvb, vgl. artikel 3.1. Ook wel een 'kapstok' voorziening genoemd.³

Voor de leesbaarheid zijn er vijf PIA's gemaakt. Deze PIA gaat over algemene aspecten en de 'kapstok' voorziening. De overige vier sluiten daarbij op aan.

¹ Memorie van toelichting, I. Algemeen, par. 1 Inleiding,

² II. Artikelgewijs, Hoofdstuk 1. Algemene bepalingen, artikel 1.3

³ Mvt, I, Algemeen, par. 3.2.2 Doel van zwaarwegend algemeen belang

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de PIA: een overzicht van de relevante feiten van de voorgenomen gegevensverwerkingen. Als de feiten onduidelijk zijn, werkt dit door in de beoordeling.

1. Voorstel



Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en context waarbinnen deze plaatsvindt op hoofdlijnen.

In het wetsvoorstel wordt voorgesteld dat in een samenwerkingsverband overheidsinstanties en soms ook private partijen gezamenlijk gegevens verwerken voor het vervullen van een bij wet of amvb omschreven doel van zwaarwegend algemeen belang.⁴ In dat samenwerkingsverband kunnen maatschappelijke vraagstukken integraal worden aangepakt waarbij verschillende instanties uit de overheid maar soms ook uit de private sector met elkaar samenwerken.

In het huidige recht brengt dat drie knelpunten met zich mee, waarvoor in het wetsvoorstel een voorziening wordt getroffen om die weg te werken.

1. In het huidige recht moet elke individuele deelnemer de noodzaak aantonen om gegevens te verstrekken aan de afzonderlijke deelnemers van het samenwerkingsverband. Een heldere basis om gegevens voor het doel van het samenwerkingsverband als zodanig te vertrekken ontbreekt veelal.
2. In het huidige recht is iedere individuele deelnemer aan een samenwerkingsverband gehouden de ontvangen gegevens vertrouwelijk te behandelen. Deze eis staat in de weg aan een gezamenlijke gegevensverwerking binnen zo'n verband. Dat belemmert de mogelijkheden om in een gezamenlijk casusoverleg⁵ gegevens over bepaalde personen en ondernemingen met elkaar in verband te brengen of een gezamenlijke data-analyse uit te voeren teneinde risico-indicatoren of risico-modellen vast te stellen, tenzij de deelnemers hun grondslag in sectorale wetgeving kunnen vinden.
3. Weer een ander knelpunt is dat sectorale wetten veelal geen goede, op samenwerkingsverbanden toegesneden, grondslagen bevatten voor verstrekking aan en verdere verwerking van gegevens door samenwerkingsverbanden waaraan ook een of meer *private partijen* deelnemen, terwijl dat met het oog op de behartiging van een doel van zwaarwegend algemeen belang wel wenselijk kan zijn.
4. Een laatste knelpunt is dat de verstrekking van de resultaten van de verwerking vanuit samenwerkingsverbanden thans vaak een suboptimale grondslag heeft als gevolg van het feit dat de grondslag voor de verstrekking van gegevens aan en de verwerking daarvan binnen een samenwerkingsverband ook al suboptimaal is of niet op samenwerkingsverband is toegesneden.

⁴ Mvt, I. Algemeen, par. 1. Inleiding

⁵ Het kan daarbij gaan om analyses in een concrete casus, bijvoorbeeld inzake de aanpak van criminaliteit, waarbij partijen gezamenlijk bepalen welke interventies de meest geschikte zijn om in de desbetreffende casus op te treden.

2. Persoonsgegevens



Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van persoonsgegevens tevens aan op wie die betrekking hebben. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificerend.

In de PIA's FEC, iCOV, RIEC's en ZVH wordt daarop ingegaan. Hetzelfde geldt t.z.t. voor de andere samenwerkingsverbanden op grond van artikel 3.1 van de WGS.

Artikel 1.5 van de WGS

De onderstaande gegevens kunnen gewoon, bijzonder, strafrechtelijk en wettelijk identificerend zijn.

1. Elke deelnemer verstrekt de bij of krachtens deze wet aangewezen categorieën van gegevens aan het samenwerkingsverband, voor zover dat noodzakelijk is voor het doel van het samenwerkingsverband, tenzij naar het oordeel van de deelnemer zwaarwegende redenen zich daartegen verzetten. Deze verplichting tot verstrekking is mede van toepassing indien een specifieke geheimhoudingsbepaling van toepassing is die het toelaat dat een ander wettelijk voorschrift daarop een uitzondering maakt.
2. Voor zover een specifieke geheimhoudingsbepaling van toepassing is die het niet toelaat dat een ander wettelijk voorschrift daarop een uitzondering maakt, verstrekt een deelnemer de gegevens op grond van de volgende uitzonderingen:
 - a. artikel 20, derde lid, van de Wet politiegegevens;
 - b. de artikelen 8b, 39fa en 51ca van de Wet justitiële en strafvorderlijke gegevens;
 - c. artikel 1:93ga van de Wet op het financieel toezicht;
 - d. artikel 63ea van de Wet toezicht accountantsorganisaties;
 - e. artikel 56a van de Wet toezicht trustkantoren 2018;
 - f. de artikelen 22d en 23aa van de Wet ter voorkoming van witwassen en financieren van terrorisme;
 - g. artikel 10i van de Sanctiewet 1977;
 - h. artikel 6a van de Wet toezicht financiële verslaggeving;
 - i. artikel 3.3 0a van de Wet handhaving consumentenbescherming;
 - j. artikel 208c van de Pensioenwet;
 - k. artikel 202c van de Wet verplichte beroepspensioenregeling.
3. Het eerste lid is mede van toepassing op persoonsgegevens van strafrechtelijke aard.
4. Onverminderd artikel 20, derde lid, van de Wet politiegegevens, verstrekt de rijksbelastingdienst, bedoeld in artikel 3 van de Algemene wet inzake rijksbelastingen, geen gegevens aan deelnemers voor zover dit private partijen zijn.

3. Gegevensverwerkingen



Geef alle voorgenomen gegevensverwerkingen weer.

De vraag welke gegevens een deelnemer als noodzakelijke gegevens in de zin van artikel 1.5 moet verstrekken, is exclusief ter beantwoording van de deelnemer zelf. Zie de desbetreffende PIA's.

Er is in het wetsvoorstel sprake van drie fasen van gegevensverwerking, namelijk: 1) verstrekking aan het samenwerkingsverband, 2) verwerking binnen het samenwerkingsverband en 3) verstrekking uit het samenwerkingsverband van de resultaten van de gegevensverwerking. In schemavorm ziet dit er als volgt uit:

Fase 1:	→ Fase 2:	→ Fase 3:
Deelnemer verstrekt gegevens aan het samenwerkingsverband (op grond van artikel 1.5 en/of de voorgestelde wijziging van de Wpg, Wjsg en andere sectorale wetten)	Deelnemers van het samenwerkingsverband verwerken gezamenlijk gegevens voor het doel van het samenwerkingsverband (op grond van artikel 1.6 en hoofdstuk 2 WGS of amvb)	Het samenwerkingsverband verstrekt de resultaten van de gezamenlijke gegevensverwerking aan een deelnemer of een derde (onder de voorwaarden van artikel 1.7)

4. Verwerkingsdoeleinden



Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Zie de artikelen 2.2, 2.10, 2.17 en 2.25 van de WGS en de afzonderlijke PIA's.

Artikel 3.1:

Bij algemene maatregel van bestuur kunnen andere samenwerkingsverbanden worden aangewezen als samenwerkingsverband in de zin van deze wet, voor een bij deze algemene maatregel van bestuur omschreven doelstelling van zwaarwegend algemeen belang inzake:

- het voorkomen en bestrijden van ernstige vormen van criminaliteit;
- het voorkomen en bestrijden van grootschalig of systematisch onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen; of
- het voorkomen en bestrijden van grootschalige of systematische ontduiking van wettelijke verplichtingen tot betaling van belastingen, retributies en rechten bij in- en uitvoer.

Het doel voor de gegevensverwerkingen moet gaan om een 'taak van zwaarwegend algemeen belang'. 'Dit is een beperkter begrip dan het begrip "taak van algemeen belang", dat in artikel 6 AVG wordt gehanteerd in de formulering van een van de rechtsgronden voor verwerking van persoonsgegevens,' aldus de MvT⁶.

Uit de MvT: 'De term "zwaarwegend algemeen belang" is opgenomen omdat, gelet op de mogelijke impact van gezamenlijke verwerking van persoonsgegevens in een samenwerkingsverband voor de persoonlijke levenssfeer van de betrokkene, voorkomen moet worden dat deze gegevens al te gemakkelijk worden gedeeld. Door opname van de term "zwaarwegend algemeen belang" is de regering ertoe gehouden een concrete onderbouwing te geven van de aanwezigheid van een zwaarwegend algemeen belang, dat voor een specifiek samenwerkingsverband de verwerking van persoonsgegevens rechtvaardigt. Hierbij is een belangenafweging vereist tussen het belang dat gediend wordt met de gezamenlijke verwerking van persoonsgegevens en het belang van de persoonlijke levenssfeer van degenen op wie de persoonsgegevens betrekking hebben. Bij deze

⁶ MvT, I Algemeen, par. 3.2.2

belangenafweging moeten ook de beginselen van proportionaliteit en subsidiariteit worden betrokken.'

5. Betrokken partijen



Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

In de artikelen 2.3, 2.11, 2.19 en 2.27 van de WGS wordt een concrete opsomming gegeven van de betrokken partijen.

In het algemeen geldt: artikel 1.3 en 1.4 van de WGS.

Zie ook H. II. Artikelsgewijs, Hoofdstuk 1. Algemene bepalingen, artikel 1.3

De deelnemers zijn gezamenlijk verwerkingsverantwoordelijke en in die zin ook gezamenlijk opdrachtgever. Dit impliceert dat een deelnemer mede bepaalt voor welke opdrachten gegevens moeten worden aangeleverd en uit dien hoofde ook opdrachten kan tegenhouden.⁷

De juridische verhoudingen tussen de deelnemers hebben uitsluitend betrekking op de nadere uitwerking van de eisen die de AVG stelt ter zake van de gezamenlijke verwerking, zoals de gezamenlijke verwerkingsverantwoordelijkheid.⁸

Het uitgangspunt van de WGS is 'dat de gezamenlijke gegevensverwerking ten dienste moet staan aan de uitoefening van de bestaande wettelijke taken en bevoegdheden van de deelnemers.'⁹

6. Belangen bij de gegevensverwerking



Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

In de afzonderlijke PIA's wordt daarop ingegaan.

Artikel 3.1.:

- a. het voorkomen en bestrijden van ernstige vormen van criminaliteit;
- b. het voorkomen en bestrijden van grootschalig of systematisch onrechtmatig gebruik van overheidsmiddelen en overheidsvoorzieningen; of
- c. het voorkomen en bestrijden van grootschalige of systematische ontduiking van wettelijke verplichtingen tot betaling van belastingen, retributies en rechten bij in- en uitvoer.

⁷ Mvt, I Algemeen, par. 3.3.1

⁸ Mvt, I Algemeen, par. 3.2.1

⁹ Mvt, II. Artikelsgewijs, Hoofdstuk 1. Algemene bepalingen, artikel 1.3

7. Verwerkingslocaties



Benoem in welke landen de voorgenoemen gegevensverwerkingen plaatsvinden.

Nederland.

8. Techniek en methode van gegevensverwerking



Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautomatiseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Zie de afzonderlijke PIA's. In geen geval zal er sprake zijn van geautomatiseerde besluitvorming door het samenwerkingsverband als bedoeld in artikel 22 AVG.¹⁰ De WGS regelt in het geval van iCOV geautomatiseerde gegevensanalyse (artikel 2.13, aanhef en onder c, WGS in samenhang gelezen met de uitwerking daarvan in de amvb).

9. Juridisch en beleidsmatig kader



Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de gegevensverwerkingen.

10. Bewaartermijnen



Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Zie artikel 1.8, zevende lid, WGS in samenhang gelezen met de uitwerking daarvan bij amvb. Zie ook de afzonderlijke PIA's, dan wel de uitvoeringsPIA's.

¹⁰ Mvt, I Algemeen, par. 10, punt 9, slot.

B. Beoordeling rechtmatigheid gegevensverwerkingen

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

11. Rechtsgrond



Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

a. Verstreking van gegevens aan een samenwerkingsverband, artikel 1.5

De WGS geeft voor verstreking van gegevens slechts een grondslag, voor zover sectorale wetten daarvoor ruimte laten, bijvoorbeeld door te bepalen dat bij wettelijk voorschrift van een eventueel gesloten verstrekkingenregime in die wet kan worden afgeweken. Voor zover die ruimte er niet is, dient in de sectorale wet zelf een grondslag voor verstreking te worden opgenomen.¹¹

Artikel 1.5, eerste lid, WGS vormt de basis voor de verstreking van gegevens aan het samenwerkingsverband en is een rechtsgrond voor de verwerking van persoonsgegevens in de zin van artikel 6, eerste lid, onder c, en derde lid, aanhef en onder b, AVG (wettelijke plicht). (MvT, artikelsgewijze toelichting artikel 1.5, eerste lid).

Artikel 6, vierde lid, aanhef AVG in verband met artikel 23, eerste lid, AVG. (MvT, H. I. Algemeen, par. 3.3.1

De grondslagen voor verwerking van persoonsgegevens bij of krachtens de WGS zijn gericht op een doel van zwaarwegend algemeen belang dat niet op voorhand verenigbaar is met de doelen waarvoor de deelnemers de te verstrekken gegevens hebben verzameld.

De verstreking van politiegegevens en van justitiële en strafvorderlijke gegevens door opsporingsambtenaren en officieren van justitie aan een samenwerkingsverband valt wel onder de reikwijdte van de richtlijn gegevensbescherming opsporing en vervolging. Dit betekent dat die verstreking moet voldoen aan de vereisten zoals die zijn neergelegd in de (voorgestelde wijzigingen van) Wpg en de Wjsg.¹²

De WGS past binnen de voorwaarden die de AVG stelt. De AVG biedt een rechtsgrond voor verwerking van persoonsgegevens, als deze voortvloeit uit een wettelijke verplichting of noodzakelijk is voor de vervulling van een taak van algemeen belang en deze taak is vastgesteld bij lidstatelijk recht.¹³ De WGS biedt deze lidstatelijke basis.

b. Verwerking van gegevens binnen een samenwerkingsverband, artikel 1.6: artikel 6, eerste lid, onder e, van de AVG.¹⁴

¹¹ MvT, I Algemeen, par. 3.3.1

¹² MvT, I Algemeen, par. 6

¹³ Artikel 6, eerste lid, onder c en e, en derde lid, aanhef en onder b, AVG.

¹⁴ MvT, I Algemeen, paragraaf 3.2: "Het wetsvoorstel regelt dat een samenwerkingsverband gezamenlijk gegevens mag verwerken voor zover dat noodzakelijk is voor een bij of krachtens deze

- c. Verwerking van gegevens met private deelnemers: zie hierboven.
- d. Verstrekking van de resultaten van de verwerking uit een samenwerkingsverband, artikel 1.7. Na de ontvangst van de resultaten is artikel 6, eerste lid, onder c, e of f, AVG de rechtsgrond voor de verwerking.¹⁵

12. Bijzondere persoonsgegevens



Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dat is toegestaan.

Artikelen 1.5, derde lid, 1.6, tweede lid, 1.7, zevende lid, en 2.29 WGS

13. Doelbinding



Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

MvT, Par. 3.3.1:

"Het principe van doelbinding is (...) één van de belangrijkste principes in het gegevensbeschermingsrecht en dient daarom ook voor samenwerkingsverbanden het uitgangspunt te blijven. Wel is het wenselijk om, indien daartoe een duidelijke noodzaak bestaat, ruimte te scheppen voor een samenwerkingsverband waaraan deelnemers persoonsgegevens verstrekken voor een ander doel dan waarvoor zij deze hebben verzameld, ook als dit onverenigbaar is met dat oorspronkelijke doel. Samenwerkingsverbanden stuiten namelijk soms op het probleem dat een verstrekking van gegevens aan dat verband door een van de deelnemers en de verwerking daarvan binnen het verband in onvoldoende mate beantwoordt aan dit principe van doelbinding. Dit principe kan op gespannen voet staan met het uitgangspunt van de integrale, multidisciplinaire benadering door een samenwerkingsverband. Daarmee is niet gezegd dat het wenselijk is dit principe voor samenwerkingsverbanden in de zin van de WGS te allen tijde buiten toepassing te laten. De grondslagen voor verwerking van persoonsgegevens bij of krachtens de WGS zijn gericht op een doel van zwaarwegend algemeen belang dat niet op voorhand verenigbaar is met de doelen waarvoor de deelnemers de te verstrekken gegevens hebben verzameld.

wet vastgesteld doel van zwaarwegend algemeen belang. Dit moet worden beschouwd als een taak van algemeen belang als bedoeld in artikel 6, eerste lid, onder e, van de AVG."

¹⁵ MvT, artikelsgewijze toelichting bij artikel 1.7, eerste lid, WGS: "Heeft de (ontvangende) deelnemer een taak van algemeen belang, dan kan deze de resultaten verwerken op grond van een (in sectorale wetgeving gedefinieerde) taak van algemeen belang, bedoeld in artikel 6, eerste lid, onder e, AVG. Betreft het een private deelnemer (zonder taak van algemeen belang), dan mag die de resultaten verwerken voor een gerechtvaardigd belang als bedoeld in artikel 6, eerste lid, onder f, AVG. In geval van de uitvoering van wettelijke verplichtingen is artikel 6, eerste lid, onder c, AVG de rechtsgrond voor de verwerking."

Artikel 6, vierde lid, aanhef, AVG bepaalt dat de verwerking voor een ander, onverenigbaar, doel mag als dat een basis heeft in het lidstatelijk recht (dus de WGS). Het lidstatelijk recht moet dan wel één van de belangen van artikel 23, eerste lid, AVG beschermen. (...)

De WGS bewerkstelligt dat verstrekking van persoonsgegevens door een deelnemer aan het samenwerkingsverband voor het doel van dat verband, niet verenigbaar hoeft te zijn met de oorspronkelijke doeleinden waarvoor de persoonsgegevens worden verwerkt.”

Op verschillende manieren wordt echter gewaarborgd dat de doeleinden ook weer niet in te ver verwijderd verband komen te staan:

- aanwijzing als deelnemer is uitsluitend mogelijk indien deelname noodzakelijk is ten behoeve van het doel van het samenwerkingsverband;
- bij de aanwijzing als deelnemer bij of krachtens de WGS, worden de taken van die deelnemer geformuleerd ten dienste waarvan deze deelneemt;
- verstrekking van de resultaten van de gezamenlijke gegevensverwerking aan een deelnemer is uitsluitend mogelijk voor de vervulling van een publiekrechtelijke taak die aan de deelnemer is opgedragen, wanneer deze verenigbaar is met het doel van het samenwerkingsverband, of indien het een private deelnemer zonder publiekrechtelijke taak betreft, ten behoeve van de behartiging van de gerechtvaardigde belangen of uitvoering van wettelijke plichten van deze private deelnemer, wanneer deze verenigbaar zijn met het doel van het samenwerkingsverband.

14. Noodzaak en evenredigheid



Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

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

Zie Mvt, I. Algemeen, paragraaf 7. Grondrechtelijke aspecten.

15. Rechten van de betrokkene



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

Een deelnemende overheidsinstantie of een deelnemend overheidsorgaan moet als contactpunt worden aangewezen in de zin van artikel 26 AVG. Het contactpunt treedt voor burgers op als aanspreekpunt voor het uitoefenen van rechten op grond van de AVG.¹⁶
Zie ook de uitwerking in de amvb op grond van de WGS.

¹⁶ Mvt, II Artikelsgewijs H. 1. Algemene bepalingen, artikel 1.4

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de gegevensverwerking zoals in onderdeel A en B zijn beschreven en beoordeeld. Het gaat hierbij overigens niet om de risico's van de verwerkingsverantwoordelijke zelf.

16. Risico's



Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;**
- b. de oorsprong van deze gevolgen;**
- c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;**
- d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.**

De WGS bevat slechts in beperkte mate nieuwe verwerkingsmethoden: de iCOV themarapportage (artikel 2.13, aanhef en onder c, WGS in samenhang gelezen met de uitwerking daarvan in de amvb). De risico's kunnen gelegen zijn in de analysemethoden, als daaraan bepaalde vooroordelen ten grondslag liggen, of in de gebrekkige kwaliteit van de data die in de analyse worden betrokken. Daarom bevatten met name de artikelen 1.8 en 1.9 van de WGS en de bijbehorende amvb een groot aantal waarborgen die dergelijke risico's beperken.

D. Beschrijving voorgenomen maatregelen

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen. Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de PIA is, als het gaat om beveiligingsmaatregelen, expertise over informatiebeveiliging belangrijk.

17. Maatregelen



Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Om de risico's te minimaliseren, bevatten de WGS en de bijbehorende amvb talrijke waarborgen om de bescherming van persoonsgegevens te versterken. Ze vormen een concretisering en aanvulling op de waarborgen uit de AVG. Daarbij regelt de WGS diverse vormen van toezicht en verantwoording in aanvulling op de AVG. Allereerst beoordelen de rechtmatigheidsadviescommissies de rechtmatigheid van de gegevensverwerking van het samenwerkingsverband structureel (artikel 1.8, zesde lid, WGS) en moeten zij aandacht hebben voor het tegengaan van risico's op ongelijke behandeling en discriminatie. Ook moet elk samenwerkingsverband een onafhankelijke coördinerend functionaris voor de gegevensbescherming (FG) hebben (artikel 1.4, tweede lid, WGS), die samen met de FG's van de deelnemers toezicht houdt op de gegevensverwerking. Verder zijn onafhankelijke, periodieke privacy audits verplicht, waarvan de resultaten aan de AP moeten worden gezonden (artikel 1.10 WGS).

Zie over generieke waarborgen ook blz. 2 van de MvT:

"Deze hebben betrekking op onder meer de aanwijzing van de verwerkingsverantwoordelijken, de mogelijkheid om bij amvb voorwaarden en beperkingen aan de verwerkingen te stellen, de verlening van toegang tot de systemen waarin de samenwerkingsverbanden gegevens verwerken aan uitsluitend door de deelnemers geautoriseerde medewerkers, het loggen van gegevens die noodzakelijk zijn voor controle en toezicht, het instellen van een rechtmatigheidscommissie die de rechtmatigheid van de verwerking van persoonsgegevens door het samenwerkingsverband beoordeelt, het treffen van technische en organisatorische maatregelen om de kwaliteit van de gezamenlijke gegevensverwerking te bevorderen, geheimhouding en het opstellen van een jaarverslag inzake de gegevensverwerking (zie nader § 3.4)."



Maatregelen
nemen

Privacybewustwording

Doelbinding

Noodzaak

Effecten in kaart

PIA

Bescherming van
persoonsgegevens

Risico's

minimaliseren

Richtinggevend

Rechtsgrond

Met open vizier



DPIA Rapportage Wetsvoorstel Gegevensvergaring openbare orde

Ministerie van Justitie en Veiligheid

Beleidsdirectie Politie en Veiligheidsregio's
Politiebestel, bevoegdheden & informatiefunctie

Den Haag, juli 2025



Vaststelling

Beleidsdirectie Politie en Veiligheidsregio's
Politiebestel, bevoegdheden & informatiefunctie.

Versie: 1.0

Status: Vastgesteld

Revisie:

Versie	Datum	Toelichting
Versie 0.1	mei 2025	Concept omschrijving voorstel, persoonsgegevens en gegevensverwerkingen.
Versie 0.2	14 juni 2025	Verwerking feedback en eerste aanzet verwerkingsdoeleinden en betrokken partijen.
Versie 0.3	4 juli 2025	Verwerken feedback betrokken partijen versie 0.2
Versie 1.0	10 juli 2025	Vastgesteld door de beleidsdirectie.

Voorwoord	8
Managementsamenvatting	11
Beschrijving kenmerken gegevensverwerkingen	
1. Voorstel	134
2. Persoonsgegevens	17
3. Gegevensverwerkingen	23
4. Technieken en methoden van de gegevensverwerkingen	25
5. Verwerkingsdoeleinden	29
6. Betrokken partijen	31
7. Belangen bij de gegevensverwerkingen	34
8. Verwerkingslocaties	35
9. Juridisch en beleidsmatig kader	37
10. Bewaartermijnen	39
Beoordeling rechtmatigheid gegevensverwerkingen	
11. Rechtsgrond	43
12. Bijzondere persoonsgegevens	44
13. Doelbinding	45
14. Noodzaak en evenredigheid	46
15. Rechten van betrokkenen	49
Beschrijving en beoordeling risico's voor de betrokkenen	
16. Risico's voor betrokkenen	52
Maatregelen en restrisico's	
17. Maatregelen	59

Voorwoord

In deze DPIA rapportage worden de bevindingen uiteengezet van de uitgevoerde DPIA voor het Wetsvoorstel gegevensvergaring openbare orde (hierna Wetsvoorstel).

Voor het opstellen van deze rapportage is gebruik gemaakt van het template “model DPIA rapportage Rijksdienst”. Hiertoe is in 17 paragrafen, gebaseerd op Artikel 35 Algemene Verordening Gegevensbescherming (hierna AVG) en Artikel 4c van de Wet politiegegevens (hierna Wpg), zo helder en nauwkeurig mogelijk, een antwoord geformuleerd op de relevante vragen voor de beoordeling van privacyrisico's verbonden aan voorstellen van wet, voorgenomen beleid en verwerkingen.

Met name deel III, de toelichting op de gehanteerde begrippen in het model is van belang bij het schrijven van de DPIA. Hierin wordt per paragraaf beschreven wat wordt verwacht qua beschrijving bij de desbetreffende paragraaf. De toelichtingen uit deel III zijn opgenomen in deze DPIA-rapportage opdat de begrippen eenduidig worden gehanteerd.

