AUTORITEIT
PERSOONSGEGEVENS

Datum
8 oktober 2021

Ons kenmerk
z2021-12791

# Besluit inzake de vergunningaanvraag voor de verwerking van persoonsgegevens van strafrechtelijke aard ten behoeven van derden van de verwerking 'Frauderegistratiesysteem' van de Vereniging Veilig Ondernemen Door Informatie Op Maat (VODIOM); z2021-12791

## 1 – Inleiding: aanleiding vergunningaanvraag

1. Op 5 juli 2021 heeft de vereniging VODIOM– ingevolge artikel 33, vierde lid, aanhef en onder c, van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) – aan de Autoriteit Persoonsgegevens (AP) de vergunningaanvraag over *cross-sectorale gegevensdeling t.b.v. fraudebestrijding (Frauderegistratiesysteem)* overhandigd. Deze aanvraag is bij de AP bekend onder z2021-12791 onder de naam 'Vergunning VODIOM'. Ter onderbouwing van de aanvraag heeft de vereniging VODIOM een protocol d.d. 5 juli 2021 en een data protection impact assessment (gegevensbeschermingseffect-beoordeling, ook wel DPIA genoemd) d.d. 12 maart 2021 (zoals gemaild op 9 juli 2021) bijgevoegd. Het aanvraagformulier is op 20 juli 2021 per post nagezonden op verzoek van de AP. Ook heeft de vereniging VODIOM een Deelnemersreglement Frauderegistratiesysteem d.d. 5 juli 2021 bijgevoegd.

2. Op grond van artikel 33, vierde lid, aanhef en onder c, UAVG mogen persoonsgegevens van strafrechtelijke aard ten behoeve van derden worden verwerkt indien de AP een vergunning voor de verwerking heeft verleend. Ingevolge artikel 33, vijfde lid, UAVG kan een vergunning slechts 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 de betrokkene niet onevenredig wordt geschaad. Aan de vergunning kunnen door de AP voorschriften worden verbonden.

3. In het navolgende concludeert de AP dat er geen vergunning voor de verwerking van gegevens van strafrechtelijke aard ten behoeve van derden kan worden verleend, omdat de door VODIOM beoogde verwerking van strafrechtelijke persoonsgegevens van vermoedelijke fraudeurs ten behoeve van derden in strijd is met het subsidiariteitsbeginsel en het proportionaliteitsbeginsel, en daarmee niet noodzakelijk is met het oog op een zwaarwegend belang van derden.

## 2 – Procedureverloop

4. Op 15 december 2020 is de vergunningaanvraag met zaaknummer z2020-21313 ingediend door de vereniging VODIOM.

5. Op 21 januari 2021 heeft de AP met de vereniging VODIOM overlegd over deze vergunningaanvraag. Daarbij heeft de AP aangegeven dat de vergunningaanvraag op fundamentele inhoudelijke punten niet voldoet aan de eisen die voortvloeien uit de (U)AVG en dat de vergunningaanvraag - zoals ingediend op 15 december 2020 – zal worden afgewezen.

6. Per e-mail van 22 januari 2021 heeft de AP de fundamentele inhoudelijke punten opgesomd die in elk geval nog qua motivering aangevuld moeten worden en daarbij mogelijke procesafspraken voorgesteld.

7. Op 27 januari 2021 heeft de vereniging VODIOM schriftelijk laten weten dat de vergunningaanvraag met zaaknummer z2020-21313 wordt ingetrokken.

8. Op 28 januari 2021 heeft de AP schriftelijk bevestigd dat de vergunningaanvraag met zaaknummer z2020-21313 is ingetrokken.

9. Op 23 juni 2021 heeft MKB-NL – namens vereniging VODIOM - informeel laten weten dat de aangepaste/aangevulde vergunningaanvraag begin juli 2021 ingediend zal worden.

10. Op 24 juni 2021 heeft de AP (informeel) laten weten dat binnen afzienbare tijd de *Handreiking cross-sectorale gegevensdeling* gepubliceerd zal worden. In deze handreiking wordt ingegaan op de problematiek van de vergunningaanvraag van vereniging VODIOM. Door de AP is geadviseerd om deze handreiking af te wachten en (ná publicatie daarvan) de punten uit deze handreiking te verwerken in de nog in te dienen vergunningaanvraag.

11. Op 24 juni 2021 heeft de MKB-NL – namens vereniging VODIOM - aangegeven dat zij hierop niet kan wachten. Daarop heeft de AP de concept-handreiking onder embargo gedeeld, zodat de punten uit de handreiking nog verwerkt kunnen worden in de nog in te dienen vergunningaanvraag.

12. Op 5 juli 2021 is de vergunningaanvraag van vereniging VODIOM met zaaknummer z2021-12791 over cross-sectorale gegevensdeling t.b.v. fraudebestrijding (Frauderegistratiesysteem) overhandigd door Els Prins (secretaris MKB-Nederland) en Jacco Vonhof (voorzitter MKB-Nederland) aan Monique Verdier (vicevoorzitter AP).

13. Op 9 juli 2021 heeft vereniging VODIOM een aangepaste vergunningaanvraag toegestuurd, waarbij de correcte versie van de DPIA is toegevoegd.

14. Op 15 juli 2021 heeft de AP schriftelijk aangegeven dat de vergunningaanvraag incompleet is, omdat het aanvraagformulier ontbreekt bij de stukken. De AP heeft de termijn opgeschort totdat het aanvraagformulier is aangeleverd.

15. Op 20 juli 2021 heeft vereniging VODIOM de vergunningaanvraag aangevuld met het aanvraagformulier.

16. Op 3 september 2021 heeft de AP uitstel aangevraagd voor de behandeling van deze vergunningaanvraag.

## 3 – Feitelijke weergave van de voorgenomen verwerking

### Inleiding

17. Om de directe schade van fraude voor de betrokken partijen terug te dringen en de maatschappelijke impact van fraude te verkleinen, zijn de partijen voornemens om een zogenaamd '*Frauderegistratiesysteem*' in te richten. Het initiatief voor het inrichten van het Frauderegistratiesysteem ligt bij vereniging VODIOM. Vereniging VODIOM is een initiatief van MKB-Nederland, VNO-NCW en Fleur van Eck. Het initiatief wordt ondersteund door Vereniging COIN[1], Thuiswinkel.org en Currence[2], omdat de achterban van deze organisaties en hun klanten slachtoffer zijn van fraude.[3]

18. Het Frauderegistratiesysteem dient de volgende (zwaarwegende) belangen: (1) bescherming van de betrouwbaarheid en de integriteit van het handels verkeer, (2) de bescherming van consumenten/burgers tegen fraude en (3) de bescherming van de Deelnemers tegen fraude. Meer specifiek heeft het Frauderegistratiesysteem tot doel te voorkomen dat Deelnemers slachtoffer worden van fraudeurs die al eerder aangiftewaardige fraudehandelingen hebben gepleegd bij een of meerdere andere Deelnemers. Het Frauderegistratiesysteem moet:
a) Deelnemers die slachtoffer zijn geworden van fraude of wier dienstverlening wordt misbruikt voor fraude in staat stellen om andere Deelnemers voor soortgelijke fraude en/of misbruik van dienstverlening te behoeden; en
b) Deelnemers wier dienstverlening wordt misbruikt voor frauduleuze doeleinden beter in staat stellen daar onderzoek naar te doen.[4]

19. In het Frauderegistratiesysteem wil men relevante gegevens betreffende fraudegevallen tussen verschillende sectoren delen. In de aanvraag van de vereniging VODIOM gaat het om de sectoren betaalindustrie, online retail en telecommunicatie.[5] In het bijzonder gaat het om (identificerende) gegevens van de vermoedelijke fraudeplegers zoals naam, adres en woonplaats.[6] Het systeem is primair gericht op het delen van gegevens betreffende vormen van fraude die voortkomen uit misbruik van identificerende gegevens.[7] De partijen zijn voornemens om het systeem te vullen met persoonsgegevens die verband houden met '*aangiftewaardige frauduleuze activiteiten*'.[8]

20. Het Frauderegistratiesysteem kan alleen worden gevuld met de door de organisaties overeengekomen set van persoonsgegevens. Het kan hierbij gaan om fraude die is gepleegd door individuen of

[1] Vereniging COIN is een samenwerking van Nederlandse aanbieder van elektronische communicatiediensten en –netwerken.
[2] Currence is merkeigenaar van iDEAL, iDIN, Incassogemachtigden en Acceptgiro en faciliteert marktwerking met kwaliteit en veiligheid van betalingsverkeer.
[3] Zie: DPIA VODIOM, p. 7
[4] Zie: Protocol, p. 9.
[5] Zie: DPIA VODIOM, p. 4.
[6] Zie: DPIA VODIOM, p. 6.
[7] Zie: DPIA VODIOM, p. 7.
[8] Zie: DPIA VODIOM, p. 7.

