AUTORITEIT
PERSOONSGEGEVENS

Besluit inzake de vergunningaanvraag voor de verwerking van gegevens van strafrechtelijke aard ten behoeve van derden van de verwerking 'Fraudehelpdesk' van Safecin; z2018-12010.

1 Inleiding: aanleiding vergunningaanvraag

1. Op 16 januari 2019 heeft de Stichting aanpak financieel-economische criminaliteit in Nederland (Safecin) – ingevolge artikel 33, vierde lid, aanhef en onder c, van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) – bij de Autoriteit Persoonsgegevens (AP) een vergunningaanvraag ingediend. Deze aanvraag is bij de AP bekend onder z2018-12010 onder de naam 'Vergunning Fraudehelpdesk'. Ter onderbouwing van de aanvraag heeft Safecin een protocol en een data protection impact assessment (gegevensbeschermingseffectbeoordeling, ook wel DPIA genoemd) 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 Safecin onvoldoende de verantwoordingsplicht heeft nageleefd en de noodzaak en proportionaliteit van de voorgenomen verwerking onvoldoende heeft aangetoond.

2 Procedureverloop

4. Bij besluit van 25 mei 2009 heeft de rechtsvoorganger van de AP, het College bescherming persoonsgegevens (CBP), een rechtmatigheidsverklaring aan Safecin afgegeven voor de verwerking van strafrechtelijke gegevens ter preventie van acquisitiefraude zoals neergelegd in het Protocol Safecin. Deze rechtmatigheidsverklaring geldt voor een periode van zes jaar en liep derhalve tot 25 mei 2015.[1]

5. Vanaf juni 2015 is met Safecin een informeel overlegtraject gestart over een nieuw protocol. Dat nieuwe protocol betreft verwerkingen van strafrechtelijke gegevens ter preventie van meer vormen van fraude dan enkel acquisitiefraude. Het CBP heeft destijds aangegeven dat op basis van dat protocol, in het kader van een voorafgaand onderzoek, geen rechtmatigheidsverklaring kan worden afgegeven, omdat het werkveld van Safecin veel groter is geworden.[2] Zonder voorafgaand

[1] Bij de AP bekend onder nummer z2009-00959.
[2] Bij de AP bekend onder nummer z2015-00367.

onderzoek was de verwerking van strafrechtelijke gegevens onder de Wet bescherming persoonsgegevens (Wbp) onrechtmatig.

6. In november 2016 is er opnieuw contact geweest over een herschreven protocol. De rechtsopvolger van het CBP, de AP, heeft nogmaals aangegeven dat het protocol niet kon leiden tot een rechtmatigheidsverklaring. In januari 2017 is door de AP nogmaals aangegeven dat verwerkingen zonder goedgekeurd protocol niet rechtmatig zijn en dat de AP handhavend op kan treden als Safecin zonder voorafgaand onderzoek strafrechtelijke gegevens verwerkt.[3]

7. In januari 2018 heeft Safecin opnieuw een herschreven protocol ingediend. Hierover hebben in februari, maart en juli 2018 gesprekken plaatsgevonden waarin is aangegeven dat met inwerkingtreding van de AVG geen rechtmatigheidsverklaring meer wordt afgegeven, maar dat een vergunning voor het verwerken van strafrechtelijke gegevens dient te worden aangevraagd. Inhoudelijk is ook op het protocol ingegaan en is aangegeven dat dit protocol niet door de eisen van een vergunningverlening zou komen.[4]

8. Bij brief van 17 juli 2018 heeft de AP uiteengezet dat het protocol niet toetsbaar is. Daarnaast heeft de AP aan Safecin kenbaar gemaakt dat voor september 2018 een nieuw protocol inclusief DPIA dient te zijn ingediend.

9. Op 31 augustus 2018 heeft Safecin een nieuw herschreven protocol aan de AP voorgelegd. Na telefonisch contact is op 13 september 2018 de DPIA door de AP ontvangen.

10. Op 27 november 2018 heeft de AP bericht dat het protocol wederom onvoldoende toetsbaar is en dat de informele contacten die sinds 2015 liepen zullen worden afgesloten. Op 3 en 4 december 2018 is dit telefonisch toegelicht.

11. Per e-mail van 14 december 2018 heeft de AP kenbaar gemaakt dat de brief van 27 november 2018 niet kwalificeert als een besluit in de zin van de Algemene wet bestuursrecht (Awb).

12. Bij brief van 16 januari 2019 heeft Safecin de AP formeel verzocht een vergunning te verlenen op basis van het protocol van 31 augustus 2018.