In de Management Summary worden de belangrijkste bevindingen samengevat en is voorzien van een overzicht met de conclusies die getrokken zijn bij de uitwerking van de paragrafen.

Leeswijzer

De rapportage bestaat uit een vijf onderdelen:

Management Samenvatting (Op welke wijze wordt zorgdragen voor het borgen van de privacy van betrokkene)

In de managementsamenvatting zijn de belangrijkste punten van de DPIA-rapportage beschreven, met name de geïdentificeerde risico's en de te treffen mitigerende maatregelen.

Onderdeel A. Beschrijving kenmerken gegevensverwerkingen (Wat is het voorstel betreffende de te verwerken gegevens)

Hierin worden de gegevensverwerkingen behandeld welke voortvloeien uit het uitvoeren van het onderhavige wetsvoorstel. Inzichtelijk wordt gemaakt welke overwegingen hebben geleid hebben tot het formuleren van het Wetsvoorstel Gegevensvergaring openbare orde. Daarnaast is uiteengezet welke gegevens het betreft, welke partijen betrokken zijn en de wijze van verwerking het betreft.

Onderdeel B. Beoordeling rechtmatigheid gegevensverwerkingen (is het voorstel zoals uiteengezet onder A te realiseren met in achtname van de privacy rechten van de betrokkene?)

In dit onderdeel wordt de rechtmatigheid van de verwerkingen welke voortvloeien uit het uitvoeren van het onderhavige wetsvoorstel zoals uiteengezet bij onderdeel A beoordeeld.

Onderdeel C. Beschrijving en beoordeling privacyrisico's betrokkenen (Welke privacyrisico's zijn te benoemen voor hetgeen wat wordt voorgesteld)

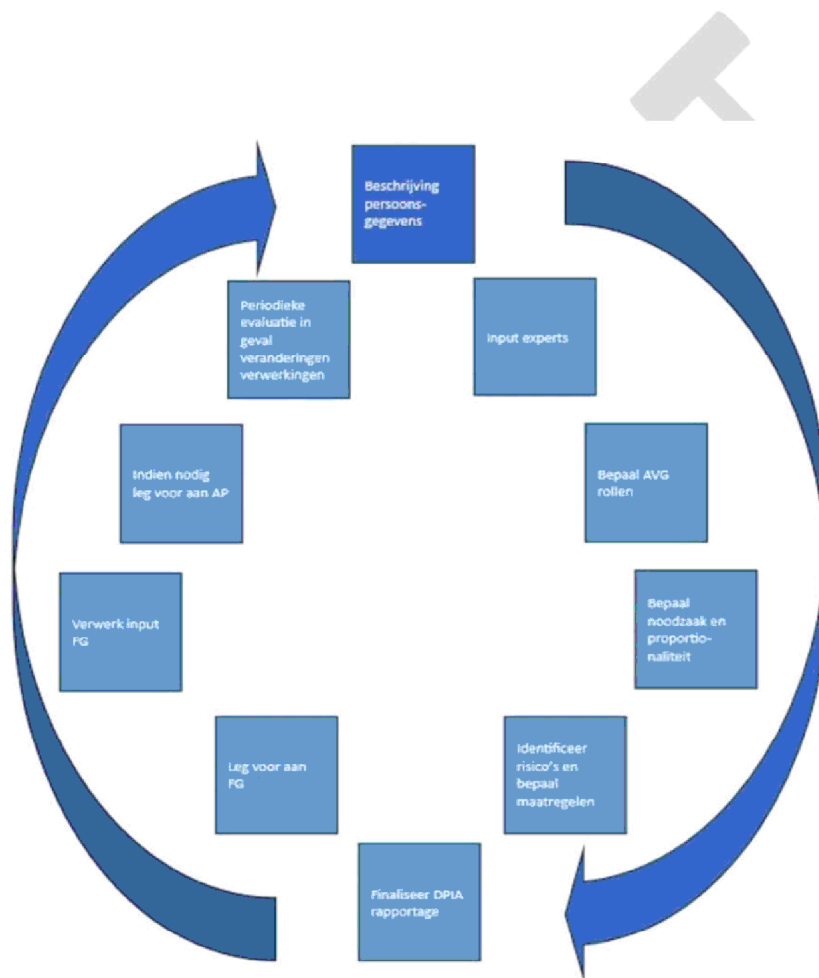
Hierin worden de risico's voor de rechten en vrijheden van betrokkenen beschreven en beoordeeld van de gegevensverwerkingen voortvloeien uit het uitvoeren van het onderhavige wetsvoorstel zoals uiteengezet bij onderdeel A.

Onderdeel D. Maatregelen en restrisico's (Hoe kunnen we de geïdentificeerde risico's voorkomen)

In dit onderdeel worden de mitigerende maatregelen beschreven welke zijn opgenomen in het wetsvoorstel om de geïdentificeerde en beoordeelde privacyrisico's uit onderdeel C. adequaat, naar de eisen en standaarden van deze tijd, te mitigeren.

Dit is het rapportagemodel van het Rijksmodel DPIA. Een DPIA wordt uitgevoerd door de 17 paragrafen in de navolgende pagina's zo helder en nauwkeurig mogelijk in te vullen en te beschrijven.

Processtappen uitvoeren DPIA



Managementsamenvatting

Voorstel

Er is een Privacy Impact Analyse uitgevoerd voor het gebruik van persoonsgegevens binnen de context van het Wetsvoorstel Gegevensvergaring openbare orde.

Met dit wetsvoorstel wordt voorzien in het scheppen van een wettelijke basis (grondslag) voor het verzamelen van bepaalde (persoons)gegevens voor de openbare-ordetaak. Gebleken is dat artikel 3 van de Politiewet hiertoe onvoldoende ruimte biedt. Op basis van dit artikel is het voor de ambtenaren van politie slechts mogelijk informatie te vergaren uit publiek toegankelijke bronnen voor zover er hierbij een *niet meer dan geringe inbreuk* op de persoonlijke levenssfeer van burgers wordt gemaakt. Dat betekent dat op basis van artikel 3 van de Politiewet 2012 slechts in beperkte mate persoonsgegevens worden overgenomen.

Verstoringen van de openbare orde hebben steeds vaker hun wortels in het online domein of worden van daaruit aangejaagd of versterkt. Daarom is in het online domein ook veel informatie over potentiële ernstige verstoringen te vinden die essentieel is voor de burgemeester en de politie om hun taak ter handhaving van de openbare orde naar behoren te kunnen uitoefenen. In het online domein is deze feitelijke informatie onmogelijk op voorhand te scheiden van persoonsgegevens. Bij vergaring van informatie in het online domein wordt dan ook al snel een meer dan geringe inbreuk gemaakt op de persoonlijke levenssfeer.

Het wetsvoorstel reguleert daarom specifieke bevoegdheden voor de burgemeester en de politie zodat zij in voorkomende gevallen meer zicht op mogelijk ernstige verstoringen kunnen krijgen. Op basis van een verbeterde informatiepositie is het mogelijk adequaat te handelen opdat een ernstige verstoring zo veel mogelijk wordt voorkomen, belet of beëindigd.

Concreet betreft het de volgende bevoegdheden voor de burgemeester: Het geven van een bevel aan de politie, op basis van een machtiging van de rechter-commissaris, tot het vergaren van online relevante (persoons)gegevens. Hierbij gaat het om:

- Het zoeken naar en het overnemen van persoonsgegevens uit publiek toegankelijke bronnen en;
- Het in publiek toegankelijke bronnen gericht volgen van personen van wie aannemelijk is dat zij een substantiële rol hebben in een mogelijke ernstige verstoring en in het kader daarvan persoonsgegevens overnemen.

Geïdentificeerde privacyrisico's en (voorgenomen maatregelen)

Bij het gebruik van persoonsgegevens is altijd sprake van een inbreuk op de privacy van degene van wie de gegevens worden gebruikt. In dit geval gaat het om een impact op de rechten van degenen die online berichten plaatsen, degenen die deze berichten lezen en hierop reageren en van degenen die onderwerp zijn van een bericht.

Met de introductie van de bevoegdheden voor de burgemeester waarin het wetsvoorstel gegevensvergaring openbare orde voorziet wordt het mogelijk om een min of meer compleet beeld van bepaalde delen van het persoonlijke leven van de betrokkenen te verkrijgen.

Hiervoor is een wettelijke grondslag vereist met de hierbij horende checks and balances. Het wetsvoorstel voorziet hierin.

Conclusie

Alles overziend kan gesteld worden dat er bij het opstellen van het wetsvoorstel de nodige checks & balances zijn voorzien voor het borgen van de privacy van de betrokkenen.

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

Onder A wordt de eerste stap beschreven van de DPIA: een overzicht van alle relevante feiten van de voorgenomen gegevensverwerkingen. Essentieel is dat de feiten helder en volledig zijn, want het resterende deel van de DPIA is gebaseerd op wat in dit onderdeel is beschreven.

CONCEPT

1. Voorstel

Beschrijf het voorstel waar de DPIA op toeziet op [hoofdpijnen](#) en benoem hoe het voorstel tot stand is gekomen en wat de beweegredenen zijn achter de totstandkoming van het voorstel.

Toelichting

Er moet een DPIA worden uitgevoerd, omdat de verwerking van persoonsgegevens risico's met zich meebrengt die impact hebben op de rechten en vrijheden van de betrokkenen. In geval van formuleren van een wetsvoorstel moet een DPIA worden uitgevoerd voor de verwerking van persoonsgegevens die daarbij aan de orde zijn.

De DPIA heeft als doel deze risico's te identificeren, te beoordelen en zoveel mogelijk te verminderen (mitigeren). Echter, voor de uitvoering van een legitieme DPIA moet duidelijk zijn op welke verwerkingen van persoonsgegevens deze betrekking hebben (gegevensverwerkingen).

Met een korte en bondige beschrijving van de gegevensverwerkingen, wordt de reikwijdte van het DPIA-rapport duidelijk en wordt voorkomen dat bij het nalopen van de 17 paragrafen verschillend wordt gedacht.

Ter controle of de beschrijving van het voorstel compleet is kunnen de volgende punten worden nagegaan:

1. Wat is de aanleiding voor het voorstel;
2. Vervangt of vernieuwt het voorstel een bestaande situatie en is deze bestaande situatie beschreven in relatie tot de nieuwe situatie;
3. Welke organisaties zijn betrokken bij het voorstel;
4. Is bij het voorstel sprake van privacy by design en is beschreven hoe deze beginselen geïmplementeerd zijn; en
5. Wat zijn de redenen dat het voorstel op deze manier tot stand is gekomen en wordt uitgevoerd?

Privacy by Design

Privacy by design, ook wel gegevensbescherming door ontwerp genoemd, houdt in dat privacy en gegevensbescherming mee worden genomen *als eisen bij het formuleren van een wetsvoorstel*. Dit beginsel is een verplichting op basis van de Wet Politiegegevens (Wpg).

In beginsel moet een zo klein mogelijke inbreuk op de privacy van betrokkenen plaatsvinden bij gegevensverwerkingen die voortvloeien uit het uitvoeren van het wetsvoorstel. Welke praktische maatregelen kunnen worden genomen om invulling te geven aan privacy by design?

Om dit te bepalen kan rekening worden gehouden met de volgende elementen:

- De stand van de techniek die van toepassing is in het verwerkingsproces;
- De uitvoeringskosten;
- De aard, omvang, context en het doel van de verwerking; en
- De risico's voor de betrokkene

Deze elementen bepalen samen de maatregelen die opgenomen dienen te worden in het wetsvoorstel opdat het voorstel met de nodige privacybeschermende waarborgen is omkleedt.

Inleiding

Als gevolg van de vlucht die technologische ontwikkelingen genomen hebben en de snelheid waarmee deze elkaar opvolgen, hebben verstoringen van de openbare orde steeds vaker hun wortels in het online domein of worden van daaruit aangejaagd of versterkt. In het online domein is veel informatie te vinden over een ernstige verstoring die al gaande is of mogelijk gaat plaatsvinden.

Deze informatie heeft politie nodig om zicht te krijgen op de ernstige verstoring van de openbare orde en een goede toereikende informatiepositie te verkrijgen. Op basis van deze informatie kan politie een inschatting maken welke inzet passend is opdat een grootschalig evenement in goede banen geleid kan worden. Het huidige van toepassing zijnde wettelijke kader met name het taakstellende artikel 3 van de Politiewet 2012 biedt onvoldoende ruimte voor het verkrijgen van een goed informatiepositie.

Dit vloeit voort uit de jurisprudentie betreffende toepassing artikel 3 Politiewet. Op basis daarvan mag de politie persoonsgegevens verzamelen als de politietaak hierom vraagt, mits er niet meer dan een geringe inbreuk wordt gemaakt op het grondrecht van bescherming van de persoonlijke levenssfeer. Feitelijk is hiervan sprake zolang met de verzamelde persoonsgegevens geen min of meer compleet beeld van bepaalde delen van het persoonlijke leven van de betrokkenen wordt verkregen. Deze geringe inbreuk vormt dan ook de grens voor de grondslag van het verzamelen van gegevens voor de openbare-ordetaak. Met het Wetsvoorstel Gegevensvergaring openbare orde wordt hiervoor een wettelijke grondslag gecreëerd.

Met de introductie van de bevoegdheden voor de burgemeester waarin het Wetsvoorstel Gegevensvergaring openbare orde voorziet wordt het mogelijk om via online gegevensvergaring een min of meer compleet beeld van bepaalde delen van het persoonlijke leven van de betrokkenen te verkrijgen uit publiek toegankelijke bronnen. In voorstel zijn de nodige checks & balances opgenomen zodat het recht op privacy en het recht op veiligheid, twee kanten van dezelfde medaille, met elkaar in evenwicht zijn¹.

Voorstel bevoegdheden

Kern van het wetsvoorstel is dat aan de burgemeester twee te onderscheiden bevoegdheden worden toegekend waarmee de politie onder zijn gezag in staat wordt gesteld om in *publiek toegankelijke bronnen persoonsgegevens te vergaren* over een ernstige verstoring van de openbare orde. De voorgestelde bevoegdheden kunnen worden ingezet indien *aanwijzingen bestaan* dat een ernstige verstoring zal plaatsvinden, maar ook als de verstoring al gaande is.

Dit vormt een aanvulling op artikel 3 van de Politiewet 2012. Doel van deze twee bevoegdheden is *om ernstige verstoringen van de openbare orde te voorkomen, te beletten of te beëindigen*. Dit is onderdeel van de politietaak om de openbare orde daadwerkelijk te handhaven. Als zodanig staat de politie onder het gezag van de burgemeester, die belast is met de handhaving van de openbare orde binnen zijn eigen gemeente.

Strikte voorwaarden (Checks & Balances Veiligheid en Privacy)

Aan de inzet en uitoefening van de voorgestelde bevoegdheden worden strikte voorwaarden gesteld, alsmede aan de verwerking van de persoonsgegevens die met de uitoefening van de bevoegdheden worden vergaard.

- Ten eerste is het aan het bevoegde gezag, de burgemeester, om met inachtneming van de wettelijke voorwaarden te bepalen of en op welke wijze de bevoegdheden door de politie worden uitgeoefend.
- Voordat de burgemeester overgaat tot het afgeven van een bevel daartoe, dient hij daarvoor een machtiging van de rechter-commissaris te hebben gevorderd en verkregen.
- Als niet langer aan de voorwaarden voor de uitoefening van de bevoegdheden wordt voldaan, trekt de burgemeester het bevel in.
- Het wetsvoorstel voorziet daarnaast in een aangepast regime voor de verwerking van de persoonsgegevens die met de uitoefening van de bevoegdheden worden vergaard.
- Dit regime is strikter dan het reguliere regime in de Wet politiegegevens. Zodra blijkt dat de vergaarde persoonsgegevens van geen betekenis zijn voor het onderzoek naar de ernstige verstoring van de openbare orde, moeten deze worden vernietigd.

¹ Rapport, Autoriteit Persoonsgegevens, Veiligheid en Privacy, op zoek naar een nieuwe balans. COT Instituut voor Veiligheids- en Crisismanagement, Universiteit Utrecht, Boom Juridische uitgevers, Den Haag 2007

- Dat geldt ook voor de vergaarde persoonsgegevens die niet langer noodzakelijk zijn voor het onderzoek of na afloop van een periode van een half jaar waarin wordt gezien of deze verder verwerkt moeten worden.

De te verwerken gegevens

Met de introductie van het Wetsvoorstel worden persoonsgegevens verwerkt op basis waarvan een min of meer compleet beeld van bepaalde delen van het persoonlijke leven van betrokkenen kunnen worden verkregen uit publiek toegankelijke bronnen. Beide bevoegdheden uit het wetsvoorstel zijn erop gericht dezelfde (persoons)gegevens, die in eerste instantie deels feitelijk van aard kunnen zijn, uit publiek toegankelijke bronnen te vergaren over de ernstige verstoring van de openbare orde, zoals datum, tijdstip, locatie, alsmede de ernst (bv. geweldsindicatoren, context) en omvang van de verstoring (bv. aantal personen). In publiek toegankelijke bronnen zijn gegevens van meer feitelijke aard over verstoringen van de openbare orde dusdanig verknoot met persoonsgegevens dat deze niet kunnen worden vergaard zonder daarbij ook persoonsgegevens over te nemen. Mede daarom strekken de bevoegdheden tot het overnemen van persoonsgegevens.

Het gaat om gegevens zoals de datum, het tijdstip en de locatie van de ernstige verstoring en de ernst en de omvang van de verstoring, bijvoorbeeld het aantal mensen of bepaalde groeperingen die betrokken zijn. Deze gegevens zijn mogelijk op internet geplaatst in combinatie met gegevens over gedrag en gevoelens. Doordat de online geplaatste gegevens vergezeld kunnen gaan van meningen, voorkeuren en sociale contacten, kunnen ook die gegevens als gevolg van dit wetsvoorstel worden verwerkt.

Impact op de privacy van de betrokkene huidige instrumentarium

Op grond van artikel 3 van de Politiewet 2012 kan de politie ter handhaving van de openbare orde enig onderzoek verrichten in publiek toegankelijke bronnen, zolang daarmee een niet meer dan geringe inbreuk op de persoonlijke levenssfeer wordt gemaakt.

De reikwijdte van de inzet van het huidige instrumentarium onder gelding van artikel 3 van de Politiewet is in de jurisprudentie beperkt met het oog op het beperken van de impact op de privacy rechten van betrokkene. Gezien de digitalisering van de samenleving hebben steeds vaker veel openbare-ordeverstoringen hun wortels in het online domein en online aangejaagde openbare ordeverstoringen kunnen in een korte tijd uitmonden in openbare ordeverstoringen in de fysieke wereld.

Impact op de privacy van de betrokkene inzet nieuwe bevoegdheden

Om het noodzakelijke politietoetreden in de fysieke wereld adequaat te laten plaatsvinden, zal de politie en de burgemeester in de aanloop hiernaartoe kennis moeten kunnen nemen van informatie die duidt op dergelijke dreigingen en deze gegevens indien nodig te delen met de burgemeester als bevoegd gezag. Het gaat hierbij om ontwikkelingen van maatschappelijke onrust die veelal online ontstaan maar een verhoogd risico hebben op een problematische uitwerking in de fysieke wereld.

Bij het vergaren van gegevens in de online wereld kan er al snel sprake zijn van een meer dan geringe inbreuk op een grondrecht, omdat – in tegenstelling tot de fysieke wereld – informatie over iemands persoonlijke leven en de informatie over de openbare ordeverstoring allemaal online te vinden zijn.

Denk bijvoorbeeld aan het volgen van een voor eenieder toegankelijk onlineprofiel van een persoon voor het maken van een inschatting of er een escalatie zal plaatsvinden in de publieke ruimte die leidt tot een ernstige verstoring van de openbare orde, aangejaagd door deze persoon zelf of volgers van het betreffende profiel.

Doordat deze persoon veel deelt op X zal er een goed beeld gevormd kunnen worden van bepaalde aspecten van het persoonlijke leven van de betreffende social media-gebruiker. Hierin is politie allerminst geïnteresseerd, maar doordat gebruikers van online platforms ook gegevens posten uit de persoonlijke levenssfeer (mogelijk ook in dezelfde post), kunnen deze gegevens ook worden

waargenomen en overgenomen. Vanuit het perspectief van de Privacywetgeving is het van belang de privacyrisico's te onderkennen, te beoordelen en zorg te dragen voor borging van de rechten van de betrokkenen. In dit Wetsvoorstel is hierin middels het formuleren van checks & balances voorzien.

CONCEPT

2. Persoonsgegevens

Beschrijf alle persoonsgegevens die worden verwerkt. Classificeer deze persoonsgegevens naar: gewoon, gevoelig, bijzonder, strafrechtelijk en wettelijk identificatienummer. Geef per categorie persoonsgegevens aan welke persoonsgegevens worden verzameld en geef aan wat de bron is van deze persoonsgegevens.

Toelichting

Betrokkenen zijn alle geïdentificeerde of identificeerbare natuurlijke personen binnen de gegevensverwerkingen, oftewel de personen over wie de persoonsgegevens worden verwerkt. Denk hierbij aan:

- Medewerkers,
- Consumenten,
- Cliënten,
- Bezoekers.

Definitie persoonsgegevens

Onder persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon². De term 'natuurlijke personen' betekent hier levende mensen. Informatie over overleden personen, rechtspersonen, dieren, zaken en objecten zijn in principe geen persoonsgegeven³. Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, waaronder selectietechnieken.³¹

Hieronder staan voorbeelden van categorieën persoonsgegevens en type persoonsgegevens die binnen die categorie vallen:

- Naam (voornaam, achternaam, voorvoegsel, initialen)
- Contactgegevens (huisadres, telefoonnummer, e-mailadres)
- Demografische gegevens (leeftijd, geboortedatum en -plaats, geslacht, nationaliteit, opleiding, IQ)
- Apparaat- en internetgegevens (IP-adres, MAC-adres, metadata*, locatie-informatie, geografische informatie**, loggegevens)

Overige persoonsgegevens (voertuigidentificatienummer, persoonlijke voorkeuren).

* Ook metadata zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Over het algemeen is een type metadata op zichzelf niet voldoende identificerend, maar meestal worden meerdere type metadata verzameld van gebruikers. Al deze gegevens gecombineerd met elkaar kan leiden tot identificeerbaarheid van een individu. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, wanneer een document is opgesteld of voor het laatste bewerkt, wanneer is ingelogd, hoelang de gebruiker ingelogd is gebleven, welke webpagina's zijn aangeklikt en de geschreven taal.

** Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Denk hierbij aan de koppeling van gegevens uit de basisregistratie adressen en gebouwen aan andere gegevens en het monitoren van de locaties van voertuigen.

² Artikel 4, eerste onderdeel, AVG en artikel 3, eerste onderdeel, Richtlijn (Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.)

³ Overweging 27 bij de AVG.

Gevoelige persoonsgegevens

Alle overige persoonsgegevens die niet kwalificeren als bijzonder of strafrechtelijk worden in dit model aangemerkt als gewone persoonsgegevens. Gewone persoonsgegevens *betekent niet dat geen sprake is van een hoog risico*. Bepaalde persoonsgegevens kunnen door *de context* waarin zij worden gebruikt *gevoelig zijn en daardoor een hoog risico* met zich meebrengen.

Daarom wordt de categorie gevoelige persoonsgegevens hier onderscheiden, ondanks het feit dat deze categorie niet in de AVG en Wpg voorkomt.

Voorbeelden van gevoelige persoonsgegevens zijn:

- Gegevens over de financiële situatie van de betrokkene;
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
- Gegevens die betrekking hebben op kwetsbare groepen;
- Gebruikersnamen, wachtwoorden en andere inloggegevens;

Gegevens die kunnen worden misbruikt voor (identiteits)fraude en Communicatie- en locatiegegevens⁴.

Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn persoonsgegevens die in principe verboden zijn om te verwerken.

Om bijzondere persoonsgegevens toch rechtmatig te verwerken moet een uitzonderingsgrond uit de AVG/Wpg van toepassing zijn. In de AVG en de Wpg is een limitatieve opsomming opgenomen van deze bijzondere persoonsgegevens:

Ras of etnische afkomst;
Politieke opvattingen;
Religieuze of levensbeschouwelijke overtuigingen;
Het lidmaatschap van een vakbond;
Genetische gegevens;
Biometrische gegevens met het oog op de unieke identificatie van een persoon;
Gegevens over gezondheid;
Gegevens over seksueel gedrag of seksuele gerichtheid⁵.

Voorbeelden van bijzondere persoonsgegevens zijn: het adressenbestand van een kerkblad, gegevens die via een apothekers-app worden verwerkt, ziekte- en verzuimgegevens van werknemers en de ledenlijst van een politieke partij.

Beeldmateriaal

Uit beeldmateriaal zoals foto's en camerabeelden kunnen bijzondere persoonsgegevens, zoals etnische afkomst, religieuze overtuiging of medische gesteldheid, worden afgeleid. Echter, bij beeldmateriaal is pas sprake van de verwerking van bijzondere persoonsgegevens wanneer de verwerking van het beeldmateriaal het doel heeft om onderscheid te maken met die bijzondere persoonsgegevens. Wanneer het doel van de verwerking niet is gericht op het maken van onderscheid op basis van die bijzondere persoonsgegevens, dan wordt verondersteld dat geen bijzondere persoonsgegevens worden verwerkt.

Genetische gegevens

Genetische gegevens zijn persoonsgegevens over overgeërfde of verworven genetische kenmerken van een persoon die unieke informatie verschaffen over de fysiologie of gezondheid en die met name voortkomen uit een analyse van een biologisch monster van die persoon⁶. Denk hierbij aan: chromosomen, DNA of RNA en erfelijke ziekten.