bedrijven.[9] Daarbij wordt de aard van de frauduleuze activiteit vermeld. Deze persoonsgegevens worden opgeslagen in het frauderegistratiesysteem en kunnen op aanvraag inzichtelijk worden gemaakt voor de deelnemende organisaties wanneer dit noodzakelijk wordt geacht.[10] De gegevensdeling kan alleen plaatsvinden tussen organisaties die lid worden van de vereniging VODIOM.[11]

21. Het beheer van het Frauderegistratiesysteem zal worden uitgevoerd door vereniging VODIOM. Het gaat hierbij specifiek om de inrichting van de database. Vereniging VODIOM draagt ook zorg voor het beleid op van het gebruik van het frauderegistratiesysteem.[12]

22. Voor de technische en organisatorische maatregelen zijn de partijen voornemens om aan te sluiten bij CIFAS, een frauderegistratiesysteem dat in het Verenigd Koninkrijk gebruikt wordt.[13] Het daadwerkelijke beheer wordt verzorgd door het Engelse CIFAS in de hoedanigheid van verwerker. De vereniging VODIOM is voornemens een licentie af te nemen van het Engelse CIFAS voor een Nederlandse versie daarvan (software as a service).[14] Onder randnummers 45 tot en met 53 volgt meer hierover.

### Betrokkenen

23. De persoonsgegevens die worden geregistreerd in het frauderegistratiesysteem betreffen verschillende categorieën betrokkenen:
    a) fraudeurs (waaronder ook begrepen katvangers[15]);
    b) (potentiële) slachtoffers (personen met een beschermde status).[16]

24. Ook worden er gegevens van medewerkers van de vereniging VODIOM en de deelnemende organisaties geregistreerd omdat zij het frauderegistratiesysteem gebruiken.[17]

### Persoonsgegevens

25. Bij het aanmelden van een zaak dienen de volgende persoonsgegevens te worden geregistreerd over de fraudeurs en katvanger(s):[18]
    a) naam (voornaam en achternaam);
    b) initialen;
    c) (aflever)adres (woonplaats, postcode, straatnaam en huisnummer);
    d) naam rechtspersoon;
    e) KvK nummer;

[9] Zie: DPIA VODIOM, p. 8.
[10] Zie: DPIA VODIOM, p. 7.
[11] Zie: DPIA VODIOM, p. 8.
[12] Zie: DPIA VODIOM, p. 8.
[13] Zie: DPIA VODIOM, p. 7.
[14] Zie: DPIA VODIOM, p. 8.
[15] Volgens de vereniging VODIOM maken fraudeurs veelal gebruik van katvangers die hen bewust helpen de fraude te plegen. De vereniging VODIOM schaart katvangers daarmee ook onder het begrip 'fraudeur' en registreert ook katvangers in het frauderegistratiesysteem.
[16] Zie: DPIA VODIOM, p. 10.
[17] Zie: DPIA VODIOM, p. 10.
[18] Zie: DPIA VODIOM, p. 13 en bijlage 2 van het Protocol.

f) telefoonnummer;
g) e-mailadres;
h) accountnaam / gebruikersnaam;
i) IP-adres;
j) apparaat gegevens (type, MAC-adres);
k) IBAN/rekeningnummer;
l) Geboortedatum;
m) documentnummer identiteitsbewijs, paspoort, rijbewijs, id-kaart.

26. Naast deze persoonsgegevens worden ook gegevens over het fraudegeval zelf (de modus operandi) opgeslagen:
    a) gegevens order / bestelling / dienst;
    b) aard / type fraude (beschrijving vormen van fraude);
    c) indicatie van de ernst / omvang van de fraude.

### Geregistreerde fraudevormen

27. In de DPIA staat vermeld dat fraude voor vereniging VODIOM een vorm van oplichting is waarbij bepaalde zaken anders worden voorgedaan dan dat ze daadwerkelijk zijn om daar voordeel uit te behalen. Om van fraude te spreken moet het gaan om een opzettelijke handeling waarbij een fraudeur gebruik maakt van een valse naam of hoedanigheid, een listige kunstgreep of kunstgrepen en/of een samenweefsel van verdichtsels met het oogmerk zich ten koste van anderen te bevoordelen dan wel te verrijken.[19]

28. Er is naar het oordeel van vereniging VODIOM sprake van fraude wanneer:
    a) opzettelijk is gehandeld;
    b) een misleidende voorstelling van zaken is gegeven;
    c) met het oogmerk economisch voordeel te behalen;
    d) er een benadeelde is; en
    e) sprake is van onrechtmatig of onwettig handelen.

    Als aan deze elementen (cumulatief) wordt voldaan is sprake van fraude. De fraudevormen die relevant zijn beperken zich tot horizontale fraude, met een specifieke focus op fraude gericht tegen bedrijven en fraude gericht op consumenten (waar bedrijven ook door gedupeerd kunnen worden).[20]

29. Het Frauderegistratiesysteem is bedoeld om informatie te delen tussen de aangesloten organisaties ten behoeve van de bestrijding van fraude die wordt gepleegd door individuen of bedrijven. De fraudezaken die opgenomen worden in het frauderegistratiesysteem, hebben betrekking op zaken waarbij een fraudeur (al dan niet geholpen door een katvanger) deelnemers heeft opgelicht dan wel tracht op te lichten. VODIOM benoemt de volgende primaire verschijningsvormen van fraude die in het frauderegistratiesysteem kunnen worden geregistreerd:[21]
    a) Overname van faciliteiten;
    b) Misbruik van faciliteiten;

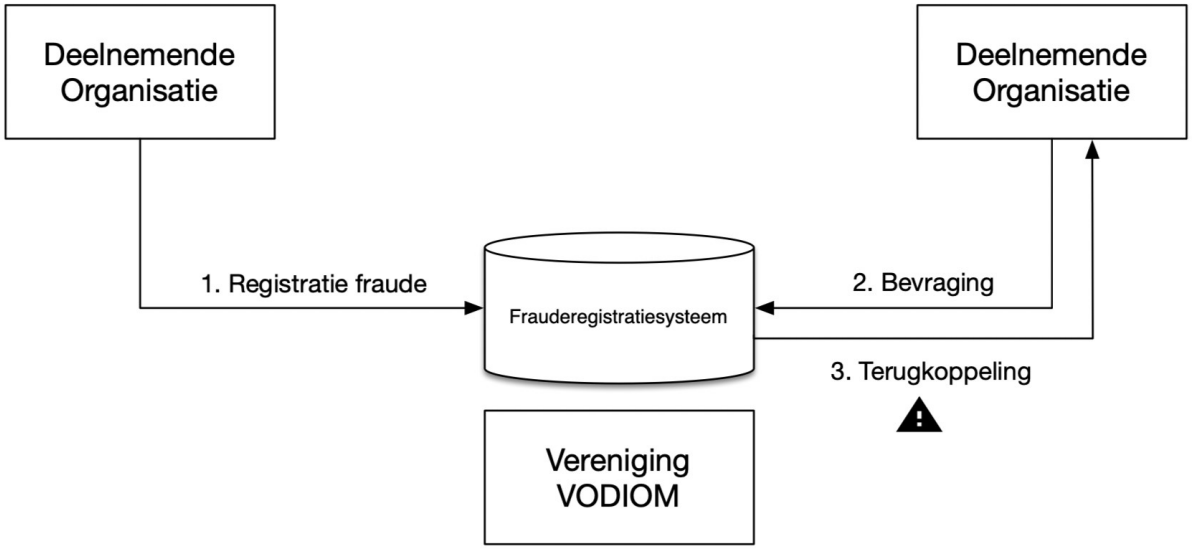
[19] Zie: DPIA VODIOM, p. 5-9.
[20] Zie: DPIA VODIOM, p. 5-9.
[21] Zie: DPIA VODIOM, p. 5-9.

c) Misbruik van gegevens;
d) Opzettelijke niet-nakoming.

Deze vormen van fraude zijn strafbaar gesteld in de titels XII en XXV van het Wetboek van Strafrecht. De deelnemers beperken zich tot de registratie van fraudeurs tot die gevallen waarbinnen het handelen van de fraudeurs past binnen de delictsomschrijvingen uit deze titels.[22]

### Procedurebeschrijving gegevensverwerking - frauderegistratiesysteem[23]

30. Het Frauderegistratiesysteem kent twee componenten: het registreren van gegevens betreffende fraudeurs door deelnemers en de raadpleging door deelnemers. Hieronder volgt de schematische weergave van de inrichting van het Frauderegistratiesysteem[24] en een toelichting van de vereniging VODIOM hierop.