13. Op 17 januari 2019 heeft de AP per brief gewezen op de formele procedure voor het aanvragen van een vergunning en verzocht om nadere informatie, namelijk het door de AP ter beschikking gestelde aanvraagformulier voor vergunningen en nadere uitwerking in de DPIA waaruit blijkt of sprake is van hoge restrisico's bij de verwerking.[5]

14. Bij brief van 6 februari 2019 heeft Safecin de aanvraag aangevuld. Bij brief van 11 februari 2019 heeft de AP de ontvangst van voornoemde brief schriftelijk bevestigd.

15. Bij brief van 4 april 2019 heeft de AP de beslistermijn verlengd met een periode van drie maanden.

[3] Bij de AP bekend onder nummer z2016-11822.
[4] Bij de AP bekend onder nummer z2018-00681.
[5] Bij hoge restrisico's van een verwerking moet bij de AP conform art. 36, eerste lid, van de AVG een voorafgaande raadpleging worden aangevraagd alvorens tot aanvraag van een vergunning te komen.

3 Feitelijke weergave van de voorgenomen verwerking

16. De Stichting aanpak financieel-economische criminaliteit in Nederland (Safecin) exploiteert de Fraudehelpdesk. De Fraudehelpdesk is de merk- en verzamelnaam voor de verwerkingen die Safecin uitvoert. Hierna zal naar Safecin als verwerkingsverantwoordelijke worden gerefereerd en naar de Fraudehelpdesk als de verzamelnaam voor (de uitvoering van) de verwerkingen van persoonsgegevens.

17. De Fraudehelpdesk van Safecin ontvangt meldingen van mogelijk gedupeerde burgers en bedrijven over verschillende soorten financieel-economische fraude. De Fraudehelpdesk onderzoekt en verrijkt deze meldingen en legt deze meldingen vast. Op verschillende manieren worden deze meldingen – inhoudende (persoons)gegevens – gedeeld met derden, onder andere via de website van de Fraudehelpdesk, via media, via partnerorganisaties en via aangesloten bedrijven. Deze gegevens kwalificeren volgens Safecin als strafrechtelijke gegevens in de zin artikel 10 van de AVG.

18. De verwerkingen van de Fraudehelpdesk zijn volgens het protocol op te splitsen in een aantal stappen: allereerste ontvangt de Fraudehelpdesk via een online formulier, telefonisch, per post of per e-mail meldingen van fraude. Deze meldingen worden in twee systemen vastgelegd: het meldingensysteem Fraudemelding (FM) en het meldingensysteem Valse E-mail (VE). Via het meldingensysteem VE komen meldingen van bijvoorbeeld phishing en malware binnen; de overige meldingen komen in het meldingensysteem FM.

19. Meldingen over betrokkenen die al bekend zijn in het meldingensysteem FM worden meteen opgeslagen. Meldingen over betrokkenen die nog niet bij de Fraudehelpdesk bekend zijn worden nader onderzocht. Voor zover mogelijk wordt de nauwkeurigheid en betrouwbaarheid van de melding gecontroleerd. Daarnaast wordt voor verschillende fraudetypes de melding aan verschillende criteria getoetst. Er worden geen anonieme meldingen vastgelegd. Bij alle meldingen wordt dus ook informatie over de melder geregistreerd. Als uit de inhoud van de melding of het aanvullend onderzoek blijkt dat de melding geen betrekking heeft op een frauduleuze activiteit wordt de melding verwijderd met inachtneming van bewaartermijnen.

20. Meldingen via het meldingensysteem VE worden geautomatiseerd geanalyseerd en vervolgens door de Fraudehelpdesk gevalideerd. Wanneer sprake is van ‘valse e-mail’ wordt de melding vastgelegd. Mocht uit de analyse of validatie blijken dat er geen sprake is van ‘valse e-mail’ dan wordt de melding met inachtneming van bewaartermijnen verwijderd.

21. Tot slot wordt de informatie uit de meldingensystemen gebruikt voor diverse producten die de Fraudehelpdesk ‘verdere verwerkingen’ noemt: het informeren van de melder, de IBAN-check, verklaringen voor juridische procedures, uitwisseling met derden op basis van een convenant, openbare publicatie en wetenschappelijk onderzoek. Ook wordt de informatie na een vordering door een bevoegde autoriteit verstrekt.

22. Het product ‘informeren van de melder’ omvat een algemene informatievoorziening voor de melder van een mogelijke frauduleuze activiteit en eventuele doorverwijzing naar andere instanties.