⁴ Stcrt. 2013, nr. 5174, 'CBP Richtsnoeren: Beveiliging van persoonsgegevens', p. 14.

⁵ Artikel 9, eerste lid, AVG en artikel 10 van de Richtlijn.

⁶ Artikel 4, dertiende onderdeel, AVG en artikel 3, twaalfde onderdeel, Richtlijn.

Biometrische gegevens

Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedrag gerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd⁷.

Denk hierbij aan: vingerafdrukken, irispatroon, gezichtsprofiel, looppatroon en stemgeluid. Foto's (en andere gegevens die hierboven zijn genoemd) vallen overigens alleen onder de definitie van biometrische gegevens wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie mogelijk maken⁸.

Gegevens over gezondheid

Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon⁹.

Denk hierbij aan: gewicht, hartslag, handicap, ziekterisico of verleende gezondheidsdiensten.

Nationaliteit en ras/etnische afkomst

Een persoonsgegeven is niet alleen bijzonder wanneer het direct het desbetreffende bijzondere persoonsgegeven onthult. Ook gegevens die *indirect dergelijke informatie onthullen*, dienen aangemerkt te worden als bijzondere categorieën van persoonsgegevens¹⁰.

Wanneer het gegeven 'nationaliteit' wordt verwerkt in combinatie met gegevens als geboorteland, geboorteplaats, herkomst en/of pasfoto, dan blijkt uit rechtspraak dat deze gegevens gecombineerd wel leiden tot gegevens waaruit het ras of etnische afkomst blijkt¹¹.

Echter, volgens de AP is pas sprake van het verwerken van bijzondere persoonsgegevens wanneer *het verwerken van het gegeven 'nationaliteit' tot doel heeft om onderscheid te maken naar ras of etnische afkomst*, of indien het voor de verwerkingsverantwoordelijke redelijkerwijs voorzienbaar is dat *de verwerking tot het maken van onderscheid naar ras of etnische afkomst zal leiden*¹². Het gebruik van nationaliteit kan wel leiden tot de beoordeling dat het een gevoelig persoonsgegeven is, zoals in het kader van fraudebestrijding en het gebruiken van nationaliteit als indicator van fraude¹³.

Daarom is het *voor de beoordeling van ieder verwerkt persoonsgegeven zeer van belang om vast te stellen wat het doeleinde is van de verwerking van desbetreffende persoonsgegevens*.

Ook moet worden beoordeeld of in desbetreffende gegevensverwerking het *neutrale gegeven 'nationaliteit' potentieel kan leiden tot discriminatie van de betrokkene* en welke andere mogelijke risico's de verwerking heeft voor de betrokkene.

⁷ Artikel 4, veertiende onderdeel, AVG en artikel 3, dertiende onderdeel, Richtlijn.

⁸ Overweging 51 AVG.

⁹ 40 Artikel 4, vijftiende onderdeel, AVG en artikel 3, veertiende onderdeel, Richtlijn.

¹⁰ 41 Kamerstukken II 2017/18, 34851, nr. 3, p. 40.

¹¹ Vergelijk overweging 5 van de uitspraak van de rechtbank Rotterdam van 16 mei 2012 (ECLI:NL:RBROT:2012:BW5513), overweging 4.1 van de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 13 augustus 2014 (ECLI:NL:RVS:2014:3002) en overweging 13 tot en met 16 van de uitspraak van de rechtbank Rotterdam van 11 september 2018 (ECLI:NL:RBMNE:2018:4404). Deze overige verwerkte gegevens zijn bijvoorbeeld: geboorteland, geboorteplaats, herkomst en/of pasfoto.

¹² Autoriteit Persoonsgegevens, 'Belastingdienst/Toeslagen. De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag', Onderzoeksrapport z2018-22445, p. 35.

¹³ Kamerstukken II, 35 510, nr. 2, Parlementaire ondervragingscommissie Kinderopvangtoeslag, 'Ongekend Onrecht. Verslag - Parlementaire ondervragingscommissie Kinderopvangtoeslag', 17-12-2020.

Strafrechtelijke persoonsgegevens

Strafrechtelijke persoonsgegevens zijn persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen¹⁴. Verder worden ook persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag als strafrechtelijke persoonsgegevens beschouwd¹⁵.

Het gaat hier zowel om veroordelingen als om verdenkingen van strafbare feiten. Meer in het algemeen, gaat het om persoonsgegevens die betrekking hebben op *gedragingen die aanleiding geven tot maatschappelijke afkeuring en de bescherming van deze persoonsgegevens heeft als doel om te voorkomen dat betrokkenen gestigmatiseerd worden of op andere manier ernstige wijze inbreuk wordt gemaakt op hun privé- of beroepsleven*¹⁶.

Volgens rechtspraak van het Europese Hof van Justitie zijn er drie criteria relevant om te beoordelen of sprake is van strafrechtelijke persoonsgegevens in de zin van artikel 10 AVG:

- Juridische kwalificatie van het strafbare feit naar nationaal recht;
- Aard van het strafbare feit; en
- De zwaarte van de sanctie die aan de betrokkene kan worden opgelegd. Zelfs voor strafbare feiten die naar nationaal recht niet als strafbare feiten in strafrechtelijke zin worden gekwalificeerd, kan uit de aard van het strafbare feit zelf en/of uit de zwaarte voortvloeien dat sprake is van strafrechtelijke persoonsgegevens¹⁷.

Voorbeelden van strafrechtelijke persoonsgegevens zijn:

- Proces-verbaal,
- Sepotbeslissing,
- Strafblad, relaas verhoor en
- Aanvraag voor een toevoeging in een strafzaak.

Strafrechtelijke persoonsgegevens kunnen, bijvoorbeeld, ook voorkomen in zwarte lijsten en een Verklaring Omtrent Gedrag (VOG). Dat is niet per definitie het geval, omdat een zwarte lijst ook kan bestaan uit negatieve gegevens over personen die niet strafrechtelijk van aard zijn en in een VOG kunnen strafrechtelijke persoonsgegevens ontbreken.

Wees echter wel bewust dat dergelijke documenten strafrechtelijke persoonsgegevens kunnen bevatten; *de beoordeling van strafrechtelijke persoonsgegevens dient breder te worden gelezen dan strafbare feiten die direct een relatie hebben met handelingen die vallen onder het strafrecht.*

Nationale identificatienummers

Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, mag uitsluitend worden gebruikt ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald¹⁸.

Het gebruik van deze nummers is dus enkel toegestaan wanneer dit in de wet is geregeld en dient zorgvuldig plaats te vinden. De gedachte hierachter is dat nationale identificatienummers de *koppeling van verschillende bestanden aanzienlijk vergemakkelijkt*. Een verkeerde verwerking of misbruik van dit nummer kan grote gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene. Nationale identificatienummers die ter identificatie van een persoon bij wet zijn voorgeschreven zijn bijvoorbeeld¹⁹:

¹⁴ 45 Artikel 10 AVG.

¹⁵ 46 Artikel 1 UAVG.

¹⁶ Arrest van het Hof (Grote Kamer), C-439/19, 22-06-2021, ECLI:EU:C:2021:504.

¹⁷ Idem

¹⁸ Artikel 46 UAVG.

¹⁹ Het verdient hierbij opmerking dat deze lijst geen limitatieve opsomming is van nationale identificatienummers.

- Burgerservicenummer (BSN)²⁰,
- BIG-nummer (beroepen in de individuele gezondheidszorg),
- Vreemdelingennummer,
- Onderwijsnummer,
- Strafrechtketennummer.

Bron persoonsgegevens

Met de bron van de persoonsgegevens wordt aangegeven *waaruit en/of van welke personen of organisaties de persoonsgegevens worden verkregen*.

Wanneer de persoonsgegevens *niet direct van de betrokkene komen*, dan is het van belang om de *organisatie te noemen waar de gegevens vandaan komen*, vanuit welke tool/platform de gegevens worden gedeeld, met welk doeleinde de persoonsgegevens oorspronkelijk zijn verzameld en op grond waarvan de persoonsgegevens verstrekt mogen worden.

Bijvoorbeeld:

- De persoonsgegevens worden verkregen via een interne database.

De database is opgenomen in een Microsoft Excel-bestand. De database is in beheer van organisatie x. Organisatie x verwerkt deze persoonsgegevens met doeleinde y.

Het is van belang dat bekend is wat de herkomst is van de persoonsgegevens²¹.

Tabel 2.1.

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoonsgegevens (gewoon, gevoelig, bijzonder, strafrechtelijk, identificatienummer)	Bron
Mensen die gebruik maken van social media (plaatser bericht betreffende verstoring openbare orde)	Gegevens over de persoon	Naam, nick name, woonplaats, geslacht, seksueel geaardheid, ras of etnische afkomst, gezondheid, politieke opvattingen en godsdienstige of levensbeschouwelijke overtuigingen	Gewoon en bijzonder	De informatie komt van de betrokkene zelf via social media
	Beeldmateriaal	Foto's en camerabeelden		
	Gegevens over gedrag	Oproepen die kunnen leiden tot ernstige openbare-ordeverstoringen of zelfs rellen	Gewoon, gevoelig en strafrechtelijk	
Mensen die gebruik maken van social media (personen die bijvoorbeeld reageren op een bericht met	Gegevens over de persoon	Naam, nickname, woonplaats, geslacht, seksueel geaardheid, ras of etnische afkomst,	Gewoon en bijzonder	De informatie komt van de betrokkene zelf via social media

²⁰ Overheidsorganen kunnen bij het verwerken van persoonsgegevens gebruik maken van het BSN, met inachtneming van de Wet algemene bepalingen Burgerservicenummer.

²¹ Artikel 3 Wpg, lid 5.

Categorie betrokkenen	Categorie persoonsgegevens	Persoonsgegevens	Type persoonsgegevens (gewoon, gevoelig, bijzonder, strafrechtelijk, identificatienummer)	Bron
betrekking tot de (verwachte) openbare-ordeverstoring)		gezondheid, politieke opvattingen en godsdienstige of levensbeschouwelijke overtuigingen		
	Gegevens over ideologieën, politieke opvattingen, geloof	-	Bijzonder	
	Beeldmateriaal	foto's en camerabeelden		
	Gegevens over gedrag	Oproepen tot ordeverstoring, opstand, rellen	Gewoon, gevoelig, strafrechtelijk	
	Locatie- en geografische informatie	Wanneer in de berichten zelf informatie wordt gedeeld m.b.t. de locatie- en geografische informatie.	Gewoon	
	Gegevens over mogelijke openbare ordeverstoringen	Tijd, locatie, plaats, bijzonderheden aangaande ordeverstoring, context openbare orde verstoring, openbare ordeverstoringselementen	Gewoon	

Geef hier tussen de lijnen aanvullende informatie over de persoonsgegevens

Als gevolg van de ongekende mogelijkheden die de digitalisering van de samenleving met zich mee brengt, verandert ook het werkkterrein van de politie en de burgemeester als het gaat om de handhaving van de openbare orde. De online wereld en de fysieke wereld lopen meer door elkaar heen.

Door de toename in gebruik van laagdrempelige communicatiemiddelen- en technieken, zoals smartphones, tablets en sociale media wordt informatie eenvoudig sneller en virtueel verspreid. Door voornoemde ontwikkelingen wordt informatie veel toegankelijker is geworden.

Het is gebruikelijk geworden dat burgers persoonlijke informatie over zichzelf en wat hen bezighoudt online delen, bijvoorbeeld via sociale media. De geschetste ontwikkeling heeft ervoor gezorgd dat online gemeenschappen zijn ontstaan, waarin bijvoorbeeld een hobby, interesse of politieke overtuiging centraal staat. Het is gemakkelijker geworden om gelijkgestemden te vinden en groepen te vormen, waarbij de fysieke afstand geen of slechts een beperkte rol speelt. Mensen die elkaar wellicht nooit in de fysieke wereld zouden tegenkomen, ontmoeten elkaar daardoor wel online.

In het overzicht hierboven zijn de persoonsgegevens welke aan de orde zijn bij het uitoefenen van de nieuwe bevoegdheden van de burgemeester uiteengezet. Het betreft logischerwijs als gevolg van de gebruikte devices door betrokkenen naast tekst ook beeld en geluidmateriaal.

NB. Feitelijk worde met het gebruik van de nieuwe bevoegdheden dezelfde type gegevens verwerkt als o.g.v. Artikel 3 Politiewet (zie ook de uitwerking bij paragraaf 3)

3. Gegevensverwerkingen

Geef alle [gegevensverwerkingen](#) weer die voortvloeien uit het uitvoeren van het wetsvoorstel en geef aan welke categorieën persoonsgegevens zullen worden verwerkt per gegevensverwerking.

Toelichting

Om de rechtmatigheid van de gegevensverwerkingen te kunnen beoordelen, is het noodzakelijk om *alle gegevensverwerkingen in beeld* te hebben die plaatsvinden binnen de reikwijdte die in het voorstel (paragraaf 1) is opgenomen.

Onder verwerking van persoonsgegevens wordt verstaan: *elke bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens*²². Met een bewerking wordt *iedere handeling* bedoeld die met een persoonsgegeven kan worden verricht.

Denk hierbij aan: 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.

Met andere woorden, het begrip *omvat het gehele proces dat een persoonsgegeven doormaakt*, vanaf het moment van verzamelen tot en met het moment van vernietigen.

Tabel 3.1.

Gegevensverwerking	Categorieën persoonsgegevens Zie uitwerking paragraaf 2)
Volgen	Gewoon, bijzonder, gevoelig
Zoeken naar persoonsgegevens online	
Overnemen	
Verzamelen	
Analyseren	
Verrijken	
Delen	
Opslaan	
Vernietigen	

Geef hier tussen de lijnen aanvullende informatie over de gegevensverwerking

Bevoegdheden

Het Wetsvoorstel Gegevensvergaring openbare orde normeert de specifieke bevoegdheden voor de burgemeester zodat de politie onder zijn gezag online meer informatie kan vergaren met betrekking tot ernstige openbare-ordeverstoringen in het publiek toegankelijk online-domein.

²² Artikel 4, tweede onderdeel, AVG en artikel 3, tweede onderdeel, Richtlijn.

In voorkomende gevallen draagt het inzetten van deze bevoegdheden bij aan het verkrijgen van meer zicht op mogelijke ernstige verstoringen van de openbare orde.

De verkregen verbeterde informatiepositie is noodzakelijk voor het tijdig kunnen vaststellen van een passende politie-inzet ten behoeve van het voorkomen, beletten of beëindigen van een ernstige verstoring van de openbare orde. De burgemeester wordt beter geïnformeerd zodat eventueel passende bestuurlijke maatregelen kunnen worden getroffen en er keuzes kunnen worden gemaakt over de politie-inzet in de fysieke ruimte.

Concreet betreft het de volgende bevoegdheden voor de burgemeester: Het geven van een bevel aan de politie, op basis van een machtiging van de rechter-commissaris, tot het vergaren van online relevante (persoons)gegevens. Hierbij gaat het om:

- Het zoeken naar en het overnemen van persoonsgegevens uit publiek toegankelijke bronnen en;
- Het in publiek toegankelijke bronnen gericht volgen van personen van wie aannemelijk is dat zij een substantiële rol hebben in een mogelijke ernstige verstoring en in het kader daarvan persoonsgegevens overnemen.

Proces

Het te doorlopen proces voor informatievergaring waarbij de verwerkingen zoals uiteengezet in de tabel in figuur 3.1. aan de orde zijn, is op hoofdlijnen als volgt:

1. De handhaving van de openbare orde is een politiebrede taak. Door politie en wordt *informatie verzameld* en *verwerkt* met als doel het voorkomen van ernstige schendingen van de openbare orde. Ook Koninklijke Marechaussee is op basis van artikel 4 lid 1 van de Politiewet 2012 belast met de uitvoering van de politietaak op specifiek benoemde terreinen. Op deze terreinen handhaaft de Koninklijke Marechaussee de openbare orde.

Deze informatievergaring gebeurt binnen de kaders van artikel 3 en 4 Politiewet en valt om die reden buiten de scope van deze DPIA. Op het moment dat politie op basis van de door hen vergaarde informatie tot de conclusie komt dat, meer informatie nodig is en deze enkel verkregen kan worden met de inzet van de bevoegdheid bedoeld in dit wetsvoorstel, stelt de politie de burgemeester hiervan in kennis stellen en kan politie op basis van dit wetsvoorstel de burgemeester om een bevel vragen voor het inzetten van de bevoegdheid.

Dit opdat er een inschatting gemaakt kan worden voor een passend politieoptreden door politie en het gezag voor het voorkomen, beletten of beëindigen van de ernstige verstoring van de openbare orde. Deze inschatting kan anders niet gemaakt worden.

2. Op basis van de aanvraag uit stap 1. maakt de burgemeester de afweging, conform de bepalingen uit het Wetsvoorstel Gegevensvergaring openbare orde, een machtiging aan te vragen bij de rechter-commissaris voor het mogen geven van een bevel tot a. het zoeken naar relevante informatie in publiek toegankelijke online bronnen en deze over te nemen bronnen en/of b. het in publiek toegankelijke bronnen gericht volgen van personen van wie aannemelijk is dat zij een substantiële rol hebben in een mogelijke ernstige verstoring en in het kader daarvan persoonsgegevens overnemen.

4. Op basis van de machtiging door de Rechter-Commissaris, geeft de burgemeester aan de politie het bevel tot of a. of b. of een combinatie van beiden.

5. In deze stap vinden alle verwerkingen zoals uiteengezet in de tabel 3.1. plaats.

NB. De bevoegdheden kunnen worden ingezet als vervolg op de informatievergaring op artikel 3 Politiewet. Met gebruikmaking van de nieuwe bevoegdheden is de kans groter dat er met het

vergaren van de gegevens door de politie/KMAR een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven ontstaat.

Overnemen van persoonsgegevens

Voor de definitie van het begrip overnemen van persoonsgegevens²³ is in het voorstel van de wet waar mogelijk aangesloten bij het gehanteerde construct uit artikel 2.1.1 en artikel 2.8.8 van het nieuwe Wetboek van Strafvordering.

Onder het overnemen van persoonsgegevens moet worden verstaan het kopiëren van persoonsgegevens uit een externe bron. De gegevens die worden overgenomen, zijn gegevens die al zijn opgeslagen op een geautomatiseerd werk dat bereikbaar is vanaf het internet, die gepubliceerd (bijvoorbeeld een webpagina) of gedeeld (bijvoorbeeld het delen van bestanden) zijn.

Na het kopiëren komen de gegevens in de reeds ingebruikzijnde systemen van de politie.

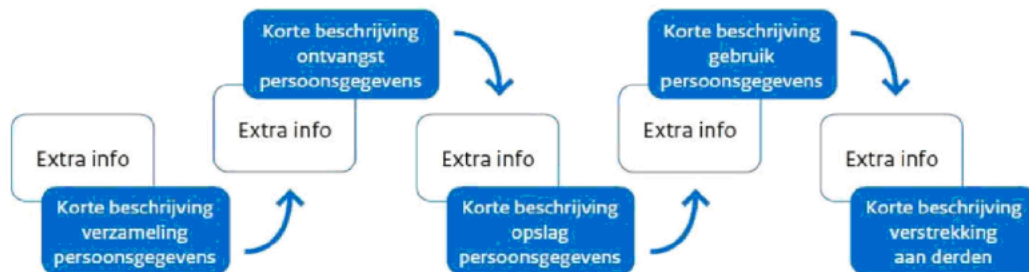
Gebruik specifieke applicaties, software, online platformen of Cloud

Zoals in de paragrafen 2 en 3 uiteengezet wordt voor de verwerking van de gegevens welke plaatsvinden o.g.v. voorstel van wet gebruik gemaakt van de bestaande systemen van de politie.

De privacyrisico's welke uit dit gebruik voortvloeien zijn buiten scope van de DPIA. Deze komen aanbod bij de DPIA voor de uitvoering van het Wetsvoorstel.

Concreet ligt de focus ervan op de inventarisatie en beoordeling van de impact van het voorstel van wet op de rechten van betrokkenen.

Vanzelfsprekend worden, voor zover aan de orde, bij de implementatie van het voorstel door de betrokken partijen de privacyrisico's geïnventariseerd, beoordeeld en gemitigeerd.



Voorbeeld van een afbeelding dat de samenhang tussen gegevensverwerkingen laat zien.

4. Technieken en methoden van de gegevensverwerkingen

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt bij het uitvoeren van het voorstel van wet. Benoem, bijvoorbeeld, of sprake is van bijvoorbeeld (semi-) geautomatiseerde besluitvorming, profilering, een Cloudoplossing of big dataverwerkingen en, zo ja, beschrijf waaruit dat bestaat.

Toelichting

Gebruikmaking van bepaalde technieken en methoden van gegevensverwerking kunnen aanvullende risico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Dit is onder meer het geval bij (semi-)geautomatiseerde besluitvorming, profilering en *big data*-verwerkingen.

²³ Kamerstukken II 2022/2023, 36 327, nr. 3, p. 680.

Geautomatiseerde besluitvorming

Uitsluitend geautomatiseerde besluitvorming is het nemen van besluiten met technologische middelen en zonder menselijke tussenkomst²⁴. Indien uitsluitend geautomatiseerde besluitvorming voor betrokkenen tot rechtsgevolgen leidt of hem anderszins in aanmerkelijke mate treft, dan is dat in beginsel verboden.²⁵

Artikel 7a Wpg voorziet in een algemeen verbod op uitsluitend geautomatiseerde individuele besluitvorming. Hiervan mag worden afgeweken indien sprake is van een van onderstaande uitzonderingen op het verbod, namelijk als het besluit:

- wordt voorzien in voorafgaande menselijke tussenkomst door of namens de verwerkingsverantwoordelijke en in specifieke voorlichting aan de betrokkene.
- niet gebaseerd wordt op de categorieën van politiegegevens, bedoeld in artikel 5 van de Wpg, tenzij de Autoriteit persoonsgegevens over de voorgenomen verwerking is geraadpleegd, overeenkomstig artikel 33b, eerste lid Wpg.

Profilering die leidt tot discriminatie van personen op grond van de in artikel 5 bedoelde categorieën van politiegegevens is verboden.

Kunstmatige intelligentie en algoritmen

Kunstmatige intelligentie, ook wel artificiële intelligentie genoemd, wordt gedefinieerd als software die is ontwikkeld aan de hand van een of meer technieken en benaderingen, die voor een bepaalde reeks door mensen gedefinieerde doelstellingen een resultaat kan genereren, zoals inhoud, voorspellingen, aanbevelingen of beslissingen.

Deze kunnen van invloed zijn op de omgeving waarmee interactie plaatsvindt tussen de software en de betrokkenen²⁶. Algoritmen en kunstmatige intelligentie worden vaak door elkaar gebruikt, maar betekenen wel iets anders. Algoritmen bestaan uit een reeks, meestal wiskundige, instructies. Wanneer deze instructies een bepaalde input krijgen, dan gaat deze door deze instructies heen en er volgt een output op basis van die instructies.

Kunstmatige intelligentie is niet gemakkelijk te definiëren, maar over het algemeen wordt deze term vereenzelvigd met machine learning algorithms.

Dit zijn algoritmen die (kunnen) leren aan de hand van het uitvoeren van de instructies. De software kan op verschillende manieren leren:

- Supervised learning: het algoritme leert aan de hand van gelabelde data met een specifiek uitgezochte dataset. Van tevoren is de data dus op zo'n manier gelabeld, dat de software op basis van die labels uitzoekt wat de correlaties zijn en hoe de data te herkennen en te gebruiken is.
- Unsupervised learning: het algoritme leert aan de hand van ongelabelde data. Zo kan de software zelf trachten structuur en correlaties te herkennen, zonder dat iemand de software de instructie heeft gegeven om specifieke labels te herkennen. Dit type algoritmen werkt met grotere datasets.
- Reinforcement learning: het algoritme leert van de eigen ervaring.

²⁴ Artikel 1 (definities Wpg) profilering: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van die gegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met de bedoeling met name aspecten betreffende zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;

²⁵ Artikel 11, eerste lid, Richtlijn.

²⁶ Artikel 3, eerste lid, Verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie.

Dat betekent dat wanneer het algoritme iets doet waarvoor het een 'beloning' krijgt, bijvoorbeeld dat wordt aangegeven dat iets goed is gedaan, dan probeert het algoritme dit gedrag vaker uit te voeren. Het doel van het algoritme is om zoveel mogelijk deze beloning te bemachtigen, waardoor het algoritme leert om de beloning op optimale manier te bereiken.

Bij de inzet van een systeem op basis van kunstmatige intelligentie of algoritmen is het van groot belang dat het systeem onderdeel uitmaakt van de DPIA en dat deze zorgvuldig wordt getest. Van groot belang is het gebruik van trainingsdata voor de systemen die geen *bias* bevatten, zodat de besluitvorming die uit het systeem komt niet bevooroordeeld of discriminerend is.

Wanneer in de DPIA sprake is van enig gebruik van kunstmatige intelligentie en/of algoritmen, dan dienen deze na afronding van de DPIA toegevoegd te worden aan het algoritmeregister.

Daarnaast is het uitvoeren van een Impact Assessment Mensenrechten en Algoritmes (IAMA) aan te raden en in sommige gevallen zelfs verplicht. Deze assessment kan gelijktijdig met de DPIA worden uitgevoerd en kent op bepaalde punten een overlap. Zie voor meer informatie sectie 1.8.

Cloud

Onder een Cloudoplossing wordt verstaan: het inzetten van een groot netwerk van servers die aan elkaar gekoppeld zijn om specifieke functies uit te voeren, zoals het opslaan en beheren van gegevens, het uitvoeren van toepassingen of het streamen van audiovisuele content. Een groot voordeel van Cloudoplossingen is dat deze schaalbaar zijn, mede deze Cloudoplossingen plaatsvinden op een virtuele infrastructuur en met relatief gemak uitgebreid kan worden.