### Stap 1 – interne registratie fraude

31. Wanneer een deelnemer een vermoeden van fraude heeft, onderzoekt de deelnemer de fraude en registreert de bevindingen in zijn eigen administratie (bronregistratie). Indien er voldoende zekerheid is over het voorval doet de deelnemer aangifte, waarna ook kan worden overgegaan tot registratie in het Frauderegistratiesysteem.[25] De deelnemer mag alleen persoonsgegeven van een betrokkene registreren in het Frauderegistratiesysteem wanneer aan de bewijslast is voldaan.[26] Volgens het protocol[27] is er aan de bewijslast voldaan als:
    a) er gerede vermoedens zijn dat fraude is of wordt gepleegd, dan wel dat gepoogd is of wordt gepoogd fraude te plegen;
    b) deze vermoedens zijn onderbouwd met duidelijk bewijs;

[22] Zie: Protocol Frauderegistratiesysteem, p. 9-11.
[23] Zie: Protocol Frauderegistratiesysteem, p. 12-15 en DPIA VODIOM, p. 11-17.
[24] Zie: DPIA VODIOM, p. 21.
[25] Zie: Protocol Frauderegistratiesysteem, p. 12.
[26] Zie: Protocol Frauderegistratiesysteem, p. 12.
[27] Zie: Protocol Frauderegistratiesysteem, p. 12.

c) de gedraging moet worden gekwalificeerd als één van de vier vormen van fraude waarop het frauderegistratiesysteem betrekking heeft en vallen binnen de delictsomschrijvingen van Titel XII en XXV van het Wetboek van Strafrecht;
d) de fraude is gepleegd in de context van het aanbieden of afnemen van goederen of diensten en/of de logistieke of financiële afhandeling daarvan;
e) er door de deelnemer aangifte is gedaan van de fraude;
f) een dossier als 'aangifte waardig' is geregistreerd; dat wil zeggen dat de bewijsvoering dusdanig moet zijn dat er genoeg informatie is om een aangifte te kunnen doen;
g) het economisch nadeel van de fraude voor de Deelnemer of diens klanten hoger is dan €250,- dan wel potentieel hoger dan €250,-;
h) een registratie alleen is opgenomen wanneer dit bij de Deelnemer heeft geleid tot een concrete actie zoals: het afwijzen van een aanvraag, het intrekken van een aanbod, of het stopzetten van de en/of toekomstige levering van producten of diensten, of het instellen van een civiele actie (formele brief, verweerschrift, incassokantoor, deurwaarder) of een concrete rechtsvordering; tenzij een (wettelijke) plicht zich hiertegen verzet; of de fraudeur reeds het volledige voordeel heeft ontvangen;
i) de Deelnemer heeft de persoonsgegevens betreffende de fraudeur reeds vastgelegd in de eigen Bronregistratie.

**Stap 2 – bevraging bij vermoeden van fraude**

32. Een deelnemende organisatie kan het Frauderegistratiesysteem bevragen als de organisatie het vermoeden heeft dat er sprake is van een (poging) tot fraude, of dat de transactie van dusdanige aard is dat het (vermogens-)risico aanzienlijk is. Er kan worden gezocht op basis van de volgende criteria:[28]
    a) voornaam (of initialen) en achternaam;
    b) adres (postcode en huisnummer);
    c) bankrekeningnummer;
    d) documentnummer van een identiteitsbewijs;
    e) e-mailadres;
    f) IP-adres.

33. Alle bevragingen worden gelogd. De bevragende organisatie moet aangeven voor welk doel het systeem wordt bevraagd.[29]

**Stap 3 – terugkoppeling bevraging Frauderegistratiesysteem**

34. Na het raadplegen van het systeem kan er sprake zijn van een hit/no hit resultaat of een volledig overzicht van de resultaten. Dit is afhankelijk van wie het systeem bevraagt. Uitsluitend medewerkers (van de deelnemers) die als taak fraudebestrijding/veiligheidszaken hebben en over voldoende kwalificaties beschikken kunnen de achterliggende gegevens binnen het systeem raadplegen en krijgen dus een volledig overzicht te zien.[30]

[28] Zie: DPIA VODIOM, p. 15.
[29] Zie: DPIA VODIOM, p. 16.
[30] Zie: DPIA VODIOM, p. 17.

## 4 – Wettelijk kader

### 4.1 Verwerking van persoonsgegevens van strafrechtelijke aard ten behoeve van derden.

Artikel 10 AVG bepaalt: "Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen op grond van artikel 6, lid 1, alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid."

Artikel 1 UAVG bepaalt: "In deze wet en de daarop berustende bepalingen wordt verstaan onder:
[…]
Persoonsgegevens van strafrechtelijke aard: persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de verordening, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag; […]"

Artikel 31 UAVG bepaalt: "Onverminderd artikel 10 van de verordening mogen persoonsgegevens van strafrechtelijke aard alleen worden verwerkt voor zover dit krachtens de artikelen 32 en 33 is toegestaan."

Artikel 33, vierde lid, aanhef en onder c, UAVG bepaalt: "Persoonsgegevens van strafrechtelijke aard mogen ten behoeve van derden worden verwerkt:
[…]
c. indien de Autoriteit persoonsgegevens met inachtneming van het vijfde lid een vergunning voor de verwerking heeft verleend."

Artikel 33, vijfde lid, UAVG bepaalt: "Een vergunning als bedoeld in het vierde lid, onderdeel c, kan slechts 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 de betrokkene niet onevenredig wordt geschaad. Aan de vergunning kunnen voorschriften worden verbonden."

## 5 – Beoordeling van de voorgenomen verwerking

35. De AP beperkt zich in het kader van de beoordeling van een vergunningaanvraag tot de beoordeling van de verwerking van persoonsgegevens van strafrechtelijke aard ten behoeve van derden, zoals omschreven in het wettelijk kader. De beoordeling is gebaseerd op de aan de verwerking ten grondslag liggende vergunningaanvraag, de met vereniging VODIOM gevoerde overleggen, het protocol Frauderegistratiesysteem (versie 5 juli 2021), de gegevensbeschermingseffectbeoordeling (DPIA) (versie 9 juli 2021) en het deelnemersreglement (versie 5 juli 2021).

36. De AP heeft geen onderzoek (ter plaatse) gedaan naar de werkwijze en de praktijk van vereniging VODIOM voorafgaand aan de vergunningsaanvraag en baseert zich op de thans voorgelegde documenten.

37. Deze vergunningsaanvraag en de beoordeling daarvan zien daarom uitsluitend op hetgeen is omschreven in de "*Procedurebeschrijving gegevensverwerking – frauderegistratiesysteem*" van dit besluit. Ofwel: vanaf het moment ná de interne registratie, indien er voldoende zekerheid is over het voorval en de deelnemer aangifte heeft gedaan, waarna ook kan worden overgegaan tot registratie in het Frauderegistratiesysteem. Vanaf dit moment is sprake van de verwerking van strafrechtelijke gegevens ten behoeve van derden, waarvoor een AP-vergunning vereist is.

### Verwerkingsverantwoordelijkheid

38. In het protocol staat vermeld: "*Voor de invoer van de Persoonsgegevens zijn de Deelnemer en de vereniging VODIOM gezamenlijk Verwerkingsverantwoordelijke. Dit omdat de Deelnemer en VODIOM gezamenlijk doel en middelen voor de registratie bepalen. Voor de opslag en het beheer van de Persoonsgegevens in het Frauderegistratiesysteem is de vereniging VODIOM zelfstandig verwerkingsverantwoordelijke. Dit omdat VODIOM doel en middelen voor de opslag en het beheer zelfstandig bepaalt, zonder directe invloed van individuele Deelnemers. Voor de raadpleging van de Persoonsgegevens zijn de vereniging VODIOM en de bevragende Deelnemer gezamenlijk Verwerkingsverantwoordelijke. Dit omdat de Deelnemer en VODIOM gezamenlijk doel en middelen voor de bevraging bepalen.*"[31]

39. In het Deelnemersreglement staat vermeld: "*De Deelnemer die Persoonsgegevens invoert in het Frauderegistratiesysteem en de Vereniging VODIOM zijn gezamenlijk verwerkingsverantwoordelijke voor de individuele registratie en opname in het Frauderegistratiesysteem. De bevragende Deelnemer en de Vereniging VODIOM zijn gezamenlijk verwerkingsverantwoordelijke voor een individuele bevraging.*"[32]

40. Uit het voorgaande blijkt dat voor de verschillende verwerkingen verschillende (gezamenlijke) verwerkingsverantwoordelijken zijn:
    a) invoer gegevens deelnemer: VODIOM en invoerende deelnemer zijn gezamenlijk verwerkingsverantwoordelijk.
    b) opslag en beheer gegevens: VODIOM is verwerkingsverantwoordelijke.
    c) raadpleging gegevens: VODIOM en de raadplegende deelnemer zijn gezamenlijk verwerkingsverantwoordelijk.

41. Een verwerkingsverantwoordelijke is conform artikel 4, aanhef, onder 7, van de AVG verwerkingsverantwoordelijk voor een '*verwerking van persoonsgegevens*' en stelt '*het doel van en de middelen voor de verwerking van persoonsgegevens*' vast. In artikel 4, aanhef, onder 2, van de AVG wordt 'verwerking' gedefinieerd als "*een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens* (…)."

42. Hoewel door VODIOM wordt aangegeven dat er een diverse schakering is van (gezamenlijke) verwerkingsverantwoordelijken (zie de voorgaande randnummers) voor de diverse stappen van de gegevensverwerking in het Frauderegistratiesysteem, wordt onvoldoende aannemelijk gemaakt dat de invoerende en raadplegende deelnemers doel en middelen bepalen en daarmee gezamenlijk verwerkingsverantwoordelijken kunnen zijn voor de gegevensverwerking in het Frauderegistratiesysteem.

[31] Zie: Protocol Frauderegistratiesysteem, p. 5 en 18.
[32] Zie: Deelnemersreglement Frauderegistratiesysteem, p. 9.

43. Het voorgaande blijkt o.a. uit de volgende handelingen:
    a) VODIOM heeft het initiatief genomen tot de inrichting van het Frauderegistratiesysteem.[33]
    b) VODIOM is verantwoordelijk voor de organisatorische inrichting van het Frauderegistratiesysteem.[34]
    c) VODIOM heeft daartoe onder meer criteria opgesteld wanneer een fraudegeval geregistreerd mag worden in het Frauderegistratiesysteem.[35]
    d) VODIOM heeft bepaald welke persoonsgegevens geregistreerd mogen worden.[36]
    e) VODIOM heeft bepaald op welke manier het Frauderegistratiesysteem geraadpleegd moet worden.[37]
    f) VODIOM heeft bepaald op welke manier toegang tot het Frauderegistratiesysteem kan worden verkregen en welke deelnemer aanspraak heeft op de hit/no hit resultaat of een volledig overzicht van de resultaten mag ontvangen.[38]
    g) VODIOM heeft het '*Deelnemersreglement Frauderegistratiesysteem (5 juli 2021)*' opgesteld en daarmee bepaald wat o.a. de toetredingscriteria zijn voor deelnemers.

44. Uit de documenten komt zodoende naar voren dat VODIOM doel en middelen bepaalt voor de genoemde verwerkingen in het Frauderegistratiesysteem, en daarmee derhalve kwalificeert als (enige) verwerkingsverantwoordelijke. Uit de toegezonden documenten blijkt niet dat de invoerende en raadplegende deelnemers doel en middelen voor de gegevensverwerking in het Frauderegistratiesysteem bepalen.

### Grensoverschrijdend karakter (verwerker)

45. Het vergunningsinstrument uit de UAVG is een nationale implementatie van de uitzondering op artikel 10 AVG. Derhalve kan de vergunning geen transnationale werking hebben.

46. Uit de documenten blijkt dat er sprake is van grensoverschrijdende verwerkingen. In het aanvraagformulier wordt aangegeven dat er gebruik zal worden gemaakt van een Engelse verwerker: CIFAS. Deze verwerker is gevestigd in het Verenigd Koninkrijk.

47. In het Protocol staat het volgende vermeld: "*CIFAS is de verwerker. CIFAS is gevestigd in het Verenigd Koninkrijk. Een verwerkersovereenkomst zal hiertoe worden afgesloten en mocht een adequaatheidsbesluit van de Europese Commissie uitblijven, zal ook een SCC worden gesloten en aanvullende maatregelen worden getroffen. In dit kader is het van belang te noemen dat de EDPB nog met een update komt van haar aanbevelingen voor te treffen aanvullende maatregelen.*"[39]

48. Verderop in het Protocol staat het volgende vermeld: "*De Persoonsgegevens worden verwerkt door CIFAS. De Persoonsgegevens worden opgeslagen op de beveiligde infrastructuur van CIFAS in het Verenigd Koninkrijk. VODIOM treft maatregelen om de doorgifte van deze Persoonsgegevens naar het Verenigd Koninkrijk als derde land*

[33] Zie: DPIA, p. 7-8.
[34] Zie: DPIA, p. 11-21.
[35] Zie: DPIA, p. 11-12.
[36] Zie: DPIA, p. 12-15.
[37] Zie: DPIA, p. 15-16.
[38] Zie: DPIA, p. 16-17.
[39] Zie: Protocol Frauderegistratiesysteem, p. 5.

*te legitimeren. Ten tijde van het schrijven van dit protocol is de situatie met betrekking tot de status van het Verenigd Koninkrijk vanuit AVG-perspectief ongewis."*[40]

49. Nu het Verenigd Koninkrijk sinds 28 juni 2021 de '*adequacy status*' heeft verkregen, hetgeen betekent dat persoonsgegevens vrijelijk mogen worden doorgegeven zonder gebruik te hoeven maken van doorgifte instrumenten, is de verwerking door de verwerker in het Verenigd Koninkrijk toegestaan.[41]

*Doorgifte naar derde landen (Microsoft)*

50. In de aangeleverde documenten wordt verder aangegeven dat: "*De Persoonsgegevens in het Frauderegistratiesysteem zijn opgeslagen in een aparte beveiligde database (tenant) bij verwerker CIFAS. Deze database wordt gehost in de Microsoft Azure Cloud. Zowel CIFAS als Microsoft zijn ISO27001 gecertificeerd. Bluecube beheert de remote desktop omgeving waarmee ingelogd kan worden op de CIFAS-omgeving. Ook Bluecube is ISO27001 gecertificeerd en als sub-verwerker gebonden aan dezelfde regels als CIFAS als verwerker*."[42]

51. Microsoft is een Amerikaans bedrijf waar de Amerikaanse wetgeving van toepassing is. Wanneer de data door Microsoft worden opgeslagen buiten de EU, dan geldt (op dit moment) in navolging van de Schrems II uitspraak van het CJEU dat doorgifte naar een derde land - in dit geval: Amerika - pas mogelijk is als er voldoende waarborgen zijn getroffen. Het enkel gebruiken van een doorgifte-instrument (in deze beschreven situatie is er een adequacy status voor de VK, zie randnummer 50), zoals genoemd in artikel 46 van de AVG, niet voldoende. Er moet daarnaast ook een analyse van het beschermingsniveau gemaakt worden en indien noodzakelijk moeten er aanvullende maatregelen getroffen worden.[43]

52. De additionele mitigerende maatregelen die de vereniging VODIOM in paragraaf 5.3.5. van de DPIA voorstelt hadden aldus per definitie al genomen kunnen worden.

53. In het protocol zijn verder geen aanwijzingen gevonden dat er een studie is gemaakt van het beschermingsniveau van Amerika, noch is er sprake van een '*standard contractual clauses*' met aanvullende maatregelen voor de doorgifte van persoonsgegevens naar Amerika. Het protocol voldoet daarmee - gelet op de vereisten in AVG en Recommendations - op dit punt niet aan de AVG, voor zover het dataopslag betreft via de Microsoft Azure Cloud in de Verenigde Staten.

## Opzet van de beoordeling

54. De beoordeling wordt hierna op de volgende manier vorm gegeven: allereerst wordt er gekeken naar de mate van verwerking van persoonsgegevens van strafrechtelijke aard (paragraaf 5.1). Als er geen

[40] Zie: Protocol Frauderegistratiesysteem, p. 20-21.
[41] URL: https://autoriteitpersoonsgegevens.nl/nl/nieuws/nieuw-modelcontract-voor-veilige-doorgifte-persoonsgegevens.
[42] Zie: Protocol, p. 19-21.
[43] URL: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/recommendations_on_measures_that_supplement_transfer_tools_to_ensure_compliance_with_the_eu_level_of_protection_of_personal_data.pdf. *"The Court states that controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. In those cases, the Court still leaves open the possibility for exporters to implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law."*

sprake is van persoonsgegevens van strafrechtelijke aard die verwerkt worden ten behoeve van derden, dan is de verwerking niet vergunningplichtig. Vervolgens wordt de verwerking getoetst aan artikel 33, vijfde lid, UAVG, dat wil zeggen (1) is de verwerking noodzakelijk voor een zwaarwegend belang van derden (paragraaf 5.2) en (2) is in zodanige waarborgen voorzien dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.

## 5.1 Verwerken van persoonsgegevens van strafrechtelijke aard

### 5.1.1 Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.

55. Het begrip 'persoonsgegevens van strafrechtelijke aard' valt uiteen in enerzijds de in de AVG genoemde persoonsgegevens van strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen en anderzijds de in de UAVG genoemde persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag. Het begrip heeft blijkens de wetsgeschiedenis zowel betrekking op 'de toepassing van het formele strafrecht', als op 'min of meer gegronde verdenkingen'.[44] Volgens vaste rechtspraak wordt onder strafrechtelijke persoonsgegevens verstaan "zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring - in de zin van artikel 350 van het Wetboek van Strafvordering - kunnen dragen."[45]

56. Uit de ingediende stukken blijkt welke persoonsgegevens en/of categorieën van persoonsgegevens zullen worden verwerkt in het frauderegistratiesysteem.[46] Hierbij gaat het onder meer om naam, adres, telefoonnummer, emailadres en KvK-nummer van de vermoedelijk fraudeur. Het systeem is op die manier ingericht dat individuen te identificeren en traceren zijn. Bovendien worden deze individuen gelinkt aan (een poging tot) frauduleus handelen en worden zij op die manier als het ware gelinkt aan strafbare feiten.

57. De AP stelt vast dat er persoonsgegevens van strafrechtelijke aard worden verwerkt. Er worden immers individuen gelinkt aan verschillende vormen van fraude, die terug te vinden zijn in het Wetboek van Strafrecht. Een individu wordt slechts dan in het Frauderegistratiesysteem opgenomen indien vereniging VODIOM en/of de deelnemende partij van mening is dat deze persoon (een poging tot) frauduleus handelen heeft verricht. De primaire verschijningsvormen van fraude welke in het frauderegistratiesysteem kunnen worden opgeslagen zijn 1) fraude door misbruik/diefstal van identificerende gegevens van slachtoffers of valse gegevens[47] en 2) fraude door misbruik te maken van identificerende gegevens van katvangers.[48]

58. De voorgenomen verwerking van de vereniging VODIOM en de deelnemende partijen valt dus in de categorie '*verwerken van persoonsgegevens van strafrechtelijke veroordelingen en strafbare feiten'* zoals bedoeld in artikel 10 van de AVG. De persoonsgegevens die de vereniging VODIOM en de deelnemende

[44] Zie: Kamerstukken II 2017/18, 34 851, nr. 3, blz. 114, en ook Kamerstukken II, 1997/98, 25 892, nr. 3, blz. 118.
[45] Zie: HR 29 mei 2009, ECLI:NL:HR:2009:BH4720, r.o. 4.4.
[46] Zie: onder 3 - feitelijke weergave van de voorgenomen verwerking.
[47] Zie: DPIA VODIOM, p. 8.
[48] Zie: DPIA VODIOM, p. 9.

partijen willen verwerken zijn zodanige concrete feiten en omstandigheden dat, mochten ze aan de rechter worden voorgelegd, die een bewezenverklaring in de zin van artikel 350 van het Wetboek van Strafvordering kunnen dragen. Mochten de verzamelde gegevens niet zodanig zijn dat zij deze toets kunnen doorstaan, dan zal de gegevensverwerking niet strekken tot het halen van het doel waarvoor de verwerking is opgezet en vanuit dat oogpunt onrechtmatig zijn. Het doel van de voorgenomen verwerking strekt immers tot de uitwisseling van informatie over fraude tussen sectoren, niet tot het uitwisselen van aannames van fraude.

## 5.2 Noodzakelijk met het oog op een zwaarwegend belang voor derden

59. De AP onderstreept dat het belang van fraudebestrijding en –preventie niet ter discussie staat, maar benadrukt evenwel dat de fraudebestrijding en –preventie in overeenstemming met de wet moet plaatsvinden. Daarbij zijn door de (Europese) wetgever drempels opgeworpen om te voorkomen dat al te lichtvaardig betrokkenen in gegevensbestanden terecht komen wat mogelijkerwijs onterecht kan leiden tot vergaande nadelige gevolgen voor betrokkenen, zoals stigmatisering of maatschappelijke uitsluiting.

60. De AP merkt op dat voor de private uitwisseling van fraude-informatie geen specifiek wettelijk kader van toepassing is. Derhalve dient te worden aangesloten op het algemene stelsel van gegevensbeschermingsbeginselen zoals neergelegd in de AVG. Het volgende is daarbij van belang. Het strafrechtdomein is met veel wettelijke waarborgen omgeven en is primair het domein van de overheid. Dit is een van de grondbeginselen van de Nederlandse rechtsorde hetgeen bijvoorbeeld blijkt uit de onschuldpresumptie en het ne bis in idem-beginsel, respectievelijk uit het exclusieve vervolgingsrecht van het Openbaar Ministerie en de politietaak zoals neergelegd in de Politiewet.[49] Ook in de AVG komt dit tot uiting in artikel 10 van de AVG, waarin wordt verplicht dat elke verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen alleen onder toezicht van de overheid plaatsvindt of indien het Unierechtelijk of lidstatelijk recht de verwerking toestaat. Onder andere een vergunning van de AP is vervat in zo'n wettelijke regeling van lidstatelijk recht waarin strafrechtelijke gegevens ten behoeve van derden mogen worden verwerkt.

61. De AP wil benadrukken dat fraudebestrijding primair een overheidstaak is. Daarnaast heeft de politie hiertoe primair een opsporingsbevoegdheid. Het strafrechtdomein beslaat daarom ook een scala aan wetten, regels en waarborgen voor betrokkenen. In artikel 10 van de AVG wordt verplicht dat elke verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen alleen onder toezicht van de overheid plaatsvindt of indien het Unierechtelijk of lidstatelijk recht de verwerking toestaat. In Nederland is artikel 10 van de AVG uitgewerkt in artikelen 1, 32 en 33 van de UAVG, waarin onder meer staat dat strafrechtelijke gegevens ten behoeve van derden alleen mogen worden verwerkt wanneer de AP daarvoor een vergunning heeft verleend.

[49] Zie: respectievelijk artikel 124 Wet op de rechterlijke organisatie en artikel 3 Politiewet 2012.

*5.2.1. Zwaarwegend belang van derden*

62. Uit de wetsgeschiedenis is - ten aanzien van het zwaarwegend belang - het volgende af te leiden: "*Het tegengaan van fraude kan als een zwaarwegend belang voor een bedrijf of onderneming worden aangemerkt. Het blijft dus op grond van deze bepaling mogelijk om zwarte lijsten te delen binnen een bepaalde bedrijfstak of bijvoorbeeld tussen winkels in een bepaald winkelcentrum.*"[50]

63. De vereniging VODIOM en de deelnemende partijen hebben als doel om een frauderegistratiesysteem in te richten dat het mogelijk maakt om cross-sectoraal gegevens over (vermoedelijke) fraudeurs te delen.[51] De partijen stellen dat het huidige systeem van fraudedetectie beperkingen heeft waardoor fraude niet effectief kan worden tegengegaan/voorkomen. De huidige frauderegistratiesystemen werken alleen binnen een sector en geven geen volledig beeld van hoe de fraude werkt en wie er fraudeert, aldus de partijen.[52]

64. De vereniging VODIOM en de deelnemende partijen willen met de voorgenomen verwerking in het frauderegistratiesysteem de directe schade van fraude voor de betrokken partijen terugdringen en de maatschappelijke impact van fraude (economische schade voor burgers en bedrijven, verlies aan vertrouwen, ondermijning, faciliteren criminaliteit en terrorisme) verkleinen.[53]

65. De AP concludeert uit bovenstaande doelstelling dat het doel van de vereniging VODIOM en de deelnemende partijen is om schade door fraude tegen te gaan voor zowel burgers als bedrijven. Dit kwalificeert als een zwaarwegend belang van derden, in de zin van artikel 33, vijfde lid, UAVG.

*5.2.2 Noodzakelijkheid*

66. Een zwaarwegend algemeen belang alleen is niet voldoende. De verwerking dient immers noodzakelijk te zijn met het oog op dit zwaarwegend algemeen belang. Het is volgens de wetgever aan de AP om vooraf, dat wil zeggen via de vergunningaanvraag, noodzaak en evenredigheid te toetsen.[54] In deze toets wordt gekeken of aan de proportionaliteit en subsidiariteit wordt voldaan. Een verwerking is proportioneel indien zij in verhouding staat tot het te dienen doel, waarbij wordt nagegaan of het middel opweegt tegen de inbreuk op de rechten en vrijheden van betrokkenen. Een verwerking is subsidiair indien er geen minder ingrijpend middel is waarmee het doel kan worden bereikt.

67. Vereniging VODIOM stelt dat het verwerken van persoonsgegevens van strafrechtelijke aard op een cross-sectorale zwarte lijst noodzakelijk is omdat fraude in Nederland een blijvend en groot probleem is. De huidige systematiek behelst volgens vereniging VODIOM beperkingen waardoor effectieve bestrijding en preventie van fraude niet mogelijk is. Deze maatregelen werken namelijk maar in één sector en geven geen volledig beeld van hoe de fraude werkt en wie er fraudeert.[55]

[50] Zie: Kamerstukken 112017-18,34851, nr. 7, Nota naar aanleiding van het verslag, p. 54-56.
[51] Zie: DPIA VODIOM, p. 7.
[52] Zie: DPIA VODIOM, p. 6.
[53] Zie: DPIA VODIOM, p. 6.
[54] Zie: *Kamerstukken* 112017-18,34851, nr.7, Nota naar aanleiding van het verslag, p. 55.
[55] Zie: DPIA VODIOM, p. 25 ev.

### 5.2.3 Cross-sectoraal delen van strafrechtelijke persoonsgegevens

68. Het cross-sectoraal delen van strafrechtelijke persoonsgegevens is een zeer ingrijpende inbreuk op het recht van gegevensbescherming van de betrokkene, in dit geval de vermoedelijke fraudeur. Om een dergelijke inbreuk te kunnen rechtvaardigen moet onder andere worden voldaan aan de zeer zware eisen van de noodzakelijkheidsafweging die komt kijken bij een cross-sectorale zwarte lijst waarin alle belangen tegen elkaar worden afgewogen.

69. De AP heeft op 15 juli 2021 de "*Handreiking cross-sectorale gegevensdeling tussen private partijen*" gepubliceerd.[56] Hierin staat dat het cross-sectoraal delen van strafrechtelijke persoonsgegevens niet is toegestaan. Slechts in zeer uitzonderlijke gevallen kan er een uitzondering op die regel worden gemaakt. Daarbij moet worden voldaan aan zeer zware eisen die voortvloeien uit de AVG en UAVG.

70. Een goede proportionaliteitsafweging is essentieel bij alle gedeelde zwarte lijsten om de noodzaak van de gegevensdeling aan te tonen. Voor een cross-sectorale gegevensdeling is dit vereiste nog relevanter, omdat de gegevens in meerdere sectoren terecht kunnen komen. De onderstaande criteria moeten extra goed worden afgewogen:
    a) Wordt een betrokkene uitgesloten van bijvoorbeeld eerste levensbehoeften of van goederen of diensten die een (klassiek of sociaal) grondrecht vertegenwoordigen?
    b) Is de betrokkene extra kwetsbaar? Zoals bij: minderjarige klanten, daklozen en (oudere) werknemers die geen mogelijkheid hebben om een eventueel ontslag aan te vechten.
    c) Is de reikwijdte van het systeem goed omschreven? Zoals: wie vult het systeem? Wie kunnen de gegevens in het systeem raadplegen? En van wie worden persoonsgegevens in het systeem verwerkt?

71. Zoals in de procesbeschrijving is vermeld, is de vereniging VODIOM voordat zij de vergunningaanvraag heeft ingediend onder embargo door de AP ingelicht over de handreiking die de AP zou publiceren over dit onderwerp. De AP heeft vereniging VODIOM in de gelegenheid gesteld om de punten die naar voren komen in deze handreiking te verwerken in de vergunningaanvraag. De vereniging VODIOM heeft aangegeven dat zij de handreiking zal verwerken in het protocol en DPIA van de thans ingediende vergunningaanvraag.

### 5.2.4 Noodzakelijkheid cross-sectorale zwarte lijst ex art. 35 UAVG

72. Hieronder wordt op de verschillende punten ingegaan die aan de orde komen in de noodzakelijkheidstoets indien een verwerkingsverantwoordelijke strafrechtelijke persoonsgegevens cross-sectoraal wil delen. Deze punten zijn terug te vinden in de *Handreiking cross-sectorale gegevensdeling tussen private partijen* die is gepubliceerd op de website van de AP.[57]

#### Afbakening sectoren (1)

73. Ten eerste moet er sprake zijn van een duidelijke cross-sectorale afbakening.[58] Alle meldingen kunnen immers in elke deelnemende sector opgeslagen worden. Dit maakt dat de inbreuk voor de persoon waarover geregistreerd wordt per definitie ingrijpender kan zijn. Iemand kan immers nadelige

[56] URL: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-duidelijkheid-over-zwarte-lijsten-delen-met-andere-sectoren.
[57] Zie: Handreiking cross-sectorale gegevensdeling tussen private partijen.
[58] Zie: Handreiking cross-sectorale gegevensdeling tussen private partijen p. 5.

gevolgen ondervinden van het geregistreerd staan in een dergelijk systeem, zoals stigmatisering of uitsluiting van bepaalde diensten of goederen.

74. In de aanvraag van de vereniging VODIOM gaat het om de sectoren betaalindustrie, online retail en telecommunicatie.[59]

75. In de stukken is onvoldoende omschreven hoe deze sectoren met elkaar samenhangen. De vereniging VODIOM geeft enkel het volgende aan: *"Wanneer iemand fraudeert bij een webshop, dan is de kans bijvoorbeeld aanwezig dat hij of zij ook fraudeert bij het afsluiten van een telefoonabonnement."*[60]

76. Een dergelijke motivering is onvoldoende om aan te tonen dat sprake is van een dermate grote verwantschap of verwevenheid tussen de sectoren, dat het een zeer ingrijpende inbreuk op het recht van gegevensbescherming van de betrokkene, namelijk registratie op een cross-sectorale zwarte lijst, zou kunnen rechtvaardigen.

77. Daarnaast wordt in de toegezonden documenten ook niet ingegaan op de vraag of het voor de hand ligt dat deze sectoren te maken krijgen met dezelfde soort fraude en/of fraudeurs en is niet onderbouwd of bepaalde criminaliteit min of meer logisch/automatisch voorkomt in een keten van sectoren als gevolg van de aard van de criminaliteit. Tot slot wordt in de stukken niet ingegaan op de vraag of het voor de hand ligt is om elkaar te waarschuwen voor bepaalde vormen van criminaliteit. Als het voor de hand ligt (en niet gekunsteld) dan is dat een indicatie dat het logisch is dat de genoemde sectoren met dezelfde criminaliteit te maken krijgen.

78. Bovendien moeten, om de proportionaliteit van de gegevensverwerking aan te tonen, de volgende aspecten in de stukken worden gemotiveerd: 1) Hoe toon je aan dat de fraude zowel in sector X als sector Y zal plaatsvinden? Dit betreft de dubbele aantoonplicht op ketenaspecten. 2) Hoe toon je aan dat iemand in al deze sectoren zal toeslaan? En: 3) In hoeverre is de dreiging van specifieke vormen van fraude concreet en evident aanwezig in de deelnemende sectoren? Deze vragen laat vereniging VODIOM onbeantwoord.

79. Gezien de bovenstaande randvoorwaarden heeft de vereniging VODIOM onvoldoende gemotiveerd waarom het noodzakelijk is om de gegevens van de betrokkenen (fraudeurs) in de benoemde sectoren cross-sectoraal te verwerken in het Frauderegistratiesysteem.

### Geografische afbakening (2)

80. Ten tweede moet er sprake zijn van een duidelijke geografische afbakening. Immers, hoe groter het geografisch gebied is dat een cross-sectorale zwarte lijst beslaat, hoe meer waarborgen noodzakelijk zijn. Door de geografische scope te verkleinen wordt de inbreuk op het recht van gegevensbescherming voor de betrokkene aanzienlijk verkleind.

[59] Zie: DPIA VODIOM, p. 4.
[60] Zie: DPIA VODIOM, p. 6.

81. In het protocol is niet toegelicht waarom is gekozen voor het gebied Nederland en in hoeverre dit gebied eventueel zou kunnen worden verkleind. Er is enkel aangegeven dat fraude in Nederland een groot probleem is.[61] Daarnaast is ook niet aangetoond dat de fraudeurs waar de cross-sectorale zwarte lijst zich op richt, door het gehele land opereren. De keuze voor het geografisch gebied is aldus ontoereikend gemotiveerd.

**Afbakening fraudevormen (3)**

82. Ten derde moet er sprake zijn van duidelijk afgebakende fraudevormen die kunnen leiden tot opname op de zwarte lijst. Daarbij moet aan de orde komen welke vormen van criminaliteit/fraude worden opgenomen op de cross-sectorale zwarte lijst in relatie tot het vooraf omschreven doeleinde, welke categorieën van gegevens op deze cross-sectorale zwarte lijst worden geregistreerd, de wijze waarop de gegevens worden verkregen, of het nodig is dat alle gegevens met alle deelnemers in alle sectoren gedeeld worden, op welke manier de verwerkingsverantwoordelijke verifieert of de gegevens juist en nauwkeurig zijn en hoe de geregistreerde persoonsgegevens tussen de deelnemers worden uitgewisseld: wanneer heeft een deelnemer recht op de cross-sectorale zwarte lijst te raadplegen en wanneer niet?

83. De vereniging VODIOM geeft in het protocol aan dat het Frauderegistratiesysteem zich beperkt tot horizontale fraude die gericht is op het onrechtmatig verkrijgen van economisch voordeel in het handelsverkeer. Het gaat daarbij specifiek om fraude die plaatsvindt in het kader van het aanbieden en afnemen van goederen en diensten, alsmede de logistieke en financiële afhandeling daarvan (opslag, transport, betaalverkeer). De fraude moet gericht zijn tegen de Deelnemer van VODIOM of diens klanten, dan wel worden gepleegd door gebruikmaking van faciliteiten van Deelnemers.[62] Het Frauderegistratiesysteem richt zich tegen fraude die wordt gepleegd door 1) overname van faciliteiten, 2) misbruik van faciliteiten, 3) misbruik van gegevens en 4) opzettelijke niet-nakoming. Deze fraudevormen vallen onder de strafbaarstelling in de titels XII en XXV van het Wetboek van Strafrecht.[63]

84. Uit het protocol blijkt dat het Frauderegistratiesysteem nadrukkelijk niet is bedoeld voor *employment screening*, beoordeling van kredietwaardigheid van personen, beoordeling voor het in aanmerking komen van basisbehoeften, goederen of diensten die een klassiek of sociaal grondrecht vertegenwoordigen of de beoordeling van het in aanmerking komen voor uitkeringen, toeslagen of andere verstrekkingen van de overheid.[64]

85. De vereniging VODIOM heeft ook uiteengezet aan welke voorwaarden een fraudegeval moet voldoen voordat deze mag worden opgenomen op de cross-sectorale zwarte lijst.[65]

86. Uit de ingediende documenten blijkt dat de vereniging VODIOM in voldoende mate heeft gezorgd voor een adequate afbakening van de fraudevormen, die in aanmerking komen voor registratie op de

[61] Zie: DPIA VODIOM, p. 5.
[62] Zie: Protocol VODIOM, p. 9.
[63] Zie: Protocol VODIOM, p. 10.
[64] Zie: Protocol VODIOM, p. 10.
[65] Zie hiervoor onder kopje 3: feitelijke weergave van de voorgenomen verwerking p. 3 ev. van dit besluit.

cross-sectorale zwarte lijst, en daarmee ook welke fraudevormen niet, en onder welke voorwaarden een fraudegeval geregistreerd mag worden op de cross-sectorale zwarte lijst. De fraudevormen zijn aldus voldoende duidelijk afgebakend en gemotiveerd.

### Bewaartermijnen (4)

87. Daarnaast moet ervoor worden gezorgd dat de cross-sectorale zwarte lijst een tijdelijk karakter heeft of dat er sprake is van zeer korte bewaartermijnen.

88. Uit het protocol blijkt dat persoonsgegevens uiterlijk drie jaar na de initiële registratie uit het Frauderegistratiesysteem verwijderd of zoveel eerder verwijderd als mogelijk met het oog op de doeleinden van de verwerking. Echter: wanneer zich ten aanzien van de (vermoedelijke) fraudeur een nieuwe aanleiding voordoet voor opname in het Frauderegistratiesysteem, wordt de bewaartermijn gestuit en vangt een nieuwe bewaartermijn van drie jaar aan.[66] Bij een foutieve registratie in het systeem of een gegrond bezwaar van de betrokkene worden de gegevens onmiddellijk verwijderd. De vereniging VODIOM stelt dat hiermee de cross-sectorale zwarte lijst van tijdelijke aard is. Gegevens die zijn toegevoegd op grond van toestemming worden verwijderd zodra de toestemming wordt ingetrokken.[67] Het gaat hierbij om vrijwillige 'beschermde registraties' van personen die het slachtoffer zijn geworden van identiteitsdiefstal.[68]

89. In de documenten staat geen motivering en/of afweging, waaruit zou moeten blijken dat de door vereniging VODIOM gehanteerde bewaartermijnen, van in principe drie jaar, daadwerkelijk noodzakelijk zijn voor de doelstellingen. Er is niet gemotiveerd of het probleem tijdelijk van aard is, het noodzakelijk is dat de cross-sectorale zwarte lijst van permanente aard is, en of het mogelijk is om kortere bewaartermijnen door te voeren.[69] Het feit dat de bewaartermijn telkens kan worden gestuit en er dan telkens een nieuwe bewaartermijn aanvangt kan er immers toe leiden dat de registratie op de cross-sectorale zwarte lijst van langdurige of zelfs permanente aard wordt. Deze inbreuk op het recht van gegevensbescherming staat niet in verhouding tot de door vereniging VODIOM opgestelde doelstellingen. De gehanteerde bewaartermijnen zijn aldus onvoldoende gemotiveerd en kan de proportionaliteitstoets niet doorstaan.

### Streng opnamebeleid (5)

90. Vervolgens moet sprake zijn van een streng opnamebeleid. De criteria op basis waarvan betrokkenen op de cross-sectorale zwarte lijst worden geplaatst moeten eenduidig en concreet zijn. Hierbij moet bijvoorbeeld rekening gehouden worden met welke vorm(en) van criminaliteit/fraude de verwerkingsverantwoordelijke wil aanpakken. Dit moet zo specifiek mogelijk én transparant zijn voor de betrokkenen. Ook moet worden bezien of achteraf goed te toetsen is of de plaatsing op de zwarte lijst rechtmatig is. Daarnaast moet in het protocol inzichtelijk worden gemaakt of er logischerwijs samenhang is tussen de vorm van criminaliteit of fraude, de diverse sectoren en de vermoedelijke fraudeur.[70]

---

[66] Zie: Protocol VODIOM, p. 20 en DPIA VODIOM, p. 37.
[67] Zie: DPIA VODIOM, p. 37.
[68] Zie: DPIA VODIOM, p. 17.
[69] Zie: Handreiking cross-sectorale gegevensdeling tussen private partijen p. 6.
[70] Zie: Handreiking cross-sectorale gegevensdeling tussen private partijen p. 6.

91. In het protocol van VODIOM wordt beschreven wanneer een deelnemende partij strafrechtelijke persoonsgegevens van een betrokkene (de vermoedelijke fraudeur) op de cross-sectorale zwarte lijst mag opnemen.[71] Er moeten onder meer 'gerede vermoedens' zijn dat het om fraude gaat of dat er fraude wordt gepleegd, dan wel gepoogd is of wordt gepoogd fraude te plegen, moeten deze vermoedens zijn onderbouwd met duidelijk bewijs en moeten de gedragingen kunnen worden gekwalificeerd als één van de vier fraudevormen waarop het Frauderegistratiesysteem betrekking heeft en vallen binnen de delictsomschrijvingen van Titels XII en XXV van het Wetboek van Strafrecht.[72]

92. De AP concludeert dat de vereniging VODIOM goed heeft nagedacht over het opnamebeleid op basis waarvan betrokkenen kunnen worden opgenomen in het Frauderegistratiesysteem. Tevens is het opnamebeleid voldoende duidelijk in de door haar aangeleverde stukken omgeschreven en gemotiveerd.

*Gegevens minderjarigen*

93. Opmerkelijk is echter het feit dat vereniging VODIOM stelt dat registratie van gegevens van kwetsbare personen, namelijk minderjarigen, in het Frauderegistratiesysteem voor hen een beschermende werking heeft.[73] Deze personen zouden op die manier minder aantrekkelijk worden voor criminele organisaties.

94. Het is echter niet een taak van de vereniging VODIOM om minderjarigen voor criminele organisaties te beschermen. Daarnaast moet juist extra voorzichtigheid worden betracht bij de verwerking van persoonsgegevens van minderjarigen, omdat zij, zoals vereniging VODIOM zelf ook stelt, een kwetsbare groep zijn. Deze extra voorzichtigheid is bovendien nóg belangrijker als het aankomt op een registratie in een Frauderegistratiesysteem.

### Beperking deelnemers

*95.* Tot slot moet het aantal deelnemers van een cross-sectorale zwarte lijst worden beperkt. Hoe meer partijen deelnemer zijn van een cross-sectorale zwarte lijst, des te groter de inbreuk op het recht van gegevensbescherming van de betrokkene. Er moet dus een goede afweging worden gemaakt welke partijen en op welke voorwaarden worden toegelaten tot de cross-sectorale zwarte lijst. De aspecten waarmee rekening dient te worden gehouden zijn de volgende: 1) wanneer mag een bepaalde partij deelnemer worden?, 2) is het mogelijk om een limitatieve lijst aan deelnemers vast te stellen?, 3) moeten alle deelnemers altijd toegang hebben tot alle gegevens of kan hier ook een beperking doorgevoerd worden? 4) de deelnemerslijst moet kenbaar zijn zodat betrokkenen hiervan kennis kunnen nemen. Het moet voor betrokkenen voorzienbaar zijn dat ze op een cross-sectorale zwarte terecht kunnen komen.

[71] Zie: Protocol VODIOM, p. 12 ev.
[72] Zie: Protocol VODIOM, p. 12.
[73] Zie: Protocol VODIOM, p. 5.

96. De vereniging VODIOM heeft hiertoe in het deelnemersreglement voorwaarden voor deelname opgenomen.[74] Een partij mag bijvoorbeeld deelnemer worden als deze aantoonbaar vatbaar is voor en te maken heeft met fraude zoals omschreven in titels IXX en XXV van het Wetboek van Strafrecht. Ook is er alleen toegang tot het Frauderegistratiesysteem voor *'gekwalificeerde medewerkers'*[75] van de deelnemende organisatie. Er wordt echter niet ingegaan op de vraag of er een limitatieve lijst van deelnemers kan worden vastgesteld.

97. Ook is niet duidelijk wat precies wordt bedoeld met 'gekwalificeerde medewerkers'. In de DPIA staat het volgende vermeld: '*Een organisatie moet aantonen dat haar personeel voldoende gekwalificeerd is om een oordeel te vellen over de registratiecriteria voor een persoon en dat er binnen de organisatie een stelsel van maatregelen is (governance) waarmee zorggedragen wordt voor een goed gebruik (inclusief een zorgvuldig autorisatieproces) van het Frauderegistratiesysteem.'*[76] Het blijft ook onduidelijk wanneer iemand dus daadwerkelijk onder de categorie 'gekwalificeerde medewerker' valt en hoe deze processen worden ingekleed. Daarnaast wordt er alleen kenbaarheid gegeven van het feit dat de partij een deelnemende organisatie is op de website van de deelnemer zelf. Hierdoor is het voor de betrokkene niet goed duidelijk dat zijn/haar gegevens ook terecht kunnen komen bij de andere deelnemende organisaties van de cross-sectorale zwarte lijst. Omdat de deelnemerslijst niet vooraf begrensd is, is bovendien voor een betrokkene vooraf niet duidelijk waar zijn/haar gegevens terecht kunnen komen. Tevens kan hierdoor op termijn een zeer lange deelnemerslijst ontstaan waardoor de inbreuk op het recht van gegevensbescherming voor de betrokkene alsmaar groter wordt.

98. De vereniging VODIOM heeft onvoldoende getracht om het aantal (toekomstige) deelnemers van de lijst zoveel mogelijk te beperken of af te bakenen. Hierdoor wordt de inbreuk op het recht van gegevensbescherming eveneens niet zoveel mogelijk beperkt.

**Tussenconclusie**

99. Hoewel de vereniging VODIOM een streng opnamebeleid heeft gerealiseerd en de fraudevormen die in aanmerking komen voor registratie op de cross-sectorale zwarte lijst duidelijk heeft afgebakend, zijn de overige fundamentele punten van de proportionaliteitsafweging in het kader van het zwaarwegend algemeen belang ex artikel 35, lid 5, UAVG onvoldoende en ontoereikend gemotiveerd. Dit betekent dat de noodzakelijkheid van de verwerking van strafrechtelijke persoonsgegevens op een cross-sectorale zwarte lijst niet is aangetoond. De beoogde cross-sectorale zwarte lijst is daarmee dus niet toegestaan.

100. Nu is geconstateerd dat deze beoogde gegevensdeling niet noodzakelijk is, gaat de AP niet verder in op de andere beoordelingspunten.

[74] Zie: Deelnemersreglement Frauderegistratiesysteem VODIOM, 5 juli 2021, p. 7 ev.
[75] Een medewerker van de deelnemende organisatie die specifiek belast is met de preventie en/of opsporing van fraude en uit hoofde van deze taak toegang heeft tot de persoonsgegevens in het frauderegistratiesysteem.
[76] Zie: DPIA VODIOM, p. 33.

## 6 – Conclusie – afwijzing vergunningaanvraag

101. De vereniging VODIOM is voornemens om met de realisatie van de cross-sectorale zwarte lijst 'Frauderegistratiesysteem' de directe schade van fraude voor de betrokken partijen terug te dringen en de maatschappelijke impact van fraude te verkleinen.

102. De AP concludeert weliswaar dat het doel van vereniging VODIOM[77] om fraude tegen te gaan waar zowel bedrijven als burgers het slachtoffer van kunnen worden kwalificeert als een zwaarwegend belang van derden in de zin van artikel 33, vijfde lid, UAVG.

103. De AP is echter van oordeel dat de vereniging VODIOM de proportionaliteit, subsidiariteit en daarmee de noodzaak van het de verwerking van strafrechtelijke persoonsgegevens onvoldoende toereikend heeft gemotiveerd. Zoals is gebleken uit de voorgaande overwegingen heeft de vereniging VODIOM de proportionaliteit en subsidiariteit, en daarmee de noodzaak van de voorgenomen verwerking, niet aannemelijk gemaakt. Het cross-sectoraal delen van de strafrechtelijke gegevens is daarmee niet toegestaan.

104. Daarnaast is de AP van oordeel dat de vereniging VODIOM niet aannemelijk heeft gemaakt dat de invoerende en raadplegende deelnemers gezamenlijk verwerkingsverantwoordelijkheid dragen voor de beoogde gegevensverwerking in het Frauderegistratiesysteem. Vereniging VODIOM lijkt eerder (primair) verwerkingsverantwoordelijke voor de gegevensverwerking in het Frauderegistratiesysteem.

105. Tenslotte is de AP van oordeel dat door het gebruik van de aparte beveiligde database bij verwerker CIFAS, die deze laat hosten in de Microsoft Azure Cloud, er waarschijnlijk sprake is van doorgifte naar derde landen (Amerika). In het protocol zijn verder geen aanwijzingen gevonden dat er een studie is gemaakt van het beschermingsniveau van Amerika, noch is er sprake van een '*standard contractual clauses*' met aanvullende maatregelen voor de doorgifte van persoonsgegevens naar Amerika. Het protocol voldoet daarmee - gelet op de vereisten in AVG en Recommendations - op dit punt niet aan de AVG.

106. De AP wijst daarom de bovenstaande vergunningaanvraag voor de verwerking van persoonsgegevens van strafrechtelijke aard ten behoeve van derden af. Er mag niet met de voorgenomen verwerking worden gestart. Als de verwerking toch plaatsvindt kan de AP handhavend optreden.

[77] Zie: Protocol p. 9: "(...) *Meer specifiek heeft het Frauderegistratiesysteem tot doel te voorkomen dat Deelnemers slachtoffer worden van fraudeurs, die eerder aangiftewaardige fraudehandelingen hebben gepleegd bij een of meerdere andere Deelnemers* (...)."

Datum
8 oktober 2021

Ons kenmerk
z2021-12791

*Den Haag, 8 oktober 2021*

Overeenkomstig het door de Autoriteit Persoonsgegevens genomen besluit,

[...]
Directeur Systeemtoezicht, Beveiliging en Technologie

**Rechtsmiddelenclausule**
Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens.
Het indienen van een bezwaarschrift schort de werking van dit besluit niet op.

Voor het indienen van digitaal bezwaar, zie www.autoriteitpersoonsgegevens.nl, onder het kopje 'Bezwaar maken', onderaan de pagina onder de kop 'Contact met de Autoriteit Persoonsgegevens'.
Het adres voor het indienen op papier is: Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag.
Vermeld op de envelop 'Awb-bezwaar' en zet in de titel van uw brief 'bezwaarschrift'.

Schrijf in uw bezwaarschrift ten minste:
• Uw naam en adres
• De datum van uw bezwaarschrift
• Het in deze brief genoemde kenmerk (zaaknummer); u kunt ook een kopie van dit besluit bijvoegen
• De reden(en) waarom u het niet eens bent met dit besluit
• Uw handtekening

Zie voor meer informatie: https://autoriteitpersoonsgegevens.nl/nl/bezwaar-maken