Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
2621849

Bijlagen
1

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 11 juni 2019
Onderwerp Beleidsreactie onderzoek 'Cross-sectorale gegevensdeling tussen private partijen voor fraudebestrijding'

Tijdens het Algemeen Overleg over financieel-economische criminaliteit op 4 oktober 2018 hebben wij uw Kamer toegezegd onderzoek te laten uitvoeren naar zogenaamde cross-sectorale (branche-overstijgende) gegevensdeling tussen private partijen ten behoeve van fraudebestrijding, een in het Verenigd Koninkrijk bestaand systeem van de organisatie Cifas hiertoe en de eventuele meerwaarde van dit systeem voor fraudebestrijding binnen de Nederlandse situatie[1]. Daarbij staat met name de vraag centraal hoe dergelijke gegevensdeling zich verhoudt tot de binnen Nederland en het Verenigd Koninkrijk geldende privacywetgeving. Met fraudebestrijding wordt gedoeld op bestrijding van de zogenaamde horizontale fraude, dat wil zeggen fraude waar burgers en bedrijven slachtoffer van worden. Voorbeelden daarvan zijn hypotheekfraude, verzekeringsfraude of faillissementsfraude.

Hierbij bieden wij u dit onderzoek aan, dat is verricht door het bureau Considerati, en gaan wij in op de bevindingen en de conclusies van de onderzoekers.

Wij stellen vast dat onderzoekers op basis van hun juridische analyse concluderen dat het fraudepreventiesysteem van Cifas in het Verenigd Koninkrijk (VK), waarin cross-sectoraal (strafrechtelijke) persoonsgegevens worden uitgewisseld, *niet één op één* binnen Nederland overgenomen kan worden. De belangrijkste reden hiervoor is dat de uitzonderingsgronden voor het verwerken van strafrechtelijke persoonsgegevens in het VK anders zijn ingericht dan in Nederland.
De analyse van onderzoekers bevestigt ons beeld dat binnen het Nederlandse wettelijk kader van de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) cross-sectorale gegevensdeling tussen private partijen mogelijk is mèt vergunning van de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens (AP) toetst of de vergunningsaanvraag voldoet aan de eisen van de AVG.
De Nederlandse wetgever heeft nog maar kort geleden met het aannemen van de UAVG, die op 25 mei 2018 in werking is getreden, gekozen voor deze weg van toetsing en vergunningverlening door de AP. Op deze wijze zijn de privacybelangen van betrokkenen geborgd. Dit betekent echter geenszins dat een (potentiële) fraudeur zich kan verschuilen achter die privacyregels. Cross-

[1] Handelingen II 2018/2019, nr. 210, p. 19, 20, 27

sectorale gegevensdeling tussen private partijen is met een vergunning van de Autoriteit Persoonsgegevens immers mogelijk. Wij wachten de ervaringen die door private organisaties worden opgedaan met hun voornemen tot cross-sectorale gegevensdeling ten behoeve van fraudebestrijding, binnen het huidige wettelijke privacy-kader af. Afhankelijk van die ervaringen zal zo nodig nieuwe wetgeving kunnen worden overwogen.

Onderzoek cross-sectorale gegevensdeling tussen private partijen voor fraudebestrijding

In hun onderzoek hebben de onderzoekers allereerst het juridisch kader van de Algemene verordening gegevensbescherming (AVG) beschreven dat voor alle landen binnen de Europese Unie sinds 25 mei 2018 geldt. Vervolgens heeft men een juridische analyse uitgevoerd naar de wettelijke eisen die binnen het Nederlandse rechtsbestel worden gesteld aan cross-sectorale gegevensdeling tussen private partijen in het kader van fraudebestrijding. Daarbij is ook de situatie betrokken dat bepaalde publieke partijen aan een dergelijke gegevensdeling zouden deelnemen. Daarna hebben onderzoekers het systeem voor cross-sectorale gegevensdeling van de organisatie Cifas in het Verenigd Koninkrijk (VK) beschreven en vastgesteld wat de juridische basis van dit systeem in het VK is.
Tot slot hebben de onderzoekers onderzocht in hoeverre het systeem van Cifas toepasbaar is in de Nederlandse situatie en welke mogelijkheden binnen de Nederlandse situatie bestaan voor cross-sectorale gegevensdeling tussen private partijen.