Hieronder volgen een aantal belangrijke aandachtspunten bij het inzetten van Cloudoplossingen: Dataclassificatie. Gegevens worden gedeeld met een derde partij in een virtuele infrastructuur, waar mogelijk ook andere partijen indirect op zijn aangesloten. Het is daarom van belang dat helder is welke gegevens met welke dataclassificatie worden gedeeld via de Cloudoplossing. Hier kan worden aangesloten op de BIO en de handreiking BIO-dataclassificatie.

Anonimisering.

Cloudaanbieders kunnen stellen dat persoonsgegevens bij het gebruik van hun dienst geanonimiseerd worden. Het is belangrijk om vast te stellen in welk stadium bij het gebruik van de Cloudoplossing de persoonsgegevens geanonimiseerd worden.

Verantwoordelijkheid. Let op de rol van de Cloudaanbieder en de mate van verantwoordelijkheid bij het aanbieden van de dienst; hoe zwaarder de rol, des te meer regie de Cloudaanbieder heeft.

Doelbinding. Hoe meer gegevens bij de Cloudaanbieder worden geplaatst, des te hoger het risico dat de Cloudaanbieder onder eigen verantwoordelijkheid gegevensverwerkingen uitvoert die niet verenigbaar zijn met het oorspronkelijke doel. Zorg in de overeenkomst met de aanbieder dat dit duidelijk is afgebakend. Afhankelijkheid. Door het plaatsen van gegevens in de Cloud ontstaat een technische afhankelijkheid, bijvoorbeeld om gegevens te verwijderen (uitvoeren bewaartermijnen) of bij de rechten van betrokkenen. Contractuele afspraken met de Cloudaanbieder over deze elementen is essentieel om te kunnen voldoen aan wettelijke verplichtingen.

Aanvullende gegevensverwerkingen. Cloudaanbieders hebben veel diensten en functionaliteiten om te leveren en het is aannemelijk dat deze worden aangeboden. Wanneer aanvullende functionaliteiten worden toegevoegd aan de dienstverlening door de Cloudaanbieder, kunnen nieuwe gegevensverwerkingen ontstaan. Nieuwe gegevensverwerkingen moeten opnieuw worden beoordeeld in de DPIA en worden toegevoegd aan het register van verwerkingsactiviteiten.

De European Data Protection Board (EDPB) heeft in 2022 een gecoördineerde handhavingsactie opgezet voor het gebruik van op Cloud gebaseerde diensten in de publieke sector. Indien gegevens opgeslagen of anderszins verwerkt worden in een publieke Cloudvoorziening is daarop het Rijksbrede Cloudbeleid van toepassing.

Profilering

Onder profilering wordt verstaan: elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling de beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen²⁷. Profilering is een procedure die een reeks statistische gevolgtrekkingen kan omvatten.

Profilering wordt vaak toegepast om voorspellingen over mensen te doen door gebruik te maken van gegevens uit verschillende bronnen om een persoon eigenschappen toe te kennen op basis van de kenmerken van anderen die in statistisch opzicht vergelijkbaar zijn²⁸.

Bepaalde gegevens, zoals de resultaten van een zoekopdracht met een zoekmachine, kunnen in combinatie met elkaar een risicoprofiel doen ontstaan. De kans hierop bestaat vooral wanneer meerdere registers met elkaar worden gecombineerd. Er kan sprake zijn van profilering wanneer:

- Op basis van een combinatie van persoonsgegevens, zoals het automerk in combinatie met de leeftijd van de betrokkene wordt besloten iemand extra te controleren;
- Gebruik wordt gemaakt van de gegevens die websitebezoekers achterlaten om de doelgroep van de website mee vast te stellen.

Denk bijvoorbeeld aan een overheidsorganisatie die persoonsgegevens gebruikt om risicoprofielen op te stellen van burgers om daar conclusies aan te verbinden. Bij verwerkingen die vallen onder de werkingssfeer van de Wpg, geldt dat profilering die leidt tot discriminatie op grond bijzondere persoonsgegevens verboden is o.g.v. Artikel 7a lid 3.

Big data

Big data is als zodanig niet gedefinieerd in de privacyregelgeving, *maar hangt als verschijnsel nauw samen met geautomatiseerde besluitvorming en profilering.*

Big data staat voor het verschijnsel dat **grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen worden geanalyseerd waarbij geautomatiseerd naar correlaties wordt gezocht die kennis kunnen opleveren om te kunnen toepassen voor beslissingen op groeps- of individueel niveau**²⁹.

In de kern komt het bij big data-analyses neer op het zoeken naar correlatie (onderlinge samenhang tussen twee reeksen van waarnemingen), in tegenstelling tot causaliteit (betrekking van oorzaak en gevolg). Toepassing van big data brengt specifieke risico's mee en vergt daarom ook specifieke maatregelen (zie onder D).

Nieuwe technologieën

Ook grote verschuivingen in de werkwijze, de manier waarop persoonsgegevens worden verwerkt en de technologie die daarbij gebruikt wordt, kunnen gevolgen hebben voor betrokkenen. Het gaat niet alleen om nieuwe vormen van technologie die nog weinig in gebruik is, maar ook om bekende technologie die op een nieuwe manier wordt ingezet.

Om dit te bepalen kunnen de volgende vragen worden gesteld. Wanneer een van de antwoorden 'ja' is, dan is hoogstwaarschijnlijk sprake van de inzet van een nieuwe technologie.

²⁷ Artikel 3, vierde onderdeel, Richtlijn

²⁸ Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van de Verordening (EU) 2016/679, p.7.

²⁹ Wetenschappelijk Raad voor het Regeringsbeleid (WRR), Big data in een vrije en veilige samenleving, rapport nr. 95, p. 21. De WRR geeft geen scherp omliggende definitie van big data, maar richt zich op de hoofdkenmerken

1) Data: het gaat om grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen, 2) Analyse: de analyse is data gedreven en zoekt geautomatiseerd naar correlaties en 3) gebruik: de analyses moeten leiden tot 'actionable knowledge' (ingrepen in de realiteit op basis van bestandsanalyses).

- a. Is de gebruikte technologie nieuw of nog niet eerder toegepast?
- b. Is de gebruikte technologie bekend maar wordt deze op een nieuwe manier ingezet?
- c. Zorgt de gebruikte technologie op zichzelf voor een verhoogd risico voor de privacy van betrokkenen?

Beschrijf hier tussen de lijnen de technieken en methoden van de gegevensverwerkingen.

Het wetsvoorstel bevat een delegatiegrondslag in artikel 5 voor het stellen van regels voor de geautomatiseerde wijze van overnemen van gegevens.

Indien in een voorstel van wet bepalingen worden opgenomen over ondersteuning op het niveau van systemen zijn deze doorgaans technisch neutraal geformuleerd. Het onderhavige wetsvoorstel voorziet in een aanvulling van bevoegdheden. Uitgangspunt hierbij is dat gebruik wordt gemaakt van de reeds in gebruik zijnde systemen.

De privacyrisico's welke gerelateerd zijn aan gebruik van reeds ingebruikzijnde systemen is dan ook buiten scope van de DPIA.

Concreet ligt de focus ervan op de inventarisatie en beoordeling van de impact van het voorstel van wet op de (inbreuk op de) privacy van betrokkenen.

Vanzelfsprekend worden, voor zover aan de orde, bij de implementatie van het voorstel door de betrokken partijen de privacyrisico's geïnventariseerd, beoordeeld en gemitigeerd conform de geldende wettelijke kaders, Rijksbeleid en standaarden.

Daarbij kan gedacht worden aan maatregelen gericht op het borgen van:

- Controle op de toegang tot de apparatuur;
- Controle op de gegevensdragers;
- Opslagcontrole;
- Gebruikerscontrole;
- Controle op de toegang tot de gegevens;
- Transmissiecontrole;
- Invoercontrole;
- Transportcontrole;
- Herstel;
- Integriteit.

5. Verwerkingsdoeleinden

Beschrijf de doeleinden van alle gegevensverwerkingen.
Voeg aanvullende informatie toe in het tekstveld.

Toelichting

De privacyregelgeving heeft als beginsel dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld³⁰.

De vaststelling van de verwerkingsdoeleinden is een noodzakelijke voorwaarde om te kunnen beoordelen of de gegevensverwerkingen die voortvloeien uit het uitvoeren van het voorstel van wet rechtmatig zijn (onder B) en om vast te stellen welke maatregelen getroffen dienen te worden om de risico's (onder C) te voorkomen of te verkleinen (onder D).

³⁰ Artikel 4, eerste lid, onder b, Richtlijn.

Omschrijf daarom per gegevensverwerking die aan de orde is de verwerkingsdoeleinden zo specifiek mogelijk. Wanneer de verzamelde persoonsgegevens oorspronkelijk zijn verzameld voor een ander doeleinde, dan is er de mogelijkheid om voor die specifieke persoonsgegevens aan te geven wat het oorspronkelijke doeleinde en het huidige (nieuwe) doeleinde is voor het verwerken van die persoonsgegevens en op grond waarvan de persoonsgegevens voor het nieuwe doeleinde mogen worden verwerkt.

Bij verwerkingsdoeleinden kan gedacht worden aan: bestuursrechtelijke handhaving, behandelen van personeelszaken, opsporen van strafbare feiten, het innen van vorderingen, het doen van leveringen en bestellingen, identificatie en authenticatie, het voorbereiden en nemen van Awb-besluiten en het behandelen van geschillen.

Denk ook aan eventuele nevendoeleinden van de gegevensverwerking, zoals: wetenschappelijk, statistisch of historisch onderzoek, archiefbeheer, declaratiedoelinden, rapportagedoeleinden, verbetering van dienstverlening of (door)ontwikkeling van beleid. De verwerkingsdoeleinden moeten zoveel mogelijk worden toegespitst op de concrete gegevensverwerking, zoals die zijn geïdentificeerd onder 3.

Tabel 5.1.

Gegevensverwerking	Verwerkingsdoeleinde	Oorspronkelijk verwerkingsdoeleinde
Volgen	-	Het voorstel van wet voorziet in de specifieke grondslag voor de verwerking met het oog op het voorkomen, beletten of beëindigen ernstige verstoring van de openbare orde.
Zoeken naar persoonsgegevens online	-	
Overnemen	-	
Verzamelen	-	
Analyseren	-	Het eerste lid voorziet in de specifieke grondslag voor de verwerking met het oog op het voorkomen, beletten of beëindigen ernstige verstoring van de openbare orde.
Verrijken	-	
Delen	-	
Opslaan	-	
Vernietigen	-	

Voeg tussen de lijnen aanvullende informatie toe over de verwerkingsdoeleinden.

Artikel 2 voorstel van wet

Het eerste lid voorziet in de specifieke grondslag voor de verwerking met het oog op het voorkomen, beletten of beëindigen van een ernstige verstoring van de openbare orde.

Onder "beletten" wordt verstaan dat de bevoegdheden ook kunnen worden uitgeoefend om de gevolgen van een ernstige verstoring van de openbare orde te beperken, bijvoorbeeld het treffen van mitigerende maatregelen voor een reeds aangevangen ernstige verstoring van de openbare orde als (onmiddellijke) beëindiging daarvan niet mogelijk blijkt.

NB. Het betreft de verwerking van *gegevens uit publiek toegankelijke bronnen (online)*.

Conclusie

Vastgesteld kan worden dat nu met het voorstel van wet helderheid wordt verschaft, het beschikbare instrumentarium voor de politie voor het uitvoeren van de taken onder het gezag van de burgemeester wordt aangevuld voor de online omgeving, de gegevensverwerkingen die voortvloeien uit het uitvoeren van het voorstel van wet als rechtmatig kunnen worden geduid.

6. Betrokken partijen

Benoem alle partijen die betrokken zijn en deel deze in per gegevensverwerking. Deel deze partijen in onder de rollen: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker, ontvanger, betrokkene(n) en derde. Wanneer bekend, benoem ook welke functionarissen/afdelingen binnen deze partijen toegang krijgen tot welke categorieën persoonsgegevens. Voeg aanvullende informatie toe in het tekstveld.

Toelichting

Om de rechtmatigheid van de gegevensverwerkingen, die voortvloeien uit het uitvoeren van het voorstel van wet, te kunnen beoordelen, moet inzichtelijk zijn welke partijen(functioneel) betrokken zijn bij welke gegevensverwerking en in welke hoedanigheid: verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke, verwerker, sub-verwerker, verstrekker of ontvanger³¹.

Wees er bewust van dat een organisatie of partij meerdere AVG-rollen tegelijk kan hebben, bijvoorbeeld dat de verwerkingsverantwoordelijke ook tegelijkertijd een verstrekker kan zijn. Een partij kan niet tegelijk verwerker en verwerkingsverantwoordelijke zijn voor dezelfde gegevensverwerking.

Verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan, die het doel van en de middelen voor de gegevensverwerkingen vaststelt.

Elke verwerking van persoonsgegevens heeft minimaal een verwerkingsverantwoordelijke. Overige partijen die bij de verwerking zijn betrokken kunnen een verwerker, een sub-verwerker of een gezamenlijke verwerkingsverantwoordelijke zijn. Om te beoordelen of een partij verwerkingsverantwoordelijke is, kan naar de volgende situaties gekeken worden:

A. Feitelijke invloed:

De verwerkingsverantwoordelijke bepaalt met welk doel de persoonsgegevens worden verwerkt en de manier waarop dat gebeurt. Als een andere partij voor dezelfde verwerking een verwerker is, moet deze partij de instructies van de verwerkingsverantwoordelijke opvolgen. Deze instructies worden meestal gegeven in een verwerkersovereenkomst.

De gezagsverhouding kan blijken uit schriftelijke afspraken maar uiteindelijk is doorslaggevende wie in de praktijk daadwerkelijk de beslissingen neemt.

Hierbij moet opgemerkt worden dat een verwerker vaak zelf bepaalt welke middelen er worden gebruikt omdat een bepaalde dienst of een bepaald product zo in de markt is gezet. Bij de beoordeling moet in die situaties met name gekeken worden naar de feitelijke invloed op het doel van de verwerking.

³¹ De Autoriteit Persoonsgegevens heeft een tabel gepubliceerd met voorbeelden van situaties en uitleg welke organisatie in die situaties welke rol uitoefenen. (<https://www.autoriteitpersoonsgegevens.nl/documenten/voorbeeldlijst-wie-is-hier-de-verwerker-en-wie-de-verantwoordelijke>)

B. Uitdrukkelijke juridische bevoegdheid

Als er in de wet staat dat een partij bepaalde persoonsgegevens mag of moet verwerken, dan is deze partij daarvoor de verwerkingsverantwoordelijke. Als een partij daarbij ondersteunt, zonder zelfstandig een beroep te kunnen doen op deze wettelijke bepaling, dan is deze partij een verwerker.

C. Impliciete bevoegdheid

Als er geen uitdrukkelijke juridische bevoegdheid bestaat om persoonsgegevens te verwerken dan kan een impliciete bevoegdheid een doorslaggevende factor spelen in het vaststellen of een partij als verwerkingsverantwoordelijke kwalificeert. Denk aan een werkgever die persoonsgegevens van zijn medewerkers verwerkt of een vereniging die de gegevens van haar leden verwerkt.

Verwerker

Verwerker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Dat betekent dat de verwerker persoonsgegevens verwerkt direct onder instructies van de verwerkingsverantwoordelijke.

De verwerker is een persoon of organisatie buiten de organisatie van de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke en verwerker moeten onderling schriftelijk vastleggen wie waarvoor verantwoordelijk en aansprakelijk is .

Deze afspraken moeten worden vastgelegd in een verwerkersovereenkomst.

Een partij is alleen verwerker voor zover het verwerken van persoonsgegevens de primaire opdracht van een andere organisatie is. En deze partij niet rechtstreeks onder het gezag van die organisatie valt.

De verwerker verwerkt persoonsgegevens in opdracht van de verwerkingsverantwoordelijke en niet voor eigen doeleinden. Indien de gegevens wel voor eigen doeleinden worden gebruikt dan is deze partij (voor dat gedeelte van de verwerking van persoonsgegevens) aan te merken als verwerkingsverantwoordelijke.

Dit is vaak het geval als de diensten die de partij aanbiedt niet primair tot doel hebben om persoonsgegevens te verwerken.

Als een partij onder het rechtstreeks gezag van de verwerkings-verantwoordelijke valt dan is deze partij ook geen verwerker, dit is bijvoorbeeld het geval als iemand gedetacheerd is. De gedetacheerde persoon is in die situatie onderdeel van de organisatie van de verwerkingsverantwoordelijke voor wat betreft het verwerken van persoonsgegevens.

Sub-verwerker

De sub-verwerker is de natuurlijke persoon, rechtspersoon of overheidsorgaan die ten behoeve van de verwerker specifieke taken uitvoert in het kader van de samenwerking tussen de verwerker en de verwerkingsverantwoordelijke.

Een sub-verwerker is dus de verwerker van de verwerker.

De verwerker dient schriftelijke toestemming te vragen aan de verwerkingsverantwoordelijke en schriftelijke afspraken met de sub verwerker vast te leggen die wat betreft privacy verplichtingen tenminste hetzelfde strenge niveau hebben als de afspraken die zijn gemaakt tussen de verwerkingsverantwoordelijke en de verwerker. Hiervoor sluit de verwerker een verwerkersovereenkomst af met de sub-verwerker.

Gezamenlijke verwerkingsverantwoordelijken

Wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen van de verwerking bepalen, dan zijn zij gezamenlijke verwerkingsverantwoordelijken en moeten zij onderling vastleggen wie waarvoor verantwoordelijk en aansprakelijk is.

Een belangrijk criterium voor de beoordeling of sprake is van gezamenlijke verwerkingsverantwoordelijkheid is het volgende: is het mogelijk voor het verwerkingsproces of processen die in deze DPIA worden beoordeeld om door te gaan zonder de samenwerking tussen de twee (of meer) organisaties?

Wanneer organisaties namelijk individueel toch het proces kunnen uitvoeren, dan is sprake van individuele verwerkingsverantwoordelijkheid. Wanneer sprake is van onlosmakelijke processen, dan is waarschijnlijk sprake van gezamenlijke verwerkingsverantwoordelijkheid³².

Het is belangrijk dat gezamenlijke verwerkingsverantwoordelijken een regeling treffen waarin de verantwoordelijkheden voor de naleving van de AVG-regels worden vastgelegd. Hierin moet, bijvoorbeeld, worden vastgelegd wie verantwoordelijk is voor het afhandelen van een datalek en wie welke verantwoordelijkheden heeft bij het afhandelen van verzoeken van betrokkenen. De belangrijkste aspecten van de regeling moeten worden meegedeeld aan de betrokkenen, bijvoorbeeld door middel van een privacyverklaring.

Ontvanger

Ontvanger is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan aan wie/waaraan de persoonsgegevens worden verstrekt.

Verstrekker

Verstrekker is de natuurlijke persoon, de rechtspersoon of het overheidsorgaan die/dat de persoonsgegevens verstrekt aan een andere partij.

Derde

Een derde is een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die geen betrokkene, verwerkingsverantwoordelijke, verwerker of een persoon is die rechtstreeks onder gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is om de persoonsgegevens te verwerken.

De derde is wel een persoon of organisatie die betrokken is bij de gegevensverwerking, maar daar niet op een directe manier mee te maken heeft. De derde komt, bijvoorbeeld, naar voren bij de juridische grondslag 'gerechtvaardigd belang van een derde'. Op basis van deze juridische grondslag kan een verwerkingsverantwoordelijke gegevens verwerken op basis van de belangen van een derde.

Tabel 6.1

Naam partij	Rol partij	Persoonsgegevens
Burgemeester	Verwerkingsverantwoordelijke	Voor de te verwerken gegevens zie paragraaf 2.
Politie	Verwerkingsverantwoordelijke	
KMAR	Verwerkingsverantwoordelijke	
Rechter Commissaris	Verwerkingsverantwoordelijke	
Mensen van wie gegevens worden verwerkt	Betrokkene	Voor de te verwerken gegevens zie paragraaf 2.

³² Guidelines 07/2020 on the concepts of controller and processor in the GDPR (https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf)

Voeg tussen de lijnen aanvullende informatie toe over de betrokken partijen.

In het voorstel van wet is in Artikel 1 (begripsbepaling) het volgende opgenomen.

Artikel 1, eerste lid, bevat definities van begrippen die in het wetsvoorstel worden gebruikt.

Onder ambtenaar van politie moet ten eerste worden verstaan de *ambtenaar van politie*, bedoeld in artikel 2, onder a en c, van de Politiewet 2012, die is aangesteld voor de politietaak.

In het tweede lid is geregeld dat daaronder mede moet worden verstaan: *de militair van de Koninklijke marechaussee*, voor zover diegene binnen een gemeente optreedt ter handhaving van de openbare orde onder gezag van de burgemeester.

In artikel 11 en 14 van de Politiewet 2012 ligt besloten dat politie en Kmar de handhaving van de openbare orde uitvoeren onder gezag van de burgemeester. Dat geldt ook voor uitvoering van de bevoegdheden uit het wetsvoorstel gegevensvergaring openbare orde: de burgemeester waar de ernstige verstoring mogelijk en/of hoofdzakelijk plaatsvindt is het gezag.

Conclusie

Vastgesteld kan worden dat nu met het voorstel van wet een expliciet doel voor verwerking in de wet is opgenomen inclusief de rollen, het beschikbare instrumentarium voor de politie voor het uitvoeren van de taken onder het gezag van de burgemeester wordt aangevuld voor de online omgeving voor zover dat publiek toegankelijke bronnen betreft, de gegevensverwerkingen die hieruit voortvloeien als rechtmatig kunnen worden geduid.

7. Belangen bij de gegevensverwerkingen

Beschrijf alle belangen die de betrokken partijen hebben bij de gegevensverwerkingen. Vraag betrokkenen of hun vertegenwoordigers ook naar hun mening over de verwerking indien relevant. Licht deze mening toe onder het belang van de betrokkenen.

Toelichting

Bij de beoordeling van de rechtmatigheid van de gegevensverwerkingen kunnen de belangen die met de gegevensverwerkingen gemoeid zijn een rol spelen. Kortom, wat zijn de voornaamste belangen en redenen dat het voorstel is geïnitieerd?

Het kan hierbij zowel gaan om de private belangen van de verwerkings-verantwoordelijke, betrokkene en derden als het algemeen belang.

Denk hierbij bijvoorbeeld aan:

- Bedrijfsbelangen,
- Financiële en commerciële belangen,
- Het handhaven van juridische vorderingen,
- Toezicht op medewerkers ten behoeve van de veiligheid
- Managementdoeleinden, (nationale of openbare) veiligheid, zoals de preventie van fraude, misbruik en netwerkbeveiliging
- Gezondheidsredenen

Tabel 7.1.

Betrokken Partij	Belangen
Burgemeester	Handhaving van de openbare orde en veiligheid
Politie	

Betrokken Partij	Belangen
KMAR	Uitvoering geven aan de taak de openbare orde daadwerkelijk te handhaven en daarvoor de benodigde informatie te vergaren
Rechter Commissaris	Waarborgen zorgvuldig en gepast gebruik van de bevoegdheden (sturend)
Betrokkene	Veilige samenleving Bescherming van de privacy Recht op vrije meningsuiting, Recht van vergadering en betoging

Voeg tussen de lijnen aanvullende informatie toe over de belangen

Als gevolg van de digitalisering van de samenleving en de veelheid aan mogelijkheden die hieruit voortvloeien om online met elkaar te communiceren is het voor de politie het huidige instrumentarium voor het handhaven van de openbare orde ontoereikend. De reden hiervan is dat het in toenemende mate lastig geworden is om in publiek toegankelijke bronnen gegevens over een ernstige verstoring van de openbare orde te vergaren zonder daarmee persoonsgegevens over te nemen die met het oog op de handhaving van de openbare orde noodzakelijk zijn. In dat geval zou de politie immers een meer dan beperkte inbreuk maken op de persoonlijke levenssfeer en dat is niet toegestaan binnen het huidige wettelijke kader. Het gevolg hiervan is dat de politie en de burgemeester! niet adequaat de openbare orde kunnen handhaven. Op basis van het huidige instrumentarium is het slechts mogelijk uit publieke bronnen een gefragmenteerd of beperkt beeld te verkrijgen van de ontwikkeling van ernstige verstoringen van de openbare orde. De online wereld is steeds meer een belangrijke factor is bij het ontstaan of de (verdere) ontwikkeling van ernstige verstoringen van de openbare orde in de fysieke wereld. Het belang van de betrokken partijen (met uitzondering van de rechter-commissaris) zoals hierboven in de tabel uiteengezet is gebaat bij het verkrijgen van aanvullende bevoegdheden om een goed beeld te kunnen vormen of een online-gebeurtenis zich ontwikkelt tot een ernstige openbare ordeverstoring in het fysieke domein.

Conclusie

Vastgesteld kan worden dat nu met het voorstel van wet een expliciet doel voor verwerking in de wet is opgenomen inclusief de rollen, het belang ervan overtuigend is beargumenteerd, het beschikbare instrumentarium voor de politie voor het uitvoeren van de taken onder het gezag van de burgemeester wordt aangevuld voor de online omgeving in publiek toegankelijke bronnen, de gegevensverwerkingen die hieruit voortvloeien als rechtmatig kunnen worden geduid.

8. Verwerkingslocaties

Benoem in welke landen de gegevensverwerkingen plaatsvinden. Beschrijf het doorgiftemechanisme dat van toepassing is wanneer verwerkingslocaties buiten de Europese Economische Ruimte bevinden en noem of en welke aanvullende maatregelen van toepassing zijn. Voeg aanvullende informatie toe in het tekstveld.

Toelichting

De fysieke locaties waar de gegevensverwerkingen plaatsvinden, kunnen aanvullende risico's met zich brengen en daarom onderworpen zijn aan strengere regels en aanvullende maatregelen vereisen. Ook heeft de verwerkingslocatie invloed op de competentie van de (leidende) privacy toezichthouder.

Denk hierbij aan iedere locatie waar de desbetreffende verwerking van persoonsgegevens plaatsvindt; niet alleen de opslag van persoonsgegevens, maar bijvoorbeeld ook de locaties waar de gegevens worden geopend, gestreamd of tijdelijk worden opgeslagen.

Om te borgen dat de regels betreffende de bescherming van persoonsgegevens niet omzeild worden door persoonsgegevens in een ander land te verwerken, staat in de AVG dat gegevensverwerkingen buiten de Europese Economische Ruimte³³ enkel onder bepaalde omstandigheden zijn toegestaan. Dit is het geval wanneer gebruik wordt gemaakt van een daarvoor bestemd **doorgiftemechanisme**. Dit is bijvoorbeeld het geval indien het derde land naar het oordeel van de Europese Commissie een passend beschermingsniveau heeft (een adequaatheidsbesluit)³⁴ of indien gebruik wordt gemaakt van passende waarborgen om de betrokkenen te beschermen.

Passende waarborgen zijn modelcontractbepalingen (SCCs) en gedragscodes. Verder kan ook gebruik worden gemaakt van bindende bedrijfsvoorschriften (BCR's).

Indien het doorgiftemechanisme **niet gebaseerd is op een adequaatheidsbesluit** dient er een Data Transfer Impact Assessment (DTIA) uitgevoerd te worden om vast te stellen of de nationale wetgeving in het land waarnaar de persoonsgegevens worden gestuurd geen afbreuk doen aan het gekozen doorgiftemechanisme. Daarnaast zijn een aantal specifieke situaties waarin gegevensverwerkingen in een derde land toch toegestaan ondanks het ontbreken van een passend beschermingsniveau en passende waarborgen, zoals uitdrukkelijke toestemming van de betrokkene, noodzakelijk wegens gewichtige redenen van algemeen belang en noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Zie deel III van het Rijksmodel DPIA voor meer informatie over de doorgiftemechanismen.

Tabel 8.1

Gegevensverwerkingen	Verwerkingslocaties	Doorgiftemechanisme	Maatregelen
Volgen	Kortheidshalve wordt hier verwezen naar de tekst bij aanvullende informatie hieronder.		
Zoeken naar persoonsgegevens online			
Overnemen			
Verzamelen			
Analysen			
Verrijken			
Delen			
Opslaan			
Vernietigen			

Voeg hier tussen de lijnen aanvullende informatie over de verwerkingslocaties toe.

Zoals in de paragrafen 2 en 3 uiteengezet, wordt voor de verwerking van de gegevens welke plaatsvinden o.g.v. voorstel van wet *gebruik gemaakt van de bestaande systemen van de politie*.

Conclusie

Nu dat voor de verwerking van de gegevens welke plaatsvinden o.g.v. voorstel van wet gebruik

³³ De Europese Economische Ruimte bestaat uit alle landen die lid zijn van de Europese Unie plus de landen IJsland, Liechtenstein en Noorwegen.

³⁴ Artikel 45 AVG

gemaakt van de bestaande systemen van de politie is vooralsnog geen sprake van nieuwe privacyrisico's welke uit dit gebruik voortvloeien.

De privacyrisico's welke gerelateerd zijn aan gebruik van reeds ingebreektzjnde systemen is dan ook buiten scope van de DPIA.

Vanzelfsprekend worden, voor zover aan de orde, bij de implementatie van het voorstel door de betrokken partijen de locaties van de verwerkingen geïventariseerd en beoordeeld en zullen waarborgen met betrekking tot doorgifte naar landen buiten de EER worden georganiseerd conform het wettelijke kader (doorgiftemechanisme).

9. Juridisch en beleidsmatig kader

Benoem alle [wet- en regelgeving](#) en beleid met mogelijke gevolgen voor de gegevensverwerkingen. De AVG en de Richtlijn³⁵ hoeven niet genoemd te worden. Voeg aanvullende informatie toe in het tekstveld.

Toelichting

Voor het benoemen van de wet- en regelgeving en beleid die van toepassing zijn op het verwerkingsproces is het aan te raden om deze in hiërarchische wijze in een overzicht op te nemen.

Bijvoorbeeld:

Internationale verdragen;
Europese verdragen, verordeningen, richtlijnen en besluiten;
Nationale wetgeving;
AMvB's, gemeentelijke verordeningen, algemeen verbindende voorschriften; en
Intern beleid.

Naast de Wpg kan (sectorale) regelgeving de mogelijkheden voor gegevensverwerkingen creëren, conditioneren of beperken.

Hieronder is een lijst van voorbeelden van dergelijke wetten. Deze lijst is niet uitputtend.

Politiewet 2012

Wet algemene bepalingen burgerservicenummer,

Wet gebruik burgerservicenummer in de zorg,

Wet basisregistratie personen,

Algemene wet inzake rijksbelastingen,

Archiefwet,

Telecommunicatiewet,

Kadasterwet,

Handelsregisterwet 2007,

Kieswet,

Wet bijzondere maatregelen grootstedelijke problematiek,

Wet op de geneeskundige behandelingsovereenkomst, Omgevingswet,

Jeugdwet,

Wet maatschappelijke ondersteuning 2015, en

Participatiewet.

Er kan ook departementaal of Rijksbreed beleid zijn dat de mogelijkheden voor de gegevensverwerkingen conditioneert of beperkt. Bijvoorbeeld ten aanzien van de opslag en beveiliging van persoonsgegevens.

³⁵ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Aan de hand van deze inventarisatie kan bij onderdeel B beoordeeld worden of de gegevensverwerkingen rechtmatig zijn en bij onderdeel D of specifieke maatregelen voorgeschreven zijn.

Tabel 9.1.

Gegevensverwerkingen	Juridisch en/of beleidsmatig kader	Wetsartikelen
Volgen	Wetboek van Strafvordering, Europees Verdrag voor de Rechten van de Mens en fundamentele vrijheden, Handvest van de grondrechten van de Europese Unie, Grondwet	o.a. Art. 8 Recht op eerbiediging van privé-familie- en gezinsleven. 11 vergaderen/ vereniging (specifiek demonstratierecht) 18 Inperking van de toepassing van beperkingen op rechten (EVRM), Art. 8 (family life), 12 (vergaderen) 52 Handvest balanceren rechten (geen absolute rechten), Art 9 (vergaderen en betogen), 10 (familylife) en 22 (geen absolute rechten, inperking onder condities)
Zoeken naar persoonsgegevens online		
Overnemen		
Verzamelen		
Analyseren		
Verrijken		
Delen		
Opslaan		
Vernietigen		

Voeg hier tussen de lijnen aanvullende informatie toe over het juridische en beleidsmatig kader toe betreffende alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen.

Verhouding van het voorstel van wet met het wetboek van Strafvordering en wisselwerking tussen verschillende privacy verantwoordingsregiems

Bij ernstige openbare orde -verstoringen kan er een samenloop zijn tussen de handhaving van de openbare orde en de strafrechtelijke handhaving van de rechtsorde.

Bij ernstige verstoringen van de openbare orde komt het vaker voor dat er ook strafbare feiten, zoals vernielingen en geweldpleging, worden gepleegd.

Het kan daarom voorkomen dat zowel de burgemeester als de officier van justitie in dat geval aanleiding zien om bevoegdheden in te zetten. Dat betekent dat er twee afzonderlijke onderzoeken worden verricht waarbij de gegevensvergaring is gericht op twee verschillende doelen waarop twee verschillende privacy verantwoordingsregiems op van toepassing zijn. Voor de verwerking van persoonsgegevens binnen de context van opsporing en vervolging door de officier van justitie geldt de Wet justitiële en strafvorderlijke gegevens. Op de verwerking van de gegevens die politie vergaart in het kader van de openbare orde onder het bevoegde gezag van de burgemeester geldt de Wet politiegegevens. Dit voor zover deze van toepassing is verklaard op informatie die wordt vergaard met het inzetten de in het Wetsvoorstel opgenomen bevoegdheden.

De geïntroduceerde bevoegdheden in het voorstel van wet mogen uitsluitend worden ingezet om een ernstige verstoring te voorkomen, te beletten of te beëindigen.

Het is in die gevallen dan ook aan de officier van justitie om te bezien of hij zelf aanleiding ziet om bevoegdheden in te zetten op grond van het Wetboek van Strafvordering. Dit staat er overigens los van dat persoonsgegevens die eenmaal zijn vergaard met de uitoefening van de voorgestelde bevoegdheden vervolgens verder verwerkt kunnen worden voor een onderzoek naar de opsporing en vervolging van strafbare feiten.

Hogere regelgeving

Het wetsvoorstel regelt bevoegdheden waarmee persoonsgegevens worden vergaard en verwerkt om ernstige verstoringen van de openbare orde te voorkomen, te beletten of te beëindigen.

Het is daarom onvermijdelijk dat de uitoefening van deze bevoegdheden een beperking van het recht op *eerbiediging van de persoonlijke levenssfeer* met zich brengt.

Daarnaast kunnen met de uitoefening van de voorgestelde bevoegdheden ook andere grondrechten worden geraakt, meer in het bijzonder het recht op *vrijheid van meningsuiting* en het *recht op vergadering en betoging*. Deze drie grondrechten worden beschermd door de Grondwet, het Handvest van de grondrechten van de Europese Unie (hierna: het Handvest) en het Europees Verdrag voor de Rechten van de Mens (hierna: het EVRM), hoewel deze bescherming niet absoluut is. Beperkingen zijn toegestaan, mits deze voldoen aan bepaalde criteria.

Conclusie

Het voorstel van wet is tot stand gekomen met in achtneming van alle wet- en regelgeving en beleid met mogelijke gevolgen voor de gegevensverwerkingen.

10. Bewaartermijnen

Bepaal de [bewaartermijnen](#) van de persoonsgegevens aan de hand van de gegevensverwerkingen en de verwerkingsdoeleinden.

Motiveer waarom deze bewaartermijnen niet langer zijn dan strikt noodzakelijk ten opzichte van de verwerkingsdoeleinden³⁶. Beschrijf wie toeziet op de bewaartermijn en de mogelijke vernietiging of archivering aan het einde van de bewaartermijn.

Voeg aanvullende informatie toe in het tekstveld.

Toelichting.

Persoonsgegevens mogen niet langer worden bewaard dan voor de verwezenlijking van de verwerkingsdoeleinden noodzakelijk is³⁷. Met andere woorden: als het voor de verwezenlijking van de verwerkingsdoeleinden niet meer noodzakelijk is de persoonsgegevens te bewaren, moeten deze worden vernietigd of geanonimiseerd.

Op het beginsel van opslagbeperking maakt de privacyregelgeving een uitzondering als de persoonsgegevens uitsluitend worden verwerkt ten behoeve van archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden. Hieraan wordt wel de eis verbonden dat passende maatregelen worden getroffen om de betrokkenen te beschermen³⁸.

Archiefwet

Niet alle persoonsgegevens in alle documenten bij alle gegevensverwerkingen moeten echter worden vernietigd of geanonimiseerd. Een gedeelte moet worden gearhiveerd op basis van de Archiefwet. Het is van belang om bewaartermijnen in de zin van de Wpg op gescheiden wijze te benaderen ten opzichte van de Archiefwet. Een deel van de overheidsinformatie, bijvoorbeeld, gaat uiteindelijk naar het Nationaal Archief of naar een lokaal of regionaal archief. De reden hiervoor is dat deze informatie belangrijk is voor publieke verantwoording, rechtsvinding en vanuit cultuur-historisch oogpunt.

De algemene regels hierover zijn opgenomen in de Archiefwet en sommige regels zijn verder uitgewerkt in het Archiefbesluit en de Archiefregeling.

³⁷ Artikel 4, eerste lid, onder e, Richtlijn.

³⁸ Artikel 4, derde lid, Richtlijn.

Relatie bewaartermijn en archivering

De bewaartermijn in de zin van de Wpg gaat specifiek over het bewaren van persoonsgegevens. Een document waarin geen persoonsgegevens zijn verwerkt of waar de persoonsgegevens geanonimiseerd zijn valt dus niet onder het bewaartermijnregime uit de Wpg.

Wanneer documenten wel persoonsgegevens bevatten, dan dient wel een bewaartermijn te worden bepaald voor die persoonsgegevens. Die bewaartermijn is, onder meer, bepaald aan de hand van het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld en verwerkt. Wanneer de bewaartermijn is afgelopen, dan betekent het dat de bewaartermijn op basis van het oorspronkelijke doeleinde is afgelopen. Als de Archiefwet of een andere archiveringsregeling van toepassing is en de gegevens gearchiveerd moeten worden, *dan is archivering het nieuwe doeleinde waarvoor de persoonsgegevens worden verwerkt*³⁹.

Beschrijven bewaartermijn

De *bewaartermijn die wordt vastgesteld* refereert aan specifieke persoonsgegevens voor een specifieke gegevensverwerking. Bijvoorbeeld, het bewaren van een naam, adres en telefoonnummer in het kader van de sollicitatieprocedure heeft een bewaartermijn van maximaal vier weken na beëindiging van de sollicitatieprocedure. Het bewaren van een naam, adres en telefoonnummer in het kader van de arbeidsovereenkomst heeft een bewaartermijn van maximaal twee jaar na beëindiging arbeidsovereenkomst.

Verder moet worden vastgesteld wat na de bewaartermijn moet gebeuren. Na de bewaartermijn kunnen twee handelingen plaatsvinden, namelijk de vernietiging/anonimisering of archivering van de persoonsgegevens om vervolgens de persoonsgegevens te vernietigen/te anonimiseren. Daarom is het ook belangrijk om te controleren of de Archiefwet, het Archiefbesluit en/of de Archiefregeling van toepassing is op de persoonsgegevens die worden verwerkt bij desbetreffende gegevensverwerking.

Stel de bewaartermijn vast door onder meer de volgende punten na te lopen:

- Ga na of een bestaande wettelijke of beleidsmatige bewaartermijn geldt voor desbetreffende gegevensverwerking.
- Wanneer het noodzakelijk is om persoonsgegevens te bewaren, bepaal concreet wat de duur is van de bewaartermijn, vanaf wanneer de bewaartermijn start, welke handelingen na de bewaartermijn moeten plaatsvinden en wie daarvoor verantwoordelijk is.

Bij conceptregelgeving zal moeten worden bepaald en gemotiveerd of het al dan niet wenselijk is om een specifieke minimale of maximale bewaartermijn voor te schrijven. Aan de hand van het uitgangspunt dat de bewaartermijn noodzakelijk moet zijn voor de verwerkingsdoeleinden, moet de gekozen termijn worden gemotiveerd. Motiveer ook het niet opnemen van een bewaartermijn.

Voeg aanvullende informatie toe in het tekstveld.

Gegevens-verwerking	Verwerkings-doeleinde	Categorie Persoons-gegevens	Bewaartermijn	Motivatie bewaartermijn
Volgen	Voorkomen, beletten of beëindigen ernstige verstoring van de openbare orde (zie paragraaf 5)	Gewoon, bijzonder, gevoelig (zie paragraaf 2)	Zolang deze noodzakelijk zijn voor het onderzoek naar de ernstige verstoring van de openbare orde of gedurende een	Deze laatste termijn van een half jaar is noodzakelijk, onder meer omdat het vaker voorkomt dat ernstige verstoringen van de
Zoeken naar persoonsgegevens online				
Overnemen				
Verzamelen				
Analyseren				

³⁹In "Generieke selectielijst voor de informatie van de politie. Vanaf 1 januari 2013", januari 2020 is beschreven op welke wijze invulling wordt gegeven aan de verplichtingen o.g.v. de Archiefwet.

Gegevens-verwerking	Verwerkings-doeleinde	Categorie Persoons-gegevens	Bewaartermijn	Motivatie bewaartermijn
Verrijken			periode van een half jaar	openbare orde strafbare feiten omvatten. Op deze wijze kan in een later stadium worden gezien of een onderzoek moet worden opgestart naar deze strafbare feiten. Na afloop van beide termijnen moeten de vergaarde persoonsgegevens worden vernietigd.
Delen				
Opslaan				
Vernietigen				

Voeg hier tussen de lijnen aanvullende informatie over de bewaartermijnen toe.

Privacy beginselen

Uit het evenredigheidsbeginsel vloeit voort dat een nationale wettelijke regeling duidelijke en nauwkeurige regels moet stellen voor de draagwijdte en toepassing ervan en ervoor zorgen dat de verwerking van gegevens voor het beletten, voorkomen en beëindigen van ernstige verstoringen beperkt wordt tot wat (strikt) noodzakelijk is⁴⁰.

Het EHRM wijst op het bijzondere belang van deze privacy beginselen en de wettelijke waarborgen daartoe als persoonsgegevens automatisch worden verwerkt en gebruikt door de politie ten behoeve van de uitoefening van de politietak⁴¹.

Hanteren van bewaartermijnen (specifieke persoonsgegevens voor een specifieke gegevensverwerking)

In het onderhavige voorstel van wet is geborgd dat zodra blijkt dat persoonsgegevens zijn vergaard die van geen betekenis zijn voor het onderzoek naar de ernstige verstoring, zoals van personen die niets met de ernstige verstoring te maken hebben, deze gegevens moeten worden vernietigd. Dit geldt ook in het geval de ernstige verstoring van de openbare orde niet plaatsvindt en ook niet aannemelijk is dat deze gaat plaatsvinden.

Passende bewaartermijnen

In het voorstel van wet is de naleving van de bewaartermijnen van de te verwerken persoonsgegevens met procedurele waarborgen omkleed.

In afwijking van artikel 9, vierde lid, van de Wet politiegegevens zijn concrete en passende bewaartermijnen opgenomen. De persoonsgegevens die met de uitoefening van de bevoegdheden worden vergaard, mogen slechts worden verwerkt voor *zolang deze noodzakelijk zijn voor het onderzoek naar de ernstige verstoring van de openbare orde of gedurende een periode van een half jaar* om te bezien of de gegevens aanleiding geven tot een nieuw onderzoek of een nieuwe verwerking.

Deze laatste termijn van een half jaar is noodzakelijk, onder meer omdat het vaker voorkomt dat ernstige verstoringen van de openbare orde strafbare feiten omvatten. Op deze wijze kan in een

⁴⁰ Uitspraak van het Hof van Justitie van 4 oktober 2024, ECLI:EU:C:2024:830 (C.G./Bezirkshauptmannschaft Landeck).

⁴¹ J.M. ten Voorde, EHRC 2015/25, EHRM, 18-09-2014, 21010/10 (annotatie).

later stadium worden gezien of een onderzoek moet worden opgestart naar deze strafbare feiten. *Na afloop van beide termijnen* moeten de vergaarde persoonsgegevens worden vernietigd.

Conclusie

Het is, zoals hierboven gemotiveerd uiteengezet, noodzakelijk om een specifieke bewaartermijn voor te schrijven voor de te verwerken gegevens gericht op het beletten, voorkomen of beëindigen van een ernstige verstoring van de openbare orde.

CONCEPT

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de gegevensverwerkingen en rechten van de betrokkene.

CONCEPT

11. Rechtsgrond

Voor het verwerken van persoonsgegevens is een grondslag nog welke is beschreven in een wet.

Toelichting

De rechtsgrond voor de verwerking van gegevens o.g.v. de Wpg dient bij wet geregeld te zijn. Voor de politie is dat de Politiewet 2012.

Beoordeel of de verwerking is toegestaan.

Tabel 12.1

Gegevensverwerking	Rechtsgrond	Toelichting op de rechtsgrond
Volgen	De rechtsgrond voor de onderhavige verwerkingen is gecreëerd met het voorstel van wet.	Zie paragraaf 1 Voorstel
Zoeken naar persoonsgegevens online		
Overnemen		
Verzamelen		
Analyseren		
Verrijken		
Delen		
Opslaan		
Vernietigen		

Voeg hier tussen de lijnen aanvullende informatie over de rechtsgronden toe.

Met het online vergaren van persoonsgegevens over een ernstige verstoring van de openbare orde wordt al snel een meer dan geringe inbreuk gemaakt op de persoonlijke levenssfeer van de betrokkenen.

Het is voorzienbaar en aannemelijk dat met de vergaarde informatie een min of meer volledig beeld kan worden verkregen van bepaalde aspecten van het persoonlijke leven van de betrokkenen.

Gelet hierop is een uitdrukkelijke wettelijke grondslag nodig. Het wetsvoorstel voorziet daarin door twee bevoegdheden voor de politie onder het gezag van de burgemeester te regelen op grond waarvan persoonsgegevens uit publiek toegankelijke bronnen rechtmatig kunnen worden vergaard.

Conclusie

De wettelijke grondslag voor de verwerking van persoonsgegevens uit publiek toegankelijke bronnen voor het beletten, voorkomen of beëindigen van ernstige verstoringen orde is in het voorstel van wet belegd. Bij het formuleren van dit voorstel zijn de privacy beginselen in acht genomen. De verwerkingen van persoonsgegevens zijn als gevolg daarvan met passende waarborgen omkleed. Vastgesteld kan worden dat de verwerking van de bijzondere categorie van persoonsgegevens zoals uiteengezet in deze paragraaf is toegestaan.

12. Bijzondere persoonsgegevens

Het verwerken van [bijzondere](#) of [strafrechtelijke](#) persoonsgegevens is in principe verboden.

Toelichting

Verwerking is pas mogelijk wanneer een [uitzonderingsgrond](#) van toepassing is. Beoordeel of een van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een nationaal identificatienummer, beoordeel of dit is toegestaan.

Voeg aanvullende informatie toe in het tekstveld.

Tabel 12.1

Gegevensverwerking	Type bijzonder persoonsgegevens	Uitzonderingsgrond
Volgen	Bijzonder	De uitzonderingsgrond is opgenomen in het voorstel van wet.
Zoeken naar persoonsgegevens online		
Overnemen		
Verzamelen		
Analyseren		
Verrijken		
Delen		
Opslaan		
Vernietigen		

Voeg hier tussen de lijnen aanvullende informatie over de bijzondere persoonsgegevens toe.

Gegevens in publiek toegankelijke bronnen die betrekking hebben op (gedrag gekoppeld aan) verstoringen van de openbare orde zijn altijd te relateren aan een of meer personen. Daaronder kunnen ook bijzondere persoonsgegevens bedoeld in artikel 10 van EU-richtlijn 2016/680 vallen, zoals informatie over seksueel geaardheid, ras of etnische afkomst, gezondheid, politieke opvattingen en godsdienstige of levensbeschouwelijke overtuigingen.

Dat geldt nog meer indien de (dreigende) ernstige verstoring van de openbare orde een achtergrond heeft in bijvoorbeeld een ideologische overtuiging van betrokkenen. Op grond van artikel 5 van de Wet politiegegevens mag de verwerking van dergelijke gegevens overigens alleen plaatsvinden indien dit onvermijdelijk is voor het doel van de verwerking en in aanvulling op de verwerking van andere politiegegevens betreffende de persoon en de gegevens daarnaast afdoende zijn beveiligd. Voor bijzondere persoonsgegevens geldt dat deze extra moeten worden beschermd, waarbij verwerkingen binnen de grenzen van het strikt noodzakelijke moeten blijven⁴². Bij het formuleren van het voorstel van wet zijn de waarborgen hiertoe opgenomen en als volgt samen te vatten. Borgen van:

Legitiem doel van algemeen belang vereiste (rechtmatig, behoorlijkheid en transparantie)
Noodzakelijkheidsvereiste (evenredigheid en subsidiariteit);
Dataminimalisatie;
Doelbinding;
Juistheid;
Opslagbeperking;
Integriteit en vertrouwelijkheid

⁴² 34 Artikel 10 van de richtlijn.

Conclusie

Bij het formuleren van het voorstel van wet met betrekking tot het verwerken van bijzondere persoonsgegevens is een wettelijke basis gecreëerd om van het verbod onder bij wet bepaalde condities af te wijken. Deze condities zijn gebaseerd op de beginselen zoals die zijn opgenomen in het EVRM, Europees Handvest en de grondwet. De verwerkingen van de gegevens binnen de context van het voorstel van wet zijn daarmee te duiden als rechtmatig.

13. Doelbinding

Als de persoonsgegevens voor een ander doeleinde worden verwerkt dan het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, beoordeel of deze (nieuwe) verdere verwerking toelaatbaar is o.g.v. de bepalingen uit de Wpg.

Voeg in het tekstveld de toets toe gebaseerd op de bepalingen uit de Wpg die betrekking hebben op het verwerken van gegevens voor een ander doel en voeg aanvullende informatie toe.

Toelichting

De Wpg⁴³ regelt dat Politiegegevens die zijn verkregen voor een doel, als bedoeld in artikel 1, onder a, kunnen worden verwerkt voor een ander doel, voor zover deze wet of Unierecht uitdrukkelijk daarin voorziet en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel.

Politiegegevens kunnen voor een ander doel dan die, bedoeld in artikel 1, onderdeel a, worden verwerkt door personen en instanties die bij of krachtens de wet met het oog op een zwaarwegend algemeen belang of wetgeving van de Europese Unie zijn aangewezen⁴⁴.

Bij conceptregelgeving moet worden beoordeeld of het noodzakelijk is om wettelijk te regelen dat verwerking voor een ander doel toegestaan is (zie ook paragraaf 14 hierna)

Gegevensverwerking	Persoonsgegevens	Doeleinde	Oorspronkelijk doeleinde
Volgen	Zie uitwerking bij paragraaf 2.		Beletten, voorkomen of beëindigen van een ernstige openbare orde verstoring.
Zoeken naar persoonsgegevens online			
Overnemen			
Verzamelen			
Analyseren			
Verrijken			
Delen			
Opslaan			
Vernietigen			

Voeg hier tussen de lijnen aanvullende informatie over de doelbinding toe.

⁴³ Artikel 3 lid 3 en 4 Wpg

⁴⁴ politiegegevens: elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de **artikelen 3 en 4 van de Politiewet 2012**, met uitzondering van: de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften; de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1° en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012;

Beoordeling noodzaak regelen bij wet verdere verwerking

Voor de verwerking van de gegevens die voortvloeien uit de inzet van de geïntroduceerde bevoegdheden in dit Wetsvoorstel is aansluiting gezocht bij de bepalingen uit de Wpg.

Bij de wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen *is met betrekking tot het bepalen van de noodzakelijkheid* van het regelen bij wet van dat een verwerking voor een ander doel bepaald dat de noodzaak hiertoe bestaat gezien de “kaders van proportionaliteit”⁴⁵.

Zoals uiteengezet in paragraaf 14 is de oorspronkelijke verwerking van de persoonsgegevens in het onderhavige wetsvoorstel met waarborgen omkleed gezien de inbreuk op de rechten van de betrokkenen. Het is dan ook in het belang van de betrokkenen om voor de verdere verwerking heldere wettelijke kaders te formuleren. Het onderhavige wetsvoorstel voorziet hierin.

Conclusie

Geconcludeerd kan worden dat er sprake is van noodzakelijkheid tot het regelen van de verdere verwerking van de persoonsgegevens die aan de orde zijn bij de inzet van de geïntroduceerde bevoegdheden. Het Wetsvoorstel voorziet hierin met het van toepassing verklaren van Artikel 9 Wpg lid 3.

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk en evenredig zijn voor het verwezenlijken van de verwerkingsdoeleinden.

Ga hierbij in ieder geval in op:

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

Toelichting

De privacyregelgeving geeft als beginsel dat de gegevensverwerking wordt beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden.

Dit beginsel van minimale gegevensverwerking/dataminimalisatie komt verder tot uitdrukking door het gebruik van het woord ‘noodzakelijk’ in artikel 6 AVG en artikel 8 Richtlijn. De AVG en Richtlijn eisen hiermee dat de gegevensverwerking noodzakelijk is voor het verwezenlijken van de doeleinden. De gegevensverwerking moet daarbij voorts de toets aan de beginselen van proportionaliteit en subsidiariteit kunnen doorstaan.

⁴⁵ Wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, Vergaderjaar 2017–2018, 34 889, Nr. 3 MEMORIE VAN TOELICHTING, blz. 62.

Proportionaliteit

Proportionaliteit betekent dat moet worden beoordeeld of de indringendheid van de gegevensverwerking in een redelijke verhouding staat tot het doel. Bij proportionaliteit wordt gewogen of de realisatie van de verwerkingsdoeleinden zodanig gewicht heeft dat de gegevensverwerkingen, gelet op de mate waarin deze de privacy beperken, deze rechtvaardigen (zijn de beperkingen van het grondrecht en het doel dat met de verwerking wordt beoogd met elkaar in balans?).

Daarbij zal onder meer moeten worden gekeken of de gegevensverwerking effectief is om het beoogde doel te bereiken en of de aangevoerde redenen relevant en toereikend zijn om het beoogde doel te bereiken.

Daarbij kunnen empirische onderzoeksresultaten helpen.

Ter beoordeling van de proportionaliteit kunnen de volgende vragen worden gesteld:

Staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?

Is de gegevensverwerking van persoonsgegevens *te verwachten en voorzienbaar* voor de betrokkenen?

Hoe *groot is het belang om de verwerkingsdoeleinden te bewerkstelligen?*

Is de gegevensverwerking het *meest effectieve middel om het doeleinde* te bereiken?

Subsidiariteit

Bij subsidiariteit wordt bekeken of de verwerkingsdoeleinden *met minder ingrijpende middelen kunnen worden bereikt* (bijvoorbeeld: kan bij het gebruik van bijzondere of strafrechtelijke persoonsgegevens hetzelfde resultaat behaald worden met gebruikmaking van een combinatie van gewone persoonsgegevens?).

Bij deze afwegingen worden de doelen, belangen en feiten zoals in beeld gebracht in onderdeel A betrokken.

Ter beoordeling van de subsidiariteit kunnen de volgende vragen worden gesteld:

1. Kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?
 - i. Kunnen *minder persoonsgegevens* worden verwerkt en hetzelfde doeleinde worden bereikt?
 - ii. Zijn er wellicht manieren om *minder gevoelige persoonsgegevens* te verwerken?
 - iii. Kunnen de persoonsgegevens in het *proces gepseudonimiseerd of geanonimiseerd* worden?
 - iv. Kunnen de *persoonsgegevens met minder partijen worden gedeeld of minder lang worden bewaard*?
2. Zijn er alternatieve minder privacy invasieve verwerkingsprocessen onderzocht en gedocumenteerd?
 - v. Welke *alternatieven zijn overwogen* en *waarom zijn deze alternatieven niet gekozen*?
 - vi. Zijn alternatieven overwogen die hetzelfde doeleinde kunnen bereiken *met minder persoonsgegevens*?
 - vii. Zijn alternatieven overwogen waarbij de gehele dienst binnen Nederland of de EU uitgevoerd kan worden?
 - viii. Zijn alternatieven overwogen waarbij de verwerker geen gebruikmaakt van sub-verwerkers buiten de EU?

Bij conceptregelgeving kunnen de uitkomsten van deze afweging worden meegenomen in de grondrechtentoets van de beleidsmonitor.

Voeg hier tussen de lijnen de beoordeling van de proportionaliteit toe.

Bij het formuleren van het onderhavige Wetsvoorstel is beoordeeld of de indringendheid van de gegevensverwerking die aan de orde is bij het toepassen van de bevoegdheden die worden geïntroduceerd in redelijke verhouding staat tot het doel. Hierbij is gewogen of de realisatie van de verwerkingsdoeleinden, het voorkomen, beletten of beëindigen van een ernstige verstoring van de openbare orde, zodanig gewicht heeft, dat het de mate van de inbreuk op de rechten van de betrokkene, rechtvaardigt.

De gegevensverwerkingen op basis van de geïntroduceerde bevoegdheden kan dan ook slechts plaats vinden indien aan de gegevensverwerking op basis van de bevoegdheden uit Artikel 3 van de Politiewet 2012 niet toereikend is om een ernstige verstoring van de openbare orde te voorkomen, beletten of te beëindigen.

Op basis van uitgebreid onderzoek naar de mogelijkheden van het voorkomen, beletten of beëindigen van ernstige verstoringen van de openbare orde met het huidige instrumentarium is geconcludeerd dat er geen andere mogelijkheden zijn anders dan het creëren van de huidige bevoegdheden. Op deze wijze wordt het huidige instrumentarium aangevuld en voldoet het aan de eisen van een digitale samenleving. Voor betrokkenen in een digitale samenleving is het van belang dat voorzienbaar is dat politie informatie vergaart over online activiteiten die leiden tot ernstige verstoringen van de openbare orde.

Conclusie

Aan de proportionaliteitseis is in het Wetsvoorstel gedegen aandacht besteed in vorm van het formuleren van passende waarborgen voor de privacy van betrokkenen. Op basis daarvan kan gesteld worden dat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding staat tot de verwerkingsdoeleinden ten behoeve van een veilige samenleving.

Voeg hier tussen de lijnen de beoordeling van de subsidiariteit toe.

Bij het formuleren van het Wetsvoorstel is zijn alle relevante aspecten met het oog op het subsidiariteitsbeginsel afgewogen.

De verwerkingsdoeleinden kunnen in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt.

In 2021 en 2022 heeft het Landelijk Overleg Veiligheid en Politie (het overleg tussen de burgemeesters, OM, de Politie en het ministerie van JenV) de opdracht gegeven om te onderzoeken of het Team Openbare Orde Inlichtingen (TOOI) in het licht van de veranderde maatschappij, de taak rond het handhaven van de openbare orde nog goed kan uitvoeren of dat hiervoor mogelijk een aanpassing in bevoegdheden nodig is.

Daarnaast bracht de Commissie modernisering opsporingsonderzoek in het digitale tijdperk (hierna: de Commissie Koops) naar voren dat het overnemen van persoonsgegevens uit publiek toegankelijke bronnen niet alleen relevant is in het kader van een onderzoek naar de opsporing en vervolging van strafbare feiten, maar ook voor andere politietaken. De Commissie Koops adviseerde daarom de wetgever in 2018 om dit ook mogelijk te maken voor onder meer de handhaving van de openbare orde.

Op 30 juni 2022 vond in de Tweede Kamer het debat over de maatschappelijke onrust rondom de stikstofcrisis plaats waarin uit de hand gelopen acties en demonstraties tegen het stikstofbeleid aan de orde kwamen.

De Tweede Kamer heeft toen met de motie Klaver het kabinet verzocht om alle instrumenten aan de politie beschikbaar te stellen om adequaat in te grijpen en de openbare orde te handhaven bij geweld, bedreiging en intimidatie. In de Kamerbrief van 23 december 2022 alsmede de Halfjaarberichten politie van 2023 en 2024, is vervolgens het beleidstraject rond de bevoegdheden van de politie voor het vergaren van informatie ten behoeve van de openbare orde en de voortgang van de verkenning naar de mogelijkheid dat de politie persoonsgegevens overneemt uit publiek toegankelijke bronnen toegelicht. Met de motie Michon-Derkzen heeft de Tweede Kamer gevraagd om versnelling van het vernieuwd handelingskader voor online gegevensverwerking. Hierop heeft de toenmalige Minister van Justitie en Veiligheid in het eerste Halfjaarbericht politie 2024 laten weten dat het beleidstraject slechts ten dele kon worden versneld, omdat voor nieuwe bevoegdheden een wetswijziging noodzakelijk was.

In vervolg hierop heeft het kabinet Schoof 2024-2025 in het Regeerprogramma aangekondigd dat de bevoegdheden van de politie om informatie te vergaren over (potentieel) grootschalige openbare ordeverstoringen worden uitgebreid.

Naar aanleiding van de recente geweldsincidenten in Amsterdam (die plaatsvonden nadat daartoe werd opgeroepen p verschillende sociale media-kanalen zoals Telegram) tegen de supporters van de Israëliische club Maccabi Tel Aviv en andere burgers met een (vermeend) Joodse achtergrond in de nacht van 7 op 8 november 2024, heeft onder meer de Minister van Justitie en Veiligheid in de Kamerbrief 'Strategie Bestrijding Antisemitisme 2024-2030' van 22 november 2024 te kennen gegeven dat een wetsvoorstel wordt voorbereid om de informatiepositie van de politie op het terrein van de openbare orde te moderniseren.

De minder privacy invasieve vergaringsmogelijkheden bieden geen soelaas voor het voorkomen, beletten of beëindigen van ernstige verstoringen van de openbare orde. Bij het vergaren van gegevens op artikel 3 politiewet moet al in een vroeg stadium worden gestopt met het vergaren van informatie omdat het risico op het maken van een meer dan beperkte inbreuk op grondrechten te groot wordt. De benodigde informatie om een ernstige openbare ordeverstoring te voorkomen, beletten of beëindigen kan dan niet worden vergaard.

Op basis van de verschillende opdrachten is binnen de politie een brede verkenning uitgevoerd naar de noodzaak voor aanvullende bevoegdheden voor informatievergaring ten behoeve van handhaving van de openbare orde.

Dit heeft geleid tot een selectie aan bevoegdheden die de informatiepositie van de politie kunnen verbeteren. In het Wetsvoorstel komen de eerste, noodzakelijk geachte, nieuwe bevoegdheden aan de orde die zien op informatievergaring in publiek toegankelijke online bronnen.

Conclusie

Zoals uiteengezet in deze subparagraaf is het Wetsvoorstel gebaseerd op een grondige en zorgvuldige analyse waarin het subsidiariteitsbeginsel uitgebreid is toegepast.

15. Rechten van betrokkenen

Beschrijf de procedure waarmee invulling wordt gegeven aan de rechten van de betrokkenen Als de rechten van de betrokkene worden beperkt, beschrijf op grond van welke wettelijke uitzondering dat is toegestaan.

Toelichting

Een van de belangrijkste aspecten uit de Wpg, zoals uiteengezet in Paragraaf 4 is dat betrokkenen een aantal rechten hebben als het gaat om de verwerking van hun persoonsgegevens. Met deze rechten kunnen betrokkenen namelijk controle houden over de verwerking van hun persoonsgegevens. Het is daarom van groot belang om bij de gegevensverwerkingen vast te stellen hoe gehoor gegeven wordt aan de privacyrechten.

Betrokkenen hebben op grond van de privacyregelgeving diverse rechten, waarin ook staat op welke wijze en onder welke omstandigheden zij die rechten kunnen uitoefenen⁴⁶.

Er zijn uitzonderingen mogelijk op de uitoefening van deze rechten, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang⁴⁷.

Geef bij de beschrijving duidelijk aan wat de procedure is voor betrokkenen om hun rechten uit te oefenen wat betreft de gegevensverwerkingen. Ga hierbij in op hoe deze procedure binnen de desbetreffende organisatie is ingebed en welke rollen verantwoordelijk zijn binnen de verschillende stappen van de procedure.

Rechten van betrokkene	Procedure ter uitvoering	Beperking op grond van wettelijke uitzondering
Recht op inzage	De procedure voor uitvoering komt aan de orde bij de implementatie van de wet door de politie.	
Recht op duidelijke informatie		
Recht op rectificatie en vernietiging		

Geef een beschrijving hier tussen de lijnen.

Op het Wetsvoorstel zijn bepaalde bepalingen uit de Wet Politiegegevens van toepassing, waaronder die over de rechten van betrokkenen gaan.

⁴⁶ Hoofdstuk III (artikelen 12-18) Richtlijn.

⁴⁷ 15 en 16, vierde lid, Richtlijn

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

CONCEPT

16. Risico's voor betrokkenen

Beschrijf en beoordeel de risico's van de gegevensverwerkingen voor de rechten en vrijheden van betrokkenen. Ga hierbij in ieder geval in op:

- welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie;
- de oorsprong van deze gevolgen;
- de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
- de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

Toelichting

Een DPIA o.g.v. de Wpg betreft een beoordeling van risico's voor de rechten en vrijheden van de betrokkenen welke aan de orde zijn op basis van het voorstel zoals uiteengezet in paragraaf 1.

Aan de hand van de aard, het toepassingsgebied, de context en de doeleinden van de gegevensverwerking dient de waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkenen te worden bepaald. Op basis van een objectieve beoordeling kan vastgesteld worden of de gegevensverwerking gepaard gaat met een (hoog) risico.

Hiervoor is het nodig om de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.

Het gaat hier om een risicogerichte benadering die kan bestaan uit de volgende stappen:

1. Risico's identificeren;
2. Risico's inschatten/analyseren;
3. Risico's beoordelen/evalueren.

Deze benadering zal in grote lijnen vergelijkbaar zijn met een risicoafweging in het kader van informatiebeveiliging bij toepassing van informatiebeveiligings-standaarden.

Risico's identificeren

De eerste stap is om potentiële risico's vast te stellen. Een risico is de situatie waarin persoonsgegevens worden verwerkt die direct of indirect (kunnen) leiden tot schadelijke gevolgen voor de rechten en vrijheden van de betrokkenen. Deze risico's zijn gebaseerd op de situatie zoals die op het moment van het schrijven van de DPIA geldt, inclusief de bestaande maatregelen die op dat moment van toepassing zijn op desbetreffende risico's.

In paragraaf 16 worden de maatregelen geïdentificeerd die aanvullend genomen worden om de geïdentificeerde risico's voortvloeiend uit de gegevensverwerkingen o.g.v. het voorstel van wet te mitigeren. Bij rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod van discriminatie.

Het voordoen van de (hypothetische) situatie kan leiden tot lichamelijke, materiële of immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de volgende situaties waar de gegevensverwerking kan leiden tot:

- Discriminatie, stigmatisering en uitsluiting;
- (Blootstelling aan) identiteitsdiefstal of -fraude;
- Financiële verliezen;
- Reputatie- of anderszins relationale schade;
- Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
- Ongeoorloofde ongedaan making van pseudonimisering;
- Of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de natuurlijke persoon in kwestie;

- Wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd om controle over hun persoonsgegevens uit te oefenen;
- Wanneer bijzondere of strafrechtelijke persoonsgegevens worden verwerkt;
- Wanneer persoonlijke aspecten worden geëvalueerd, om bijvoorbeeld beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;
- Wanneer persoonsgegevens van kwetsbare personen, zoals kinderen, worden verwerkt; of
- Wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen .

Bij (onrechtmatige) verwerkingen van persoonsgegevens kan gedacht worden aan het al dan niet opzettelijke:

- Vernietiging en verlies (beschikbaarheid);
 - Wijziging (integriteit);
 - Ongeoorloofde toegang en verstrekking (vertrouwelijkheid);
- van persoonsgegevens, of anderszins handelen in strijd met het recht .

Discriminatie

Indien sprake is van discriminatie, dan wordt er in strijd met het recht gehandeld. Discriminatie is het ongerechtvaardigd onderscheid maken tussen gelijke gevallen, dat is verboden op grond van artikel 1 van de Nederlandse Grondwet. Het recht gaat niet alleen uit van een beperkt aantal gronden waarop in principe geen besluiten mogen worden genomen (zoals godsdienst, levensovertuiging, ras of geslacht) maar verbiedt ook discriminatie 'op welke grond ook'. Niet alleen directe discriminatie is verboden, maar ook indirecte discriminatie. Dat betekent overigens niet dat het maken van onderscheid altijd verboden is. Zo is wel wettelijk toegestaan om onderscheid te maken op basis van leeftijd bij arbeid (denk aan het beëindigen van de arbeidsverhouding bij het bereiken van de AOW-gerechtigde leeftijd).

Directe discriminatie

Van directe discriminatie is sprake als een persoon op een andere wijze wordt behandeld dan een ander in een vergelijkbare situatie.

Indirecte discriminatie

Van indirecte discriminatie is sprake als een ogenschijnlijk neutrale bepaling, maatstaf of handelwijze een groep personen in vergelijking met andere groepen personen bijzonder treft. Een voorbeeld daarvan is een beveiligingssysteem op basis van gezichtsherkenning waarbij strenge kledingvoorschriften worden gesteld met als doel het hoofd en gezicht vrij te houden zodat het systeem het gezicht goed kan analyseren. Personen met hoofd- of gezichtsbedekking vanwege religieuze redenen worden door zulke voorschriften in het bijzonder getroffen.

Als er mogelijk sprake is van directe of indirecte discriminatie als gevolg van de verwerking van persoonsgegevens waar de DPIA op ziet, dan is het noodzakelijk om een anti-discriminatietoets uit te voeren, waarin uiteen wordt gezet 1) of er sprake is van onderscheid en op basis waarvan 2) waarom (voor welk doel) er onderscheid gemaakt wordt of gaat worden 3) of er sprake is van direct of indirect onderscheid 4) of deze vorm van onderscheid bij wet is toegestaan 5) welke maatregelen er genomen worden om discriminatie te voorkomen of de gevolgen daarvan te mitigeren .

Big Data

Big dataverwerkingen kunnen specifieke risico's voor de betrokkene met zich brengen. Zo kan een algoritme een correlatie ontdekken die weliswaar in statistische zin logisch is, maar die kan leiden tot vooroordelen en stereotypering, discriminatie en sociale uitsluiting of anderszins impact heeft op de betrokkenen, bijvoorbeeld bij sollicitaties, het aangaan van leningen en afsluiten van verzekeringen. Ook bestaat het risico dat de betrokkene onderworpen is aan big data-besluitvorming die hij niet begrijpt en waar hij geen invloed op heeft.

Risico's inschatten

Vervolgens moeten de benoemde risico's worden gekwalificeerd door het inschatten van de kans dat een dreiging zich voordoet en de mogelijke gevolgen daarvan voor de betrokkenen. Met andere woorden: wat zijn de gevreesde gevolgen en hoe groot is de impact daarvan op de betrokkenen? En hoe treden deze in werking en hoe waarschijnlijk is dat? Deze vragen zijn niet gericht op zwart-wit-antwoorden maar op een afweging.

Aan de hand hiervan moet een risiconiveau worden bepaald. De impact/ernst van de risico's hangt af van de context van de verwerkingen: de aard van de persoonsgegevens, de aard van de verwerkingen en de doeleinden waarvoor de gegevens worden verwerkt.

De kans dat de risico's zich voltrekken is mede afhankelijk van de middelen die de verwerkingsverantwoordelijke gebruikt bij de gegevensverwerking en de aard van de persoonsgegevens.

Persoonsgegevens die bijvoorbeeld de sleutel vormen voor toegang tot geldelijke middelen of waarmee de betrokkene reputatieschade kan oplopen, brengen risico's met zich mee. Denk hierbij aan informatie over de psychologische of medische situatie van betrokkene. Het inschatten van de ernst van het risico kan worden gedaan aan de hand van de kans en de impact dat het risico heeft.

Geef zowel de kans dat het risico plaatsvindt als de impact dat het risico heeft een classificatie: laag, gemiddeld of hoog. Vervolgens is de classificatie voor het risico op zichzelf gebaseerd op de formule kans x impact. Door deze berekening te doen aan de hand van de tabel in het rapportagemodel wordt de totale ernst van het risico ingeschat.

Gebruik voor de inschatting van de kans, impact en het risico de niveaus 'laag', 'gemiddeld' en 'hoog'. De kans wordt bepaald aan de hand van de formule kans x impact. Gebruikmaken van de bijbehorende kleuren is aan te raden. De onderstaande matrix kan worden gebruikt voor het vaststellen van de risico's voor betrokkenen.

		Kans		
		laag	midden	hoog
Impact	hoog	laag	hoog	hoog
	midden	laag	midden	hoog
	laag	laag	laag	laag

*De bovenstaande risicomatrix is illustratief. Risico's met een lage impact of lage kans worden als laag ingeschat indien het risico niet verder kan worden gemitigeerd. Zo kan bijvoorbeeld de impact van ransomware hoog zijn, maar door het nemen van de juiste technische maatregelen de kans (zeer) laag. Het risico kan dan ten behoeve van de risico-acceptatie als laag beschouwd worden.

Voeg aanvullende informatie in het tekstveld toe.

Beschrijving risico voortvloeiend uit de verwerkingen van persoonsgegevens op basis van het voorstel van wet	Kans	Impact	Risico-inschatting
Verkrijgen van een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van betrokkene	Hoog	Hoog	Hoog

Voeg hier tussen de lijnen aanvullende informatie over de risico's toe.

Beoordeling van het voorstel zoals beschreven in paragraaf 1.

Inzet van de bevoegdheid om gegevens in publiek toegankelijke bronnen te zoeken en over te nemen

In de tabel 3.1 in paragraaf 3 zijn alle verwerkingen die aan de orde zijn geïnventariseerd. Voor wat betreft de inschatting van de impact kan het volgende gesteld worden:

- Voor wat betreft het inschatten van welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie of bescherming; Verkrijgen van een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van betrokkene.
- Voor wat betreft het inschatten van de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden; De kans dat deze gevolgen zullen intreden is groot nu in het online domein de noodzakelijke informatie over ernstige verstoringen van de openbare orde grotendeels bestaat uit persoonsgegevens of gegevens die onlosmakelijk verknoopt zijn met persoonsgegevens.
- Voor wat betreft het inschatten van de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden. De impact van de inbreuk op de privacy van de betrokkene is hoog.

Inzet van de bevoegdheid tot het in publiek toegankelijke bronnen volgen van personen van wie aannemelijk is dat zij een substantiële rol hebben in een ernstige verstoring en in het kader daarvan persoonsgegevens overnemen

- Voor wat betreft het inschatten van welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen, zoals het verbod op discriminatie en privacy; Verkrijgen van een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van betrokkene.
- Voor wat betreft het inschatten van de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden; De kans dat deze gevolgen zullen intreden is groot nu in het online domein de informatie grotendeels bestaat uit persoonsgegevens of gegevens die onlosmakelijk verknoopt zijn met persoonsgegevens.

- f. Voor wat betreft het inschatten van de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.
De impact van de inbreuk op de privacy van de betrokkene is hoog.

Conclusie

Met de uitoefening van beide voorgestelde bevoegdheden is het voorzienbaar dat een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van betrokkene kan ontstaan, zoals zijn dagelijkse gewoonten, zijn permanente of tijdelijke verblijfplaats, zijn dagelijkse of andere verplaatsingen, de activiteiten die hij uitoefent, zijn sociale relaties en de sociale kringen waarin de betrokkene verkeert.

De verwerkingen zijn dan ook te kwalificeren als hoog-risicoverwerkingen.

Op basis van een objectieve beoordeling kan vastgesteld worden dat deze gegevensverwerking gepaard gaat met een (hoog) risico voor de rechten en vrijheden van de betrokkenen.

NB. Zoals uiteengezet in paragraaf 4 (toe te passen technologieën) en paragraaf 8 (verwerkingslocaties) zijn de privacyrisico's welke gerelateerd zijn aan gebruik van reeds ingebruikzijnde systemen dan ook buiten scope van de DPIA.

De focus in deze DPIA ligt op de inventarisatie en beoordeling van de impact de gegevensverwerking op basis van het voorstel van wet op de (inbreuk op de) privacy van betrokkenen.

Vanzelfsprekend worden, voor zover aan de orde, bij de implementatie van het voorstel door de betrokken partijen de nieuwe privacyrisico's geïnventariseerd, beoordeeld en gemitigeerd conform de geldende wettelijke kaders, Rijksbeleid en standaarden.

D. Maatregelen en restrisico's

In onderdeel D wordt gezien welke maatregelen kunnen worden getroffen om de in onderdeel C erkende risico's te voorkomen of te verminderen.

Welke maatregelen in redelijkheid worden getroffen is een belangenafweging van de wetgever of verwerkingsverantwoordelijke. Voor dit onderdeel van de DPIA is in het bijzonder expertise over informatiebeveiliging belangrijk.

CONCEPT

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt. Voeg aanvullende informatie in het tekstveld onder de tabellen toe.

Beschrijf ook de resterende risico's die nog aanwezig zijn na de uitvoering en/of implementatie van de geïdentificeerde maatregelen. Geef per resterend risico aan wat het niveau is van dit risico.

Geef tot slot een conclusie over de restrisico's. Zijn deze acceptabel? En is er een voorafgaande raadpleging bij de Autoriteit Persoonsgegevens nodig?

Toelichting

De privacyregelgeving geeft als beginsel dat persoonsgegevens door het nemen van passende technische en organisatorische maatregelen op dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat de persoonsgegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging⁴⁸.

In deze paragraaf worden maatregelen beschreven gericht op het mitigeren van de geïnterpreteerde privacyrisico's.

Passende technische en organisatorische maatregelen

De verwerkingsverantwoordelijke moet passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen met betrekking tot het uitvoeren van het voorstel van wet na de implementatie ervan⁴⁹.

In het begrip 'passend' ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. Het begrip 'passend' duidt mede op een proportionaliteit tussen de maatregelen en de risico's. Naarmate deze risico's groter zijn, worden zwaardere eisen gesteld aan de beveiliging van de persoonsgegevens.

Er is geen verplichting om altijd de zwaarste beveiliging te nemen. Enkel is vereist dat de maatregelen met het oog op de beschikbare technologie en uitvoeringskosten redelijk zijn⁵⁰. Deze maatregelen moeten het risico tot een aanvaardbaar niveau brengen.

Risico's volledig reduceren is niet mogelijk. Dit betekent dat er altijd een resterend risico zal overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe het tot dit restrisico is gekomen en waarom deze aanvaardbaar wordt geacht. Deze worden in paragraaf 17 geïdentificeerd.

Een passend beveiligingsniveau veronderstelt dat gewerkt wordt met een planning- en control cyclus (plan-do-check-act) aan de hand waarvan kan worden beoordeeld of de beveiliging steeds adequaat is voor de huidige stand van de techniek en de organisatie⁵¹.

Voor te treffen maatregelen kan worden aangehaakt bij beveiligingskaders en -standaarden, beste praktijken en goedgekeurde gedragscodes en certificeringsmechanismes.

⁴⁸ Artikel 4, eerste lid, onder f, Richtlijn.

⁴⁹ Artikel 29 Richtlijn

⁵⁰ Wpg 4. 6a, 6b, 14 en uitwerking in het Besluit.

⁵¹ In de Wpg zijn bepalingen opgenomen voor het inrichten van een privacy organisatie (opzet-bestaans-uitwerking).

Wanneer een of meerdere maatregelen van toepassing zijn op de gegevensverwerkingen, beschrijf dan specifiek welke beveiligingsstandaarden, praktijken, gedragscodes en/of certificeringsmechanismen van toepassing zijn en op welke manier deze in de praktijk van toepassing zijn op de gegevensverwerkingen.

Denk aan de volgende maatregelen:

- Pseudonimiseren en versleutelen van persoonsgegevens;
- Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
- Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
- Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Daarnaast kan worden gedacht aan de volgende maatregelen, mede bedoeld om ervoor te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor ze worden verwerkt, juist en nauwkeurig zijn:

- Fysieke maatregelen voor toegangsbeveiliging en logische toegangscontrole;
- Opslag van gegevens in een kluis;
- Project-, risico- en incidentenmanagement;
- Data opsplitsen;
- Dataminimalisatie;
- Back-ups;
- Integriteitscontroles;
- Meerfactor-authenticatie;
- Monitoring en logging;
- Controle van toegekende bevoegdheden;
- Privacy bewustzijn- en beveiligingstrainingen;
- Managementrapportages over risicobeheer;
- Beperken inzageniveau;
- Periodiek een audit of hack- of penetratietest uitvoeren;
- Richtlijnen inzake gebruik ICT-hulpmiddelen, zoals versleutelde USB-sticks en beveiligde opslagplekken;
- Resonable-disclosurebeleid;
- Geheimhoudingsverklaringen;
- Service level agreements (met boeteclausules);
- Verwerkersovereenkomsten.
- Screening personeel en VOG-verklaring.

Bij het bepalen van de gepaste maatregelen moet ook rekening gehouden worden met maatregelen die voortvloeien uit de Baseline Informatiebeveiliging Overheid (BIO). De maatregelen hoeven zich overigens niet te beperken tot beveiligingsmaatregelen. Denk bijvoorbeeld aan: het extra informeren van de betrokkenen, een extra keuze-, inspraak- of bezwaarmogelijkheid voor de betrokkenen, periodieke controles, toezicht verstevigen, verhogen bewustwording en dataminimalisatie.

De Richtlijn noemt tot slot de volgende maatregelen:

- Controle op de toegang tot de apparatuur;
- Controle op de gegevensdragers;
- Opslagcontrole;
- Gebruikscontrole
- Controle op de toegang tot gegevens;
- Transmissiecontrole;
- Invoercontrole;
- Transportcontrole; en

- Herstelmogelijkheid⁵².

In de Richtlijn is opgenomen dat lidstaten logbestanden van bepaalde vormen van verwerkingen dienen bij te houden, zodat het mogelijk is de reden, datum en het tijdstip van die handelingen te achterhalen. Indien mogelijk ook de identiteit van de persoon die de persoonsgegevens heeft geraadpleegd of bekend heeft gemaakt, en de identiteit van de ontvangers van die persoonsgegevens⁵³.

- Bij conceptregelgeving: *ook op het niveau van regelgeving kunnen maatregelen worden getroffen*. Denk hierbij aan het voorschrijven van *maximum bewaartermijnen*, het beperken van inzage in en besluiten over persoonsgegevens tot bepaalde functionarissen of geheimhoudingsverplichtingen.
- Het is belangrijk dat een departementale Chief Information Security Officer (CISO) de genoemde technische en maatregelen toets voordat de DPIA definitief wordt vastgesteld.

Big Data

- Bij Big data-analyses (zie paragraaf 4) waarbij persoonsgegevens worden verwerkt, dient, gelet op de daarmee gepaard gaande risico's, in het bijzonder aandacht te worden besteed aan het treffen van de volgende maatregelen:
- Zorg ervoor dat naarmate de mogelijkheden van patroonherkenning bij de toepassing van big data minder zijn, een goede validatie door experts op het desbetreffende vakgebied plaatsvindt om het risico van foutieve uitkomsten zoveel mogelijk te reduceren.
- Zorg ervoor dat de data zoveel als met een redelijke inspanning mogelijk is, up to date zijn, de te gebruiken datasets een zo gering mogelijke bias (afwijking) bevatten en dat de te gebruiken algoritmen en analysemethoden deugdelijk zijn.
- Bepaal, rekening houdend met de potentiële impact van de toepassing, de foutmarge die bij de toepassing mag optreden. Documenteer hoe deze foutmarge tot stand is gekomen.

Zorg ervoor dat nuttige informatie aan betrokkenen wordt verschaft over de gebruikte logica achter de analyse en dat voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen en analysemethoden.

Bij de toepassing van de uitkomsten van *big data*-analyses dient aandacht te worden besteed aan het treffen van de volgende maatregelen:

Zorg voor menselijke tussenkomst in het proces van geautomatiseerde besluitvorming⁵⁴. Naarmate de potentiële negatieve impact voor de betrokkene groter wordt, neemt de noodzaak voor een goede validatie en een weging van de uitkomsten navenant toe.

Resterende risico's

Na het identificeren van risico's (punt 16) en de maatregelen (punt 17) om deze risico's te mitigeren, dient te worden beoordeeld welke resterende risico's aanwezig zijn. Het is namelijk niet mogelijk om risico's met volledige zekerheid te mitigeren en dat is acceptabel. Organisaties hebben namelijk niet oneindig hoeveelheid tijd, energie en mogelijkheden om risico's volledig te mitigeren.

Bij het beoordelen van de resterende risico's is het te adviseren om aan de volgende punten aandacht te besteden:

Geef aan welke risico's (paragraaf 16) niet volledig door de genomen maatregelen (paragraaf 17) voorkomen worden.

Vermeld specifiek in welke situatie met welke persoonsgegevens een resterend risico aanwezig is. Schat het resterende risico in met de formule kans x impact en door de niveaus laag, gemiddeld en hoog te gebruiken.

⁵² Artikel 29, tweede lid, Richtlijn.

⁵³ Artikel 25, eerste lid, Richtlijn.

Beschrijf helder en duidelijk waarom deze resterende risico's na het nemen van de maatregelen acceptabel zijn.

Wanneer bij de beoordeling van de restrisico's naar voren komt dat de restrisico's een hoog risico opleveren, ondanks de genomen maatregelen, dan moet de Autoriteit Persoonsgegevens geraadpleegd worden over de gegevensverwerkingen die overwogen worden te initiëren.

Dit heet voorafgaande raadpleging.

Gebruik voor de inschattingen van de risico's de niveaus **laag**, **gemiddeld** en **hoog**.
Gebruikmaken van de bijbehorende kleuren is aan te raden.

Risico	Maatregelen	Resterend risico en risico-inschatting	Beheerder van maatregelen
Verkrijgen van een min of meer volledig beeld van bepaalde aspecten van het persoonlijk leven van betrokkene	Proces met condities aan het inzetten van de bevoegdheden (advies politie, case by case beoordeling (geen generieke bevoegdheid), verzoek aan rechter commissaris voor machtiging tot geven bevel, intrekken bevel)	laag	-
	Passende bewaartermijnen	Laag	-

NB. Bij beheerder van maatregelen is niets ingevuld. In het voorstel van wet zijn maatregelen opgenomen. Bij de implementatie van de wet door de uitvoeringsorganisaties dienen processen te worden ingericht ten behoeve van het opvolgen van de geformuleerde maatregelen. Dit is buiten scope van deze DPIA Rapportage.

Voeg hier tussen de lijnen aanvullende informatie over de maatregelen toe.

Conditie verbonden aan het toepassen van de bevoegdheid

Het is toegestaan voorgestelde bevoegdheden in te zetten om een ernstige verstoring van de openbare orde te voorkomen, te beletten of te beëindigen indien de bevoegdheden gebaseerd op Artikel 3 Politiewet 2012 ontoereikend zijn.

Geformuleerde controls (proces-niveau) in dit verband zijn:

De burgemeester beoordeelt (case by case) en beslist tot het doen van een vordering aan de rechter-commissaris, waarna de burgemeester op basis van de door de rechter-commissaris verleende machtiging het bevel kan geven tot een van de geïntroduceerde bevoegdheden of een combinatie van beiden.

Vereiste daarvoor is dat zich een ernstige verstoring van de openbare orde voordoet, dan wel dat aanwijzingen bestaan dat een ernstige verstoring zal plaatsvinden.

Periode waarin bevoegdheden worden ingezet

De verwachting is dat de bevoegdheid tot het zoeken naar en overnemen van persoonsgegevens in de regel enkele dagen tot maanden zal worden ingezet voordat de ernstige verstoring van de openbare orde zal plaatsvinden en daarmee vooral preventief van aard is. Maar niet langer dan vier weken aan een gesloten, zonder een hernieuwd toetsmoment.

Het is echter ook mogelijk dat vorenbedoelde bevoegdheid zo nodig vlak voor of zelfs nog ten tijde van de ernstige verstoring van de openbare orde zal worden ingezet, bijvoorbeeld als duidelijk is dat mensen onderweg zijn om een bepaald evenement ernstig te verstoren.

Met de inzet van de bevoegdheid tot het zoeken naar en overnemen van persoonsgegevens wordt beoogd gegevens te vergaren over het tijdstip en de locatie waarop de ernstige verstoring kan plaatsvinden, maar ook over de ernst en omvang van de te verwachten verstoring, zoals hoeveel personen op de ernstige verstoring afkomen of welke groeperingen betrokken zijn, en de context waarbinnen een ernstige verstoring plaatsvindt. De tweede bevoegdheid is gericht op een persoon die een substantiële rol heeft in het veroorzaken van een ernstige openbare orde verstoring. Gegevens die ten aanzien van deze persoon worden verzameld kunnen leiden tot (bestuurlijke) maatregelen, zoals het opleggen van een gebiedsverbod

Intrekken bevel

Als niet langer aan de voorwaarden voor de uitoefening van de bevoegdheden wordt voldaan, trekt de burgemeester het bevel in;

Zodra blijkt dat de vergaarde persoonsgegevens van geen betekenis zijn voor het onderzoek naar de ernstige verstoring van de openbare orde, moeten deze worden vernietigd. Dat geldt ook voor de vergaarde persoonsgegevens die niet langer noodzakelijk zijn voor het onderzoek of na afloop van een periode van een half jaar waarin wordt gezien of deze verder verwerkt moeten worden.

Passende bewaartermijnen

Zoals toegelicht in paragraaf 3.5 van de concept MvT bij het voorstel van wet, voorziet het wetsvoorstel in afwijking van artikel 9, vierde lid, van de Wet politiegegevens in concrete en passende bewaartermijnen.

De persoonsgegevens die met de uitoefening van de bevoegdheden worden vergaard, mogen slechts worden verwerkt voor zolang deze noodzakelijk zijn voor het onderzoek naar de ernstige verstoring van de openbare orde of gedurende een periode van een half jaar om te zien of de gegevens aanleiding geven tot een nieuw onderzoek of een nieuwe verwerking. Deze laatste termijn van een half jaar is noodzakelijk, onder meer omdat het vaker voorkomt dat ernstige verstoringen van de openbare orde strafbare feiten omvatten. Op deze wijze kan in een later stadium worden gezien of een onderzoek moet worden opgestart naar deze strafbare feiten. Na afloop van beide termijnen moeten de vergaarde persoonsgegevens worden vernietigd.

Conclusie

Op basis van hetgeen uiteen is gezet in deze paragraaf kan worden vastgesteld dat de juridische maatregelen op adequate wijze de hiervoor beschreven risico's voorkomen of te verminderen.

NB. Zoals uiteengezet in paragraaf 4 (toe te passen technologieën) en paragraaf 8 (verwerkingslocaties) vallen de privacyrisico's welke gerelateerd zijn aan gebruik van reeds ingebruikzjnde systemen buiten scope van de DPIA.

De focus in deze DPIA ligt op de inventarisatie en beoordeling van de impact de gegevensverwerking op basis van het voorstel van wet op de (inbreuk op de) privacy van betrokkenen.

Vanzelfsprekend worden, voor zover aan de orde, bij de implementatie van het voorstel door de betrokken partijen de nieuwe privacyrisico's geïnventariseerd, beoordeeld en gemitigeerd conform de geldende wettelijke kaders, Rijksbeleid en standaarden.

Voeg hier tussen de lijnen de beschrijving toe over de resterende risico's, de risico-inschatting en onderbouwing voor acceptatie resterende risico's. Noem ook of er een voorafgaande raadpleging nodig is of niet.

Bij het beoordelen van de resterende risico's is aan de volgende punten aandacht besteed:

- Of en indien voor welke risico's (paragraaf 16) niet volledig door de genomen maatregelen (paragraaf 17) de risico's voorkomen kunnen worden;
- Vermeld in welke specifiek situatie met de verwerking van welke persoonsgegevens een resterend risico aanwezig is;
- Is helder en duidelijk uiteengezet waarom deze resterende risico's na het nemen van de maatregelen acceptabel zijn.

Beoordeling restrisico

Vastgesteld kan worden dat op basis van de waarborgen:

- opgenomen in het Wetsvoorstel;
- ten behoeve van de bescherming van de rechten van betrokkenen;
- in het geval van inzetten van de nieuw geïntroduceerde bevoegdheden;
- de geïnventariseerde en beoordeelde privacy risico's in deze DPIA (paragraaf 16);
- en de onderbouwing bij de geformuleerde maatregelen in paragraaf 17
- het ingeschatte restrisico als laag en acceptabel beoordeeld kan worden.

De reden hiervoor dat bij de formulering van waarborgen in het Wetsvoorstel binnen de context waarin de bevoegdheden worden ingezet zorgvuldig zijn afgewogen in balans met de borging van andere (grond)rechten zoals recht op vergadering en veiligheid van leefomgeving. Hierbij wordt in het bijzonder de gefaseerde toepassing van bevoegdheden genoemd⁵⁵ en de case by case beoordeling van de situatie voorafgaand aan het doen van een aanvraag tot machtiging bij de rechter commissaris.

⁵⁵ Hiermee wordt bedoeld: Pas eerst nadat de bevoegdheden uit Artikel 3 Politiewet niet toereikend zijn, wordt overwogen of gebruikmaking van de nieuwe bevoegdheden uitkomst kan bieden en op welke wijze.

Verslag DPIA WGS versie 28/2/2020 ZVH – 4 maart 2020

Uitgevoerd door: 5.1.2e 5.1.2e (JenV/DGRR, 5.1.2e 5.1.2e (JenV), 5.1.2e
(JenV), 5.1.2e 5.1.2e (JenV), 5.1.2e 5.1.2e ZVH), 5.1.2e 5.1.2e JenV), 5.1.2e
5.1.2e (JenV, verslaglegging)

Algemeen

Doel van de DPIA WGS is het in kaart brengen van mogelijke gevolgen voor de privacy van betrokkenen door het wetsvoorstel gegevensverwerking door samenwerkingsverbanden (WGS). De WGS beoogt knelpunten in samenwerkingsverbanden bij het gezamenlijk verwerken van gegevens weg te nemen. Er vindt een belangenafweging plaats tussen het zwaarwegend algemeen belang in de WGS (art. 2, tweede lid, WGS) en het privacy belang van betrokkenen.

Het FEC, de iCOV, de RIEC's en de ZVH krijgen in het wetsvoorstel een expliciete grondslag om aan hen als samenwerkingsverband als geheel informatie te kunnen verstrekken; nu kan dit slechts op bilateraal niveau plaatsvinden. De samenwerkingsverbanden worden hiermee echter geen juridische entiteiten. Er is binnen de swv-en sprake van een gezamenlijke verwerkingsverantwoordelijkheid. Hiernaast biedt de WGS ruimte voor PPS, deelname van private partijen, aan samenwerkingsverbanden. De Syri-zaak heeft aangetoond dat het van essentieel belang is voldoende waarborgen in werkprocessen te hebben voor een rechtmatige en behoorlijke verwerking van persoonsgegevens. Naast de algemene beginselen in artikel 5 AVG is daarvoor met artikel 8 in de WGS een specifieke bepaling opgenomen. Op AMvB niveau kunnen nog nadere waarborgen worden opgenomen. Nieuw in het wetsvoorstel WGS is ook de zgn. leveringsplicht in artikel 5. Tegenover deze plicht staan voldoende waarborgen die recht doen aan de autonomie van de deelnemers.

Op AMvB- en uitvoeringsniveau zullen aparte DPIA's worden gemaakt.

Bespreekpunten

- De vraag is of de in artikel 47 WGS omschreven doelstelling voldoende concreet is. Daar kun je het zwaarwegend algemeen belang niet voldoende uithalen en daarbij dient complexe casuïstiek beter omschreven te worden. Complexe casuïstiek heeft betrekking op meerdere gebieden, zoals straf en zorg, waarbij naast drang ook dwang mogelijk is. Het blijft nu erg abstract. Voor een scherpere formulering van artikel 47 zou gekeken kunnen worden naar de omschrijving van complexe casuïstiek in het 'Handvat Gegevensuitwisseling in het Zorg- en Veiligheidsdomein'. Daarbij zou ook aandacht moeten worden geschonken aan de vraag wat een ZVH in welke fase mag en met wie. Er zijn twee fasen, die van de persoonsgerichte casusanalyse / persoonsgerichte aanpak en die van het uitvoeren van een gezamenlijke strategie aan de hand van geprioriteerde casussen. Ook zouden, liefst in de WGS zelf en anders bij AMvB de zwaardere gevallen benoemd moeten worden die een ZVH behandelt, bijvoorbeeld verwarde personen, en de urgentie in dat geval. In de MvT zou dan aan de hand van voorbeelden kunnen worden weergegeven waar we het precies over hebben.
Actie: artikel 47 dient scherper te zijn in de formulering van het doel van de ZVH en in de MvT dient de toegevoegde waarde van de ZVH duidelijker te worden weergegeven, m.n. ten aanzien van complexe casuïstiek.
- In de aanloop naar het casuoverleg worden ook al gegevens uitgewisseld om vast te stellen of gezamenlijke betrokkenheid nodig is. Het lastige hier is dat, zodra vaststaat dat een partij geen taak heeft, deze eigenlijk niet in het casuoverleg mag zitten. In het casuoverleg vindt eerst een verkenning plaats om te zien wie aan tafel moet komen zitten voor het casuoverleg. Stap voor stap wordt er een beeld gevormd van de persoon. Van tevoren weet je niet wie welke informatie heeft of wie betrokken moet en wil zijn en daar moet dus ruimte voor worden gegeven. Er is sprake van een aanmelding van een persoon (casus), toetsing van de aanmelding en kijken of andere partijen betrokken willen zijn. Dit houdt ook in dat er gesprekken kunnen zijn met mensen die wellicht niet nodig zijn voor de casus. Deze partijen

Met opmerkingen 5.1.2e B11: Artikel 47 is zo aangepast dat daarin nu ook een expliciete verwijzing naar de behandeling van complexe casuïstiek is opgenomen. Een verwijzing naar deze aanscherping is ook opgenomen in par. 8.1 van de MvT.

mogen de verkregen informatie dan niet verder verwerken. In dit licht bezien is de omschrijving van de grondslag in artikel 52 te vaag. In lid 7 is gepoogd het bovenstaande uit te leggen, maar het is niet helder. In de triage dient bekeken te worden welke partijen gezien hun betrokkenheid of vermoeden nodig zijn bij het opstellen van het plan van aanpak, dus een gerichte uitnodiging. Per fase dient dit goed omschreven te worden:

1. Zijn partijen noodzakelijk bij de zaak?
2. Wie zijn betrokken bij het casusoverleg?
3. Plan van aanpak en wie gaat wat doen?

De verwerker, genoemd in artikel 52, lid 2, is in dit verband de procesregisseur die de verkenning doet. De term "verwerker" zal in dat artikellid moeten worden vervangen door "de deelnemers", omdat onder de WGS de deelnemers aan een ZVH de gezamenlijke verwerkingsverantwoordelijken zijn, die ook verantwoordelijk zijn voor die rol van procesregisseur. Dat die rol in de praktijk aan iemand wordt gemandateerd, doet daar niet aan af.

- Een ZVH heeft geen gezamenlijk dossier. De dossiers liggen bij de partners. Sommige ZVH-en gebruiken GCOS. Het beheer van GCOS en de gezamenlijke verantwoordelijkheid van de deelnemers vergt nadere regeling bij AMvB.
- De passage in de derde alinea van par. 4.4. MvT waarin naar voren komt dat de WGS meer rechtszekerheid en transparantie voor de betrokken burgers en professionals biedt, past beter onder het kopje "Waarborgen". De beschrijving van de verwerkingsmethoden in die alinea is nogal summier en zou meer aandacht mogen besteden aan het feit dat de ZVH door gezamenlijk informatie van verschillende partijen te verwerken een compleet persoonsbeeld willen creëren om tot een multidisciplinair aanpak (zorg, jeugd, straf) van complexe problematiek te komen. Zoals eerder ten aanzien van artikel 52 is vermeld, is het nodig ook in deze alinea te beschrijven welke stappen men in iedere fase zet. Dan kan ook beter beargumenteerd worden dat de WGS meer rechtszekerheid en transparantie biedt.
- De vierde alinea van par. 4.4. MvT zou nog kunnen aangevuld met te wijzen op de mogelijkheid om op basis van artikel 8 waarborgen en beperkingen te stellen aan de gegevensverwerkingen door de ZVH en op artikel 4, lid 2, waarin de aanstelling van een FG wordt voorgeschreven.
- N.a.v. het laatste tekstdeel van par. 4.4. MvT rijst de vraag waarom je de informatie sneller bij elkaar zou willen hebben. Dat wordt nu niet toegelicht. Belangrijker is dat men grondiger kan verkennen wat er aan de hand is. Experts zouden ook aan de activiteiten van de ZVH moeten kunnen deelnemen en over de taakuitoefening van een deelnemer mogen adviseren, maar geen data verwerken. De passage vanaf '[ter discussie]' kan worden geschrapt, omdat het desbetreffende punt in de UPP-regelgeving komt.

Met opmerkingen 5.1.2e B2]: Het nieuwe vierde lid van artikel 52 beoogt dit te regelen.

Met opmerkingen 5.1.2e 33]: Is aangepast.

Met opmerkingen 5.1.2e 34]: GCOS is het huidige systeem, maar wordt uitgefaseerd. Daarom is het niet wenselijk om amvb het beheer van GCOS te regelen. Wat de gezamenlijke verantwoordelijken in aanvulling op wat uit de AVG aan waarborgen moeten treffen, is vastgelegd in de artikelen 8, 8a en 8b.

Met opmerkingen 5.1.2e 35]: De kopjes in deze paragraaf zijn verdwenen.

Met opmerkingen 5.1.2e B6]: Verwerkt in de tweede alinea van par. 4.4.

Met opmerkingen 5.1.2e 37]: Par. 4.4. is aangevuld met een verwijzing naar de waarborgen in de artikelen 8, 8a en 8b.

Met opmerkingen 5.1.2e B8]: In het aangepaste artikel 52, elfde lid, is ruimte geschapen om bij amvb ook experts tot het casusoverleg toe te laten.

Met opmerkingen 5.1.2e 39]: Is geschrapt.

Verslag DPIA WGS versie 28/2/2020 RIEC's - 4 maart 2020

Uitgevoerd door: 5.1.2e 5.1.2e (JenV/DGRR, 5.1.2e 5.1.2e (RIEC
5.1.2e (DGRR), 5.1.2e 5.1.2e JenV), 5.1.2e (JenV, verslaglegging)

Algemeen

Doel van de DPIA WGS is het in kaart brengen van mogelijke gevolgen voor de privacy van betrokkenen door het wetsvoorstel gegevensverwerking door samenwerkingsverbanden (WGS). De WGS beoogt knelpunten in samenwerkingsverbanden bij het gezamenlijk verwerken van gegevens weg te nemen. Er vindt een belangenafweging plaats tussen het zwaarwegend algemeen belang in de WGS (art. 2, tweede lid, WGS) en het privacy belang van betrokkenen.

Het FEC, de iCOV, de RIEC's en de ZVH krijgen in het wetsvoorstel een expliciete grondslag om aan hen als samenwerkingsverband als geheel informatie te kunnen verstrekken; nu kan dit slechts op bilateraal niveau plaatsvinden. De samenwerkingsverbanden worden hiermee echter geen juridische entiteiten. Er is binnen de swv-en sprake van een gezamenlijke verwerkingsverantwoordelijkheid. Hiernaast biedt de WGS ruimte voor PPS, deelname van private partijen, aan samenwerkingsverbanden. De Syri-zaak heeft aangetoond dat het van essentieel belang is voldoende waarborgen in werkprocessen te hebben voor een rechtmatige en behoorlijke verwerking van persoonsgegevens. Naast de algemene beginselen in artikel 5 AVG is daarvoor met artikel 8 in de WGS een specifieke bepaling opgenomen. Op AMvB niveau kunnen nog nadere waarborgen worden opgenomen. Nieuw in het wetsvoorstel WGS is ook de zgn. leveringsplicht in artikel 5. Tegenover deze plicht staan voldoende waarborgen die recht doen aan de autonomie van de deelnemers.

Op AMvB- en uitvoeringsniveau zullen aparte DPIA's worden gemaakt.

Besprekpunten

- Artikel 31: is de doelbinding in dit artikel voor uitwisselen van persoonsgegevens in de RIEC's duidelijk en concreet genoeg verwoord? In de wetstekst zelf lijkt deze te beperkt terwijl zij in de MvT juist heel ruim is omschreven. Zo dekt de wetstekst wel af hetgeen nu in de RIEC-convenanten ligt opgesloten, maar is niet duidelijk of onder deze wetstekst ook de aanpak van ondermijning, die de RIEC's in de praktijk nu ook tot hun taken rekenen, valt. Zo is het kaart brengen van het ontwrichtende karakter van ondermijning door de RIEC's breder dan sec het aanpakken van criminele activiteiten. Het zou tenminste mogelijk moeten zijn dat ook de aanpak daarvan door de RIEC's onder de WGS komt te vallen, door bijvoorbeeld bij amvb daartoe de mogelijkheid te scheppen.
- In de RIEC pyramide is in de onderste laag sprake van een persoonsgerichte aanpak van ernstige delicten en bovenaan aan de top is sprake van fenomeen-aanpak op het vlak van ondermijning. De vraag is welke gegevens in welke laag worden gebruikt. Zijn er aan de top van de pyramide persoonsgegevens nodig? Wat nodig is, zijn niet per se persoonsgegevens, maar wel data (anoniem of niet) om structuren en patronen bloot te leggen.
- De WGS dient ook verwerkingsactiviteiten de RIEC's verrichten. De RIEC's zijn bezorgd dat de beschrijving daarvan te rigide is. Ze willen deze uitbreiden naar de wijkscan en het oplossen van handavingsknelpunten. Het zou immers niet handig om een opsomming te geven waarvan nu al vaststaat dat die moet worden aangepast.
- Met betrekking tot artikel 32 geldt dat duidelijk moet zijn waarom deze deelnemers erin staan. Dienen de taken en bevoegdheden in lid 1 te staan of zouden deze ook alle op basis van lid bij amvb kunnen worden aangewezen?
- De noodzakelijke gezamenlijke en geïntegreerde aanpak van georganiseerde criminaliteit is een al een bestaande vorm van samenwerking. Er worden geen nieuwe bevoegdheden gecreëerd.

Met opmerkingen 5.1.2e B1: De tekst van artikel 31 moet worden gelezen in de context van wat in de toelichting op dat artikel staat. Uit die toelichting blijkt dat onder artikel 31 ook de aanpak van ondermijnende criminaliteit valt. Het in kaart brengen van het ontwrichtende karakter daarvan kan worden aangemerkt als een noodzakelijk onderdeel daarvan.

Met opmerkingen 5.1.2e B2: Het antwoord op deze vraag ligt opgesloten in het aangepaste artikel 36, waarin voor elke fase is aangegeven welke gegevens mogen worden gebruikt. Deze aanpassing wordt benoemd in par. 8.1 van de MvT.

Met opmerkingen 5.1.2e B3: Ondervangen door de aanpassing van artikel 31a.

Met opmerkingen 5.1.2e B4: Uit een oogpunt van voorzienbaarheid van de beperking van het recht op privacy en de democratische legitimatie daarvan dienen deze taken en bevoegdheden in de WGS zelf te staan, maar het tweede lid van artikel 32 geeft de mogelijkheid die bij amvb nader te bepalen.

- De ondersteuning die vanuit het RIEC-samenwerkingsverband wordt geboden aan bestuursorganen bij de toepassing van de Wet Bibob is een vorm van advisering, waarbij geen informatie wordt uitgewisseld. De geheimhoudingsbepaling in de Wet Bibob is absoluut. Uitzondering is in RIEC verband voor nader onderzoek, daarna is er pas sprake van de wet Bibob. Daarnaast kan de gemeente aan de RIEC-medewerker een aanwijzing geven hoe een bepaalde zaak aan te pakken. Dit staat in artikel 28 Bibob. Moet dat in de wet? Is artikel 28 Wet Bibob exclusief genoeg? Het is handig om dit in de MvT neer te zetten. Zin uit de wet Bibob toevoegen en uitleggen.
- De inhoud van de artikelen 35 en 36 kan beter bij amvb worden geregeld. Dat geeft meer flexibiliteit.
- Artikel 36, lid 8, over "hit/no hit" behoeft toelichting. Het is namelijk niet werkbaar om steeds naar fase 1 te gaan. Als er signaal komt van de politie, gaan de RIECS immers meteen over naar fase 2. En soms gaan ze over op een derde fase zonder de eerste en tweede fase te doen.
- In de MvT staat: "Zo kunnen in RIEC-verband ook ondermijningsbeelden, wijkscans, gebiedsanalyses en handhavingsknelpunten in worden kaart gebracht". Van belang is dat hier om statistische beelden gaat, niet om persoonsbeelden.
- In par. 4.3 van de MvT is nog een alinea nodig met uitleg over de rol van het LIEC en de verhouding daarvan tot de RIEC's.

Met opmerkingen 5.1.2e 35J: De toelichting op artikel 31 bevat een uitdrukkelijke verwijzing naar het kader van artikel 28 Wet Bibob.

Met opmerkingen 5.1.2e 36J: Uit een oogpunt van voorzienbaarheid van de beperking van het recht op privacy en democratische legitimatie daarvan dienen de te verstrekken gegevens zoveel mogelijk in de WGS zelf te worden opgenomen

Met opmerkingen 5.1.2e B7J: Dit is ondervangen in het nieuwe zesde lid van artikel 36.

Met opmerkingen 5.1.2e 38J: Verwerkt in de toelichting op artikel 31a.

Met opmerkingen 5.1.2e 39J: Is opgenomen in par. 4.3 van de MvT.

Verslag DPIA WGS versie 28/2/2020 FEC - 5 maart 2020

Uitgevoerd door: 5.1.2e (JenV/DGRR, 5.1.2e (FEC), 5.1.2e (FEC), 5.1.2e (OM), 5.1.2e (FG JenV), 5.1.2e (DNB), 5.1.2e (JenV), 5.1.2e (JenV, verslaglegging)

Algemeen

Doel van de DPIA WGS is het in kaart brengen van mogelijke gevolgen voor de privacy van betrokkenen door het wetsvoorstel gegevensverwerking door samenwerkingsverbanden (WGS). De WGS beoogt knelpunten in samenwerkingsverbanden bij het gezamenlijk verwerken van gegevens weg te nemen. Er vindt een belangenafweging plaats tussen het zwaarwegend algemeen belang in de WGS (art. 2, tweede lid, WGS) en het privacy belang van betrokkenen.

Het FEC, de iCOV, de RIEC's en de ZVH krijgen in het wetsvoorstel een expliciete grondslag om aan hen als samenwerkingsverband als geheel informatie te kunnen verstrekken; nu kan dit slechts op bilateraal niveau plaatsvinden. De samenwerkingsverbanden worden hiermee echter geen juridische entiteiten. Er is binnen de swv-en sprake van een gezamenlijke verwerkingsverantwoordelijkheid. Hiernaast biedt de WGS ruimte voor PPS, deelname van private partijen, aan samenwerkingsverbanden. De Syri-zaak heeft aangetoond dat het van essentieel belang is voldoende waarborgen in werkprocessen te hebben voor een rechtmatige en behoorlijke verwerking van persoonsgegevens. Naast de algemene beginselen in artikel 5 AVG is daarvoor met artikel 8 in de WGS een specifieke bepaling opgenomen. Op AMvB-niveau kunnen nog nadere waarborgen worden opgenomen. Nieuw in het wetsvoorstel WGS is ook de zgn. leveringsplicht in artikel 5. Tegenover deze plicht staan voldoende waarborgen die recht doen aan de autonomie van de deelnemers.

Op AMvB- en uitvoeringsniveau zullen aparte DPIA's worden gemaakt.

Bespreekpunten

- Doelstelling FEC: Versterken integriteit financiële sector. Ten behoeve van deze taak is sprake van structurele informatie-uitwisseling. Er is een klassieke methode ("FEC-regulier") en daarnaast de methode van casusoverleggen in Taskforces zoals de Terrorismefinanciering Taskforce en de pilot Serious Crime Taskforce. Verschillende werkwijzen en deelnemers moeten duidelijk terugkomen in de omschrijving van de wetstekst.
- De Politie en FIOD mogen in beide Taskforces op grond van artikel 20 WPG informatie uitwisselen met banken. De banken kunnen OT transactie melden. FIU kijkt ernaar en kan dan concluderen dat er sprake is van een VT. Dit komt ten goede van de opsporing. De vraag rijst of deze verwerking nog opgenomen dient te worden in de wet? Men zou kunnen zeggen dat zij valt onder het artikel over het casusoverleg.
- Willen we dat banken, zoals vastgelegd in artikel 13, eerste lid, worden uitgesloten van casusoverleg? Dan zouden zij niet meer kunnen deelnemen aan beide Taskforces. Wellicht is het handig om private partners op te nemen in de formele wet en dan bij AMvB de mogelijkheid van deelname te beperken. Hierbij moet rekening worden gehouden met het spanningsveld tussen enerzijds de wens van het FEC veel te willen doen met PPS en anderzijds de wens van de Belastingdienst op grond van de fiscale geheimhoudingsplicht geen belastinggegevens aan private partijen te verstrekken.
- In de wet dient duidelijk te worden gemaakt wat voor soort overleggen er zijn (FEC-regulier en de activiteiten van de Taskforces) en welke deelnemers.
- Algemeen opmerking: grip van de betrokkene bij de deling van persoonsgegevens in het samenwerkingsverband/verstrekking aan derden is nog onduidelijk. In de AMvB kan ook veel opgenomen worden, zoals waarborgen voor de betrokkene. Essentiële waarborgen lenen zich niet voor opneming in de AMvB, maar moeten in de wet worden opgenomen. Wel in de gaten houden dat mensen in de praktijk niet te makkelijk omgaan met deze wet en geen extra ruimte gaan zoeken.
- Voor wat betreft PPS in de wet: vanuit het FEC dient nog een standpunt te komen

Met opmerkingen 5.1.2e B1]: Is terug te vinden in de artikelen 12 en 13.

Met opmerkingen 5.1.2e B2]: Door de aanpassing van de doelomschrijving in artikel 11 valt onder de beschrijving van het signalenoverleg in artikel 15 ook de gegevensverwerking in PPS.

Met opmerkingen 5.1.2e B3]: Zie vorige opmerking.

Met opmerkingen 5.1.2e B4]: De banken zijn aangewezen in artikel 12, onder h. Beperkingen zijn mogelijk op basis van het nieuwe slot van datzelfde onderdeel en verder op basis van artikel 8, eerste lid. De uitbreiding van onderdeel h is benoemd in par. 8.1 van de MvT.

Met opmerkingen 5.1.2e B5]: Uit een oogpunt van flexibiliteit is ervoor gekozen dit nader te regelen bij amvb. Wel wordt in par. 4.1 van de MvT beschreven welke partij waaraan deelneemt.

Met opmerkingen 5.1.2e B6]: De grip van deelnemers om de verstrekking aan derden tegen te houden, is vergroot door de aanpassing van het begin van artikel 7, tweede lid. Deze aanpassing wordt benoemd in par. 8.1 van de MvT.

Met opmerkingen 5.1.2e B7]: De kern van de waarborgen is opgenomen in de WGS zelf.

- Artikel 7 lid 1 onder b: dient breder getrokken te worden. Onderdeel b dient aangevuld te worden met het woordje "verplichting(en) van private partijen".
- Artikel 7 lid 2: een deelnemer moet niet aan zwaarwegende belangen te zijn gebonden om bezwaar tegen verstrekking aan derden te kunnen maken.
- Artikel 11 lid 1: het woordje "afstemming" weglaten. Er gebeurt meer dan afstemmen. Er kan ook sprake zijn van bijvoorbeeld analyses. Ook rijst de vraag hoe PPS hierin past. Want het is nu alleen publiekrechtelijk, maar we dienen ook te kijken naar het privaatrechtelijke. Actie: Artikel 11 lid 1 dient uitgebreid te worden door toevoeging van de uitoefening van verplichtingen van banken en andere financiële instellingen ter uitvoering van de Wwft.
- Artikel 11 lid 1: doelstelling dient duidelijker te worden weergegeven. Op pagina 21 van de MvT staat dit aangegeven vanaf 'Het gezamenlijk voorkomen en etc.'. Dit zou moeten worden overgenomen in de wettekst.
- Artikel 12: Er is flexibiliteit nodig bij de deelnemers. Er zijn drie organisaties die geen vaste positie hebben in de FEC-raad. Dat zijn de Kmar, IND en BFT.
Uitleg: In de FEC raad is er sprake van participanten en partners. (WGS spreekt alleen van deelnemers). Participanten zitten niet in de FEC-raad en de partners schuiven alleen aan wanneer er sprake is van een onderwerp waar ze zich mee bezighouden. Partners zijn wel al onderdeel van de FEC, maar alleen als het gaat om beide Taskforces. Voorgesteld wordt om artikel 13 lid 2 te schrappen en de drie partners aan te wijzen in de AMvB, bedoeld in artikel 12, onder k.
- Artikel 15 lid 1: Er zijn bij het FEC verschillende verwerkingsmethoden. Bij "FEC-regulier" wordt er over en weer informatie verstrekt en daarna wordt de casus behandeld. Het initiële overleg komt dus niet in de wet voor.
Uitleg: Proces begint met een signaal van een probleem. Daarna kan een van de partners hulp vragen of kan de partner zeggen dat ze er niks aan hebben maar wellicht dat het voor een andere partner of voor het FEC nuttig kan zijn. Als er sprake is van een complex probleem, dan gaan ze over tot casusoverleg. Wat een signaal is staat in het FEC Informatieprotocol. Deze lijst is niet openbaar, maar het zou geen risico voor het FEC vormen als het wel eventueel openbaar zou zijn. Er zijn 3 adviseurs bij het FEC die toetsen aan de criteria in het Informatieprotocol. Als het probleem wordt doorgezet dan, is het probleem dus getoetst aan het Informatieprotocol en is er een gezamenlijk belang. Ook de Taskforces werken in een casusoverleg. Het programma TF werkt zowel in een casusoverleg als met gegevensanalyse.
- Artikel 15 lid 2: Zou kunnen worden geschrapt. Voorgesteld wordt om bij AMvB te regelen wat onder concrete aanwijzingen moet worden volstaan.
- Artikel 16: Wat er nu gebeurt is dat gezamenlijk verwerken niet kan en dat kan op basis van de WGS wel. Wat wel al kan en ook straks nog mogelijk is, is dat een deelnemer bilateraal kan verstrekken.
- Artikel 16: Profiling is in het geval van FEC niet nodig. Er is vooralsnog geen behoefte aan vanwege het feit dat FEC het niet doet en de noodzaak daarvan niet kan onderbouwen. Er wordt geen gebruik gemaakt van algoritmes. Alles wordt per persoon bekeken. Er worden ook in deze situatie geen personen met groepskenmerken verbonden. De groepskenmerken worden apart bekeken en worden niet gebruikt om een persoon in kaart te brengen.

Met opmerkingen 5.1.2e -B8]: Is aangepast.

Met opmerkingen 5.1.2e -B9]: Is aangepast.

Met opmerkingen 5.1.2e B10]: Is aangepast.

Met opmerkingen 5.1.2e B11]: Is aangepast.

Met opmerkingen 5.1.2e B12]: Is aangepast.

Met opmerkingen 5.1.2e B13]: Is aangepast. Deze aanpassing wordt ook benoemd in par. 8.1.

Met opmerkingen 5.1.2e B14]: Heeft geleid tot aanpassing van artikel 15, eerste lid en toevoeging aan dat artikel van het derde lid.

Met opmerkingen 5.1.2e B15]: Is aangepast.

Met opmerkingen 5.1.2e B16]: Is als mogelijkheid niet opgenomen.

Verslag DPIA WGS versie 28/2/2020 iCOV - 5 maart 2020

Met opmerkingen 5.1.2e B1]:

Uitgevoerd door: 5.1.2e 5.1.2e (JenV/DGRR, 5.1.2e (iCOV), 5.1.2e 5.1.2e
(OM), 5.1.2e (Fin), 5.1.2e (Politie), 5.1.2e 5.1.2e (FG JenV), 5.1.2e
(JenV), 5.1.2e JenV, verslaglegging)

Algemeen

Doel van de DPIA WGS is het in kaart brengen van mogelijke gevolgen voor de privacy van betrokkenen door het wetsvoorstel gegevensverwerking door samenwerkingsverbanden (WGS). De WGS beoogt knelpunten in samenwerkingsverbanden bij het gezamenlijk verwerken van gegevens weg te nemen. Er vindt een belangenafweging plaats tussen het zwaarwegend algemeen belang in de WGS (art. 2, tweede lid, WGS) en het privacy belang van betrokkenen.

Het FEC, de iCOV, de RIEC's en de ZVH krijgen in het wetsvoorstel een expliciete grondslag om aan hen als samenwerkingsverband als geheel informatie te kunnen verstrekken; nu kan dit slechts op bilateraal niveau plaatsvinden. De samenwerkingsverbanden worden hiermee echter geen juridische entiteiten. Er is binnen de swv-en sprake van een gezamenlijke verwerkingsverantwoordelijkheid. Hiernaast biedt de WGS ruimte voor PPS, deelname van private partijen, aan samenwerkingsverbanden. De Syri-zaak heeft aangetoond dat het van essentieel belang is voldoende waarborgen in werkprocessen te hebben voor een rechtmatige en behoorlijke verwerking van persoonsgegevens. Naast de algemene beginselen in artikel 5 AVG is daarvoor met artikel 8 in de WGS een specifieke bepaling opgenomen. Op AMvB niveau kunnen nog nadere waarborgen worden opgenomen. Nieuw in het wetsvoorstel WGS is ook de zgn. leveringsplicht in artikel 5. Tegenover deze plicht staan voldoende waarborgen die recht doen aan de autonomie van de deelnemers.

Op AMvB- en uitvoeringsniveau zullen aparte DPIA's worden gemaakt.

Bespreekpunten

- Artikel 21: Is het doel van iCOV hier concreet genoeg omschreven? Het doel is de integrale benadering en uiteindelijk de aanpak van frauduleuze of ondermijnende activiteiten door diverse overheidsorganisaties. Daarbij zou het begrip "oninbare vorderingen" uit een oogpunt van welbepaaldheid moeten worden aangepast, want het zijn geen oninbare vorderingen waarvoor iCOV bevestigingen doet, maar vorderingen die oninbaar dreigen te worden.
- Artikel 22: De Kansspelautoriteit (KSA) staat er nog bij als deelnemer. Als we kijken naar het doel van iCOV, zou de KSA er inderdaad bij passen: kansspel heeft de aandacht van de DNB in verband met de goede werking van de financiële markt en witwassen.
- Artikel 22, onder i: Er zijn op dit moment gesprekken met de KMAR gaande over toetreding. Dat zou mogelijk zijn op basis van dit onderdeel. Maar wat is de situatie als een partij wil uittreden? Strikt genomen moet je daarvoor de wet aanpassen. Dat duurt lang. Je wilt echter niet dat partijen zeer lang moeten wachten tot ze eruit kunnen. Kun je dit bijvoorbeeld bij AMvB regelen en later in de wet? Privacy-technisch is dit relevant, omdat partijen die voor het doel van iCOV niet meer interessant zijn, niet nodeloos lang in iCOV behoren te blijven zitten.
- Het lijkt ook wenselijk om deelnemers bij AMvB aan het samenwerkingsverband te kunnen toevoegen. Voor de democratische legitimatie van een toevoeging zou het een AMvB met nahangprocedure dienen te zijn.
- Artikel 25: Dit artikel brengt mee:
 - Doorbreking geheimhouding (fiscale geheimhouding of andere geheimhoudingsbepalingen die nationaal zijn vastgelegd, niet zijnde geheimhoudingsbepalingen die voortvloeien uit internationale en/of Europese richtlijnen);
 - Rijkere bron aan data hetgeen noodzakelijk is om representatieve beelden te genereren op basis waarvan effectievere opvolging kan worden gegeven;
 - Makkelijker opvragen data (geen vordering meer nodig). Dit is volgens de toelichting ook uitdrukkelijk de bedoeling. Het is nu erg complex nu: er is namelijk een verdenking en daarmee een vordering nodig om te kunnen uitwisselen met de politie. Dit is noodzakelijk om

Met opmerkingen 5.1.2e B2]: Is aangepast.

Met opmerkingen 5.1.2e B3]: Mij is nog steeds niet helder wat dit nu voor de positie van de KSA in de WGS betekent. Op dit moment wordt zij buiten de WGS gelaten.

Met opmerkingen 5.1.2e B4]: Zie het nieuwe artikel 3, zesde lid.

Met opmerkingen 5.1.2e B5]: Heeft tot aanpassing van artikel 22 geleid (zie nieuw onderdeel j), zij het zonder nahang.

de fiscale geheimhouding van de UAWR te kunnen doorbreken en de informatie van de Belastingdienst beschikbaar te krijgen. De rijkere bron aan data kan stigmatisering en discriminerende effecten tegengaan. Die rijkere bron aan data is niet per se in strijd met het principe van data-minimalisatie. In artikel 5 AVG, waarin dit principe is neergelegd, staat ook dat de verwerking toereikend moet zijn, d.w.z. dat er voldoende relevante data dienen te worden verwerkt om geen verkeerde en daarmee ontoereikende beelden te krijgen.

- De verwerkingsmethoden van iCOV die de drie standaardrapportages iRVI, iRR en iRT NN opleveren, en de beoogde nieuwe methode, iRT compact, moeten duidelijker in de WGS tot uitdrukking komen. De nu opgenomen beschrijving van geautomatiseerde gegevensanalyse in artikel 25 is te weinig specifiek.
- Levert de politie niet teveel aan informatie? De politie kan immers niet vooraf de relevante BVH-informatie selecteren. Op voorhand is niet te zeggen welke personen zullen worden bevraagd ten behoeve van een rapportage dan wel betrokken zullen worden bij een bevraging. Doordat ook algemene mutaties/registraties relevant kunnen zijn, is het bovendien ook beperkt mogelijk om de dataset per soort mutatie/registratie te specificeren. Nu wordt dit opgelost door een technische bewerking van een data-dump van de politie bij het OM. De vraag rijst dan of de levering van politie-data aan het OM om die bewerking uit te voeren, niet al onder de WGS valt. Die vraag is relevant, omdat bij een bevestigend antwoord de politie niet aan de proportionaliteits-eis zou voldoen, ook al doen irrelevante gegevens niet mee in de analyse die uiteindelijk wordt uitgevoerd. Overigens geldt dit ook voor de levering door de Belastingdienst.
- In hoeverre past iCOV Privacy enhancing technologies toe? Daarover zou de memorie van toelichting informatie moeten bevatten. Hiertoe heeft iCOV reeds input aangeleverd.
- Artikel 27: Pseudonimisering kan binnen iCOV alleen bij iRT NN. In die methode worden gepseudonimiseerde data verwerkt tot een product dat in eerste instantie niet tot personen herleidbaar is. Dit zou in artikel 27 tot uitdrukking moeten worden gebracht door na "pseudonimisering" in te voegen: waar mogelijk.

Met opmerkingen 5.1.2e **36j**: Heeft geleid tot aanpassing van artikel 24.

Met opmerkingen 5.1.2e **B7j**: Als het OM als verwerker voor de politie niet meer doet dan de bestanden van de politie gereed maken voor deling en vergelijking, moet dit niet als verstrekking op basis van de WGS van de ene deelnemer (politie) aan een andere deelnemer (OM) worden gezien, maar als een verwerking die aan de verstrekking door de politie aan iCOV voorafgaat. Die laatste verstrekking dient dan uiteraard wel aan het noodzakelijkheidsvereiste te worden getoetst.

Met opmerkingen 5.1.2e **B8j**: Zie passage in par. 4.2 MvT.

Met opmerkingen 5.1.2e : Heeft tot aanpassing van deze bepaling geleid, die terug te vinden is als het nieuwe vijfde lid van artikel 8b.