23. Het product 'IBAN-check' is een dienst via de site van de Fraudehelpdesk waarmee deelnemers, na inloggen, een bankrekeningnummer kunnen invoeren en op basis van hit/no-hit kunnen controleren of het nummer bekend staat bij de Fraudehelpdesk als zijnde mogelijk gebruikt bij frauduleuze activiteiten.

24. Het product 'verklaringen voor juridische procedures' is een dienst die deelnemers kunnen afnemen als zij zijn verwikkeld in een juridische procedure met een natuurlijk persoon of rechtspersoon. De deelnemer kan ten behoeve van de juridische procedure een verklaring krijgen bij de Fraudehelpdesk waarin de Fraudehelpdesk verklaart over de aard en omvang van vastgelegde meldingen over de wederpartij in de procedure.

25. Het product 'uitwisseling met derden op basis van een convenant' omvat de uitwisseling van gegevens over meldingen met andere instanties, die dezelfde doelen en nastreven en belangen behartigen als de Fraudehelpdesk.

26. Het product 'openbare publicatie' omvat enerzijds de publicatie door de Fraudehelpdesk op social media en de eigen website over verschillende frauduleuze activiteiten. Anderzijds omvat het informatievoorziening aan media over bepaalde meldingen.

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."

Artikel 6, eerste lid, aanhef en onder f, AVG bepaalt: "De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:
[…]
f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de 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."

Overweging 47 van de AVG stelt: "De gerechtvaardigde belangen van een verwerkingsverantwoordelijke, waaronder die van een verwerkingsverantwoordelijke aan wie de persoonsgegevens kunnen worden verstrekt, of van een derde, kan een rechtsgrond bieden voor verwerking, mits de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder wegen, rekening houdend met de redelijke verwachtingen van de betrokkene op basis van zijn verhouding met de verwerkingsverantwoordelijke. […] In elk geval is een zorgvuldige beoordeling geboden om te bepalen of sprake is van een gerechtvaardigd belang, alsook om te bepalen of een betrokkene op het tijdstip en in het kader van de verzameling van de persoonsgegevens redelijkerwijs mag verwachten dat verwerking met dat doel kan plaatsvinden. De belangen en de grondrechten van de betrokkene kunnen met name zwaarder wegen dan het belang van de verwerkingsverantwoordelijke wanneer persoonsgegevens worden verwerkt in omstandigheden waarin de betrokkenen redelijkerwijs geen verdere verwerking verwachten. […] De verwerking van persoonsgegevens die strikt noodzakelijk is voor fraudevoorkoming is ook een gerechtvaardigd belang van de verwerkingsverantwoordelijke in kwestie. […]"

Artikel 5, tweede lid, AVG bepaalt: "De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht")."

27. Het wettelijk kader betekent dat de AP zich in het kader van de beoordeling van een vergunningaanvraag beperkt tot de beoordeling van de verwerking van persoonsgegevens van strafrechtelijke aard ten behoeve van derden.

4.2 Zorgvuldig ontwerp voorgenomen verwerking

Artikel 35, tweede lid, aanhef en onder b, AVG bepaalt: "Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:
[…]
b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of […]"

Artikel 36, eerste lid, AVG bepaalt: "Wanneer uit een gegevensbeschermingseffectbeoordeling krachtens artikel 35 blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit."

5 Beoordeling voorgenomen verwerking

28. Aan de hand van het wettelijk kader wordt de voorgenomen verwerking beoordeeld. De beoordeling is gebaseerd op de aan de verwerking ten grondslag liggende vergunningaanvraag, de gevoerde correspondentie[6], het protocol Fraudehelpdesk[7], en de gegevensbeschermingseffectbeoordeling (DPIA)[8].

29. De AP heeft geen onderzoek gedaan naar de werkwijze en de praktijk van Safecin voorafgaand aan de vergunningsaanvraag.

30. Uit de stukken blijkt dat Safecin het doel en de middelen bepaalt voor de verwerkingen van Fraudehelpdesk en daarmee kwalificeert als verwerkingsverantwoordelijke.

31. Uit de stukken blijkt dat er geen sprake is van grensoverschrijdende verwerkingen; alle verwerkingen vinden plaats in Nederland, de gegevensdelingen vinden plaats binnen Nederland en de verwerkingen hebben hoofdzakelijk betrekking op Nederlandse betrokkenen.