Kader van de Algemene Verordening Gegevensbescherming(AVG)

Wanneer private (en eventueel publieke) partijen cross-sectoraal gegevens delen ten behoeve van fraudebestrijding vindt verwerking van persoonsgegevens plaats. Daarbij gaat het naast ‘gewone’ persoonsgegevens veelal om strafrechtelijke persoonsgegevens. Onder strafrechtelijke persoonsgegevens vallen niet alleen veroordelingen maar ook mogelijk gegronde verdenkingen. Ook in het geval dat private partijen gegevens uitwisselen over mogelijk gepleegde strafbare feiten kan er dus sprake zijn strafrechtelijke gegevens.
Op deze verwerking is de AVG van toepassing. Volgens de AVG is verwerking van persoonsgegevens alleen toegestaan als die verwerking rechtmatig is: er dient sprake te zijn van een duidelijk omschreven doel voor de verwerking, een grondslag zoals genoemd in artikel 6 van de AVG én er dient - in geval van verwerking van strafrechtelijke persoonsgegevens- een uitzonderingsgrond te zijn op het algemeen verwerkingsverbod hiervan.
Als de verwerking rechtmatig is dient deze vervolgens te voldoen aan zorgvuldigheidsvereisten, zoals het treffen het beveiligingsmaatregelen, het vereiste van dataminimalisatie, transparantie over en kwaliteit van gegevens.

Wettelijke eisen voor cross-sectorale gegevensdeling t.b.v. fraudebestrijding in het Nederlandse rechtsbestel

De AVG en de UAVG bieden binnen het Nederlandse rechtsbestel *juridische mogelijkheden tot cross-sectorale gegevensdeling tussen private partijen ten behoeve van fraudebestrijding*. Indien private partijen gegevens willen delen of mogelijk een fraudepreventiesysteem willen inrichten dienen zij allereerst voorafgaand daaraan zorgvuldig te bepalen en vast te leggen wat het precieze doel van de gegevensdeling is. Grondslag hiervoor kan gevonden worden in artikel 6 onder f van de AVG: persoonsgegevens mogen verwerkt worden indien dit noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
11 juni 2019

Ons kenmerk
2621849

verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.
Daarbij dient aan drie eisen te worden voldaan:

1. de aanwezigheid van een gerechtvaardigd belang. Volgens onderzoekers is de verwerking van persoonsgegevens, die strikt noodzakelijk zijn voor het voorkomen van fraude, te beschouwen als een gerechtvaardigd belang, zowel vanuit het oogpunt van een legitiem bedrijfsbelang als vanuit het algemeen belang;
2. de noodzakelijkheidseis: de gegevensdeling moet noodzakelijk zijn voor het doel dat daarmee wordt beoogd. Hierbij wordt mede gelet op vraagstukken van proportionaliteit en subsidiariteit. Daarbij moet ook beoordeeld worden of het doel van de verwerking in redelijke verhouding staat tot de inbreuk op de persoonlijke levenssfeer van de betrokkenen en of het belang anderszins of met minder ingrijpende middelen kan worden gediend;
3. het belang van de verwerkingsverantwoordelijke moet prevaleren boven het belang van de (potentiële) fraudeurs: er dient een weging plaats te vinden tussen de belangen van betrokkenen en het belang van de organisaties bij de bestrijding van fraude.
   Uit beslissingen van de Autoriteit Persoonsgegevens ten aanzien van zwarte lijsten leiden onderzoekers af dat daarbij goed gekeken dient te worden naar de impact van de verwerking op de rechten en vrijheden van betrokkenen. Hoe groter de impact is hoe meer waarborgen moeten worden getroffen. Zo dient onder andere goed gekeken te worden naar de wijze waarop de bewijslast wordt geregeld, het proces van raadpleging (wie krijgt toegang tot de gegevens en op welke wijze) en de scope van de gegevensdeling zowel qua omvang van de deelnemende partijen als qua zaken die kunnen worden ingediend.

Vergunning Autoriteit Persoonsgegevens

Bij het bestrijden van fraude worden strafrechtelijke persoonsgegevens verwerkt. Zoals hiervoor verwoord mogen dergelijke persoonsgegevens alleen worden verwerkt als hiervoor een uitzondering is voorzien. Deze uitzonderingsgrond kan worden gevonden in artikel 10 AVG juncto artikel 33 lid 4 sub c en lid 5 van de UAVG.
Artikel 33 lid 4 sub c bepaalt dat een dergelijke gegevensverwerking alleen kan plaatsvinden als de Autoriteit Persoonsgegevens (AP) daartoe vergunning heeft verleend. Artikel 33 lid 5 UAVG bepaalt dat deze vergunning slechts kan worden verleend, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van betrokkene niet onevenredig worden geschaad. Aan de vergunning kunnen voorschriften worden verbonden.
Private partijen, die voornemens zijn cross-sectoraal gegevens te delen ter bestrijding van fraude, dienen als verwerkingsverantwoordelijken dus gezamenlijk daartoe een vergunning aan te vragen bij de AP.

Deelname publieke partijen aan cross-sectorale gegevensdeling

Omdat aan het hierna aan de orde komende systeem voor gegevensdeling ten behoeve van fraudebestrijding van Cifas in het Verenigd Koninkrijk ook een aantal publieke partijen verbonden zijn hebben onderzoekers onderzocht of het in de Nederlandse situatie mogelijk is dat publieke partijen aan de private cross-sectorale gegevensdeling ten behoeve van fraudebestrijding deelnemen.

De AVG en de UAVG kennen hiertoe mogelijkheden. Er bestaat echter geen algemene wettelijke bepaling op grond waarvan publieke organisaties mogen deelnemen. Daarom dient per publieke partij beoordeeld te worden of een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag in de wet is vastgelegd. Er dient dan beoordeeld te worden of die taak zover strekt dat aan alle organisaties, die deelnemen aan de cross-sectorale gegevensdeling, gegevens verstrekt mogen worden door publieke partijen of dat die publieke partijen - als deelnemer of op andere wijze- gegevens mogen ontvangen.
De Wet gegevensverwerking door samenwerkingsverbanden, die momenteel in voorbereiding is, kan in de toekomst mogelijk een eenvoudiger juridische basis bieden voor een publiek-privaat samenwerkingsverband met als doel fraudebestrijding.

Het systeem van Cifas in het Verenigd Koninkrijk en de juridische basis
In het Verenigd Koninkrijk functioneert een fraudepreventiesysteem, geïnitieerd door een zevental bedrijven, van de organisatie Cifas, bestaande uit onder andere de National Fraud Database en de Internal Fraud Database. Hieraan nemen circa 400 private en enkele publieke organisaties deel, die gegevens delen ten behoeve van fraudebestrijding.
De juridische basis voor deze gegevensdeling ligt in de AVG en de Data Protection Act 2018, de uitvoeringswet van de AVG die in het VK geldt.
In de Data Protection Act 2018 is een uitzonderingsbepaling opgenomen van het verbod tot verwerking van strafrechtelijke persoonsgegevens op basis waarvan het aan 'anti-fraud organisations', zoals Cifas, is toegestaan om strafrechtelijke persoonsgegevens ten behoeve van fraudebestrijding te verwerken. In de Serious Crime Act 2007 is Cifas aangewezen als een dergelijke 'anti-fraud organisation'. Voor gegevensdeling ten behoeve van fraudebestrijding is in het VK dus geen vergunning van de privacy-autoriteit aldaar nodig.
Op basis van die Serious Crime Act zijn ook enkele publieke organisaties deelnemer of verstrekken zij gegevens aan Cifas zonder deelnemer te zijn.
Daarnaast vindt op dagelijkse basis geautomatiseerd verstrekking van strafrechtelijke persoonsgegevens, te weten de nieuwe in de Nationaal Fraud database ingevoerde fraudezaken, aan opsporingsinstanties plaats. Dit gebeurt op basis van artikel 6 lid 1 sub f AVG (gerechtvaardigd belang) en artikel 6 lid 1 sub e AVG (taak van algemeen belang). Deze taak van algemeen belang is Cifas toebedeeld in de Data protection Act 2018.
De waarborgen die Cifas moet treffen om de persoonlijke levenssfeer van betrokkenen te beschermen, heeft Cifas vastgelegd in acht principes, die nader zijn uitgewerkt in een handboek voor deelnemers.

Conclusie onderzoekers m.b.t. toepasbaarheid van het Cifas-systeem in Nederland
De onderzoekers concluderen dat het fraudepreventiesysteem van Cifas in het VK *niet één op één* binnen Nederland overgenomen kan worden. De belangrijkste reden hiervoor is dat de uitzonderingsgronden voor het verwerken van strafrechtelijke persoonsgegevens in het VK anders zijn ingericht dan in Nederland.
In het VK is in de Data Protection Act 2018 een specifieke bepaling opgenomen op basis waarvan het voor een 'anti-fraud organisation', zoals Cifas en zijn deelnemers, mogelijk is om strafrechtelijke gegevens te verwerken ten behoeve van fraudebestrijding.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
11 juni 2019

Ons kenmerk
2621849

In Nederland dienen organisaties, die voornemens zijn cross-sectoraal strafrechtelijke gegevens ten behoeve van fraudebestrijding met elkaar te delen, in tegenstelling tot de situatie in het VK op grond van de UAVG daartoe vergunning aan te vragen bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens toetst voorafgaand aan de verwerking of deze in lijn is met de AVG.
Voor wat betreft de deelname van publieke organisaties aan het Cifas-systeem kent het VK een wettelijke basis in de Serious Crime Act 2007. In Nederland bestaat een dergelijke algemene juridische basis niet en dient per publieke organisatie beoordeeld te worden of er een grondslag is tot deelname aan cross-sectorale gegevensdeling als bedoeld in artikel 6 AVG.

De onderzoekers stellen vast dat hoewel in het VK een wettelijke basis bestaat voor de inrichting van Cifas en de privacy-autoriteit in het VK (Information Commissioner's Office, ICO) (vooralsnog) geen aanleiding ziet tot handhaving, dit niet wil zeggen dat de wijze waarop het systeem van Cifas is ingericht ook binnen de Nederlandse context automatisch rechtmatig is en tot een vergunning van de Autoriteit Persoonsgegevens leidt. De AVG is weliswaar een verordening die voor alle lidstaten van de Europese Unie gelijk is, maar hij laat de lidstaten op een aantal punten wel ruimte om specifieke bepalingen op te nemen of uitzonderingen te maken. Zo konden lidstaten in hun nationale uitvoeringswetten bepalingen opnemen met betrekking tot de verwerking van strafrechtelijke en bijzondere persoonsgegevens, waarbij eigen politieke en maatschappelijke overwegingen een rol konden spelen.
Daarnaast bevat de AVG geen specifieke set van regels maar veeleer principes waaraan moet worden voldaan wanneer gegevens verwerkt worden. Deze principes zijn geformuleerd als open normen en kunnen daarom verschillende worden ingevuld. Het is aan de toezichthouder van een lidstaat om te bepalen of op juiste wijze invulling wordt gegeven aan deze principes en voldoende waarborgen zijn getroffen om de persoonlijke levenssfeer te beschermen. Vanuit de European Data Protection Board (EDPB), waarin alle toezichthouders - waaronder de Autoriteit Persoonsgegevens- zijn verenigd, worden wel richtlijnen gegeven met betrekking tot de invulling, maar er blijft een bepaalde interpretatieruimte voor lidstaten bestaan. Het kan dus zijn dat in het VK bepaalde waarborgen als afdoende worden beschouwd, terwijl de Nederlandse toezichthouder dit anders beoordeelt. Of het systeem van Cifas ook in Nederland rechtmatig zou zijn, zal dus zelfstandig door de Nederlandse toezichthouder moeten worden beoordeeld.

De onderzoekers concluderen dat het feit dat het Cifas-systeem niet één op één kan worden overgenomen *niet* betekent dat er in Nederland geen mogelijkheden zijn om tot cross-sectorale gegevensuitwisseling tussen private partijen te komen. Er bestaat immers, zoals hiervoor omschreven, de mogelijkheid voor partijen om op basis van de AVG en UAVG gezamenlijk een vergunning aan te vragen bij de Autoriteit Persoonsgegevens. Daartoe dienen die partijen eerst gezamenlijk een zogenaamde DPIA (Data Protection Impact Assessment) uit te voeren waarin de risico's van cross-sectorale gegevensdeling voor betrokkenen en maatregelen ter verkleining van die risico's in kaart worden gebracht. Ook dient gezamenlijk een privacy-protocol te worden opgesteld.
De onderzoekers verwijzen verder naar mogelijkheden die de Wet gegevensverwerking door samenwerkingsverbanden in de toekomst kan bieden voor gegevensdeling tussen publieke en private organisaties.

Tot slot wijzen onderzoekers er op dat als op termijn zou blijken dat de mogelijkheden om cross-sectoraal gegevens uit te wisselen juridische verbetering zouden behoeven mogelijk gedacht kan worden aan wijziging van de UAVG:

- ofwel het in aanvulling op artikel 33 lid 4 sub c en lid 5 UAVG creëren van een specifiek kader dat van toepassing is op de vergunningaanvraag tot cross-sectorale gegevensdeling dat randvoorwaarden en waarborgen bevat. Dit kader zou organisaties die een dergelijke vergunning willen aanvragen meer handvatten bieden.
- Ofwel het opnemen van een uitzonderingsgrond voor de verwerking van strafrechtelijke gegevens. Dit betekent dat er geen vergunning van de AP meer nodig zou zijn. Dit laat onverlet dat de AP te allen tijde de bevoegdheid behoudt om zelfstandig of op verzoek toezicht te houden.

Beleidsreactie

Horizontale fraude is een maatschappelijk probleem dat aanzienlijke financiële en emotionele schade tot gevolg kan hebben en kan leiden tot ondermijning van het economisch en financieel stelsel. Het is een dynamisch fenomeen dat vele en wisselende uitingsvormen vormen kent en in toenemende mate digitaler en internationaler wordt.

Voor een effectieve bestrijding van horizontale fraude is het van groot belang om sterk in te (blijven) zetten op het voorkomen van die fraude en op publiek-private samenwerking hierbij. De focus ligt hierbij op de vergroting van de weerbaarheid en de bewustwording van burgers en bedrijven om te voorkomen dat ze slachtoffer worden van fraude en op het opwerpen van barrières door private en publieke partijen om het de fraudeur zo moeilijk mogelijk te maken. Binnen de integrale aanpak van fraude wordt het strafrecht ingezet voor zaken waar het strafrecht het meest effectief kan zijn.

Om horizontale fraude op deze manier aan te kunnen pakken is gegevensdeling nodig. Niet alleen tussen publieke partijen en tussen publieke en private partijen, maar ook tussen private partijen onderling. Daarbij kan het nodig zijn om over de grenzen van de verschillende (private) branches heen, dus cross-sectoraal persoonsgegevens over (potentiele) fraudeurs te kunnen delen en op deze wijze te voorkomen dat burgers en bedrijven (opnieuw) slachtoffer worden. Daarbij kan het gaan om het delen van strafrechtelijke persoonsgegevens.

Tegelijkertijd is het recht op bescherming van de persoonlijke levenssfeer een grondrecht binnen Europa en binnen Nederland. Daarom worden binnen Nederland in de AVG en de UAVG aan de verwerking van (strafrechtelijke) persoonsgegevens, zoals gegevens over (potentiele) fraudeurs, strikte regels gesteld.

Op basis van hun juridische analyse concluderen de onderzoekers dat het fraudepreventiesysteem van Cifas in het VK, waarin cross-sectoraal (strafrechtelijke) persoonsgegevens worden uitgewisseld, *niet één op één* binnen Nederland overgenomen kan worden. De belangrijkste reden hiervoor is dat de uitzonderingsgronden voor het verwerken van strafrechtelijke persoonsgegevens in het VK anders zijn ingericht dan in Nederland.

Ook blijkt uit hun analyse dat binnen het in Nederland geldende wettelijk kader van AVG en UAVG cross-sectorale gegevensdeling tussen private partijen wel mogelijk is, maar mét vergunning van de Autoriteit Persoonsgegevens. Daarbij moeten (private) partijen, die voornemens zijn met elkaar gegevens uit te wisselen, goed met elkaar in kaart brengen welke (strafrechtelijke) persoonsgegevens zij met welk doel willen delen, moeten zij een privacy impact assessment (DPIA) maken om goed in kaart te brengen welke privacy-risico's voor betrokkenen aan deze gegevensdeling verbonden zijn en hoe waarborgen,

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
11 juni 2019

Ons kenmerk
2621849

zoals opgenomen in de AVG kunnen worden gecreëerd. Ook moet men een privacy-protocol opstellen. De Autoriteit Persoonsgegevens toetst vervolgens of de vergunningsaanvraag voldoet aan de eisen van de AVG.
Wij stellen vast dat de Nederlandse wetgever nog maar kort geleden – de UAVG is op 25 mei 2018 in werking getreden- voor deze weg heeft gekozen. Op deze wijze, dus mèt een toetsende rol van de AP of de voorgenomen gegevensdeling voldoet aan de uitgangspunten en normen van het Nederlandse gegevensbeschermingsrecht, zijn de privacybelangen van betrokkenen geborgd. Dit betekent echter geenszins dat een (potentiele) fraudeur zich kan verschuilen achter die privacyregels. Cross-sectorale gegevensdeling tussen private partijen is mogelijk, zoals ook de onderzoekers hebben aangegeven. Het is aan de private partijen, die voornemens zijn om cross-sectoraal gegevens uit te wisselen om fraude te voorkomen, om overeenkomstig de wettelijke kaders daarvoor vergunning van de AP te verkrijgen.

Tijdens de behandeling van het voorstel voor de UAVG heeft de minister voor Rechtsbescherming uw Kamer toegezegd direct na afronding van dit wetsvoorstel de mogelijkheden te verkennen voor verdere modernisering en verbetering van het gegevensbeschermingsrecht. In lijn met deze toezegging heeft hij toen ook de motie Koopmans c.s. overgenomen, waarin de regering werd verzocht de ervaringen met betrekking tot de UAVG te inventariseren en in het licht daarvan zo nodig maatregelen te treffen[2]. Eén van de kwesties uit de motie betreffen de privacyaspecten rond het branchebreed aanleggen van zwarte lijsten van fraudeurs.
In zijn brief van 1 april 2019[3] heeft de minister voor Rechtsbescherming aangegeven dat het delen van zogenaamde zwarte lijsten van fraudeurs tússen branches (in deze brief aangeduid als het cross-sectoraal delen van gegevens tussen private partijen) op basis van de UAVG mogelijk is. Hiervoor is, zoals ook de onderzoekers aangeven, een vergunning van de AP nodig.
Op het voorstel van VNO-NCW en MKB Nederland in een brief van 19 september 2018 om de UAVG te wijzigen in die zin dat de UAVG een expliciet wettelijke grondslag zal bevatten voor het cross-sectoraal uitwisselen van gegevens over fraudeurs, geeft de minister voor Rechtsbescherming aan dat er eerst ervaringen moeten zijn opgedaan met de huidige wijze waarop gegevensdeling in de UAVG is geregeld voordat er aanleiding kan zijn om wijziging van de UAVG te overwegen. Daarbij heeft hij aangegeven samen met VNO-NCW en MKB Nederland in gesprek te zullen gaan met de AP over de betekenis van de nieuwe toepasselijke aanvraagprocedure voor nieuwe aanvragen voor cross-sectorale uitwisseling van gegevens over fraudeurs. Dit gesprek heeft plaatsgevonden op 6 juni jl. In dit gesprek werd bevestigd dat cross-sectorale uitwisseling van strafrechtelijke gegevens op basis van een door de AP te verlenen vergunning mogelijk is, als deze uitwisseling noodzakelijk is met het oog op een zwaarwegend belang van bepaalde private partijen en is voorzien in voldoende waarborgen dat personen niet ten onrechte op bijvoorbeeld een zwarte lijst komen te staan. In het licht van de eisen van noodzakelijkheid, subsidiariteit en proportionaliteit moet de vergunningaanvraag goed zijn onderbouwd en dienen de waarborgen steviger te zijn naarmate de scope van de lijst en de impact van plaatsing daarop groter zijn. Tegen deze achtergrond is denkbaar dat een vergunningaanvraag wordt ingediend voor de uitwisseling van strafrechtelijke gegevens ten behoeve van de aanpak van bijvoorbeeld vastgoedfraude door naast betrokken partijen, zoals

[2] Kamerstukken II 2017/18, 34 851, nr. 19
[3] Kamerstukken II 2018/19, 32 761, nr. 132 p. 9

notarissen, makelaars, banken en pandeigenaren, die aan deze vereisten voldoet. Een dergelijke vergunningaanvraag zou op eenzelfde leest kunnen worden gestoeld als het te actualiseren Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (Pifi) dat gegevensuitwisseling tussen banken en verzekeraars mogelijk maakt om de continuïteit en integriteit van deze twee sectoren te bewaken. Het gesprek heeft op deze wijze over en weer verhelderd waartoe een vergunningaanvraag zou kunnen dienen en aan welke eisen deze dient te voldoen.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum
11 juni 2019

Ons kenmerk
2621849

Wij wachten de ervaringen die door private organisaties worden opgedaan met hun voornemen tot cross-sectorale gegevensdeling ten behoeve van fraudebestrijding en eventuele daarbij spelende knelpunten binnen het huidige wettelijke privacy-kader af. Afhankelijk van die ervaringen zal zo nodig nieuwe wetgeving kunnen worden overwogen.

Tot slot

Horizontale fraude veroorzaakt grote schade en het voorkomen daarvan is van groot belang. Het delen van gegevens over fraudeurs tussen private (en publieke) partijen kan daarbij noodzakelijk zijn. Dit dient echter altijd te gebeuren binnen de in Nederland geldende privacywetgeving. Of het huidig wettelijk kader, dat op dit moment voorziet in het door de wetgever gewenste beschermingsniveau van betrokkenen, met het oog op fraudebestrijding en daarvoor benodigde cross-sectorale gegevensdeling, aangepast zou moeten worden, is mede afhankelijk van de ervaringen die door de betrokken (private) organisaties nog opgedaan moeten worden. Die ervaringen wachten wij af.

De minister voor Rechtsbescherming,

Sander Dekker

De minister van Justitie en Veiligheid,

Ferd Grapperhaus