32. De beoordeling wordt hierna op volgende manier vorm gegeven: allereerst wordt er gekeken naar de mate van verwerking van persoonsgegevens van strafrechtelijke aard (paragraaf 5.1). Als er geen sprake is van persoonsgegevens van strafrechtelijke aard dan is de verwerking niet vergunningplichtig.[9] Vervolgens wordt de verwerking getoetst aan artikel 33 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 worden geschaad (paragraaf 5.3). Tot slot wordt ingegaan op het zorgvuldig ontwerp van een gegevensverwerking (paragraaf 5.4).

5.1 Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

33. 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. 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".[10]

34. Uit de ingediende documenten blijkt niet duidelijk welke persoonsgegevens of categorieën van persoonsgegevens worden verwerkt in het kader van de activiteiten van de Fraudehelpdesk. In eerdere correspondentie heeft Safecin zelf aangegeven dat, mede gelet op de doelstelling van de

[6] Zie voor contactmomenten paragraaf 2 'Procedureverloop'.
[7] Protocol Verwerking strafrechtelijke persoonsgegevens Fraudehelpdesk; concept versie 0.9 d.d. 31 augustus 2018.
[8] Rapport Gegevensbeschermingseffectbeoordeling Fraudehelpdesk, versie 2.1, d.d. januari 2019.
[9] Overigens is daarmee niet direct gegeven dat de verwerking rechtmatig is.
[10] HR 29 mei 2009, ECLI:NL:HR:2009:BH4720, r.o. 4.4.

Fraudehelpdesk om gegevens aan derden te verstrekken, persoonsgegevens van strafrechtelijke aard worden verwerkt.[11]

35. De AP acht het aannemelijk dat er persoonsgegevens van strafrechtelijke aard worden verwerkt, gezien de doelstelling van de Fraudehelpdesk en de focus op verschillende vormen van fraude, hetgeen een verzamelbegrip is van verschillende strafbare feiten. Meer specifiek komt de AP op basis van de aanvraag tot de conclusie dat de verwerkingen van de Fraudehelpdesk vallen in de categorie 'persoonsgegevens van strafbare feiten'. De meldingen die de Fraudehelpdesk ontvangt, hebben immers geen betrekking op feiten of omstandigheden die reeds tot een rechterlijk oordeel hebben geleid. De persoonsgegevens die de Fraudehelpdesk beoogt te 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 daarmee de voorgaande toets doorstaan wordt, dan zal de gegevensdeling niet strekken tot het halen van het doel waarvoor de verwerking is opgezet en vanuit dat oogpunt onrechtmatig zijn. Het doel van de Fraudehelpdesk strekt immers tot de uitwisseling van informatie over fraude, niet tot het uitwisselen van aannames van fraude.[12]

36. Een vergunning is een ontheffing op een verbod, de rechtszekerheid is er mee gebaat een duidelijke afbakening van die ontheffing weer te geven in de vergunning. De AP heeft derhalve Safecin verzocht het protocol te beperken tot enkel die gegevensverwerkingen die persoonsgegevens van strafrechtelijke aard bevatten.[13] Door het in de DPIA en het protocol ontbreken van overzichten bij welke verwerkingen welke persoonsgegevens of categorieën van persoonsgegevens worden verwerkt, kan de AP met onvoldoende zekerheid vaststellen welke verwerkingen vergunningplichtig zijn. Nu Safecin heeft verzocht een vergunning te verlenen voor verwerkingen in een protocol waarin ook niet-vergunningplichtige verwerkingen zijn opgenomen, zal de AP de aanvraag behandelen voor zover zij het aannemelijk acht dat de verwerkingen onder de vergunningplicht vallen.

5.2 Noodzakelijk met het oog op een zwaarwegend belang van derden

37. De AP onderstreept dat het belang van fraudebestrijding en –preventie niet ter discussie staat, maar benadrukt evenwel dat de fraudebestrijding en –preventie wel 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 die mogelijkerwijs onterecht kunnen leiden tot vergaande nadelige gevolgen voor betrokkenen, zoals stigmatisering of maatschappelijke uitsluiting.

38. 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

[11] Gesprek van 5 juli 2018.
[12] In voorkomend geval is een dergelijke uitwisseling strafbaar op grond van de wettelijke bepalingen over smaad(schrift) of laster.
[13] Gesprek van 5 juli 2018 en brief van 17 juli 2018.

vervolgingsrecht van het Openbaar Ministerie en de politietaak zoals neergelegd in de Politiewet.[14] Ook in de AVG komt dit tot uiting in artikel 10 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 zo'n wettelijke regeling van lidstatelijk recht waarin strafrechtelijke gegevens ten behoeve van derden mogen worden verwerkt.

39. Er bestaat voor private organisaties geen algemene wettelijke verplichting of taak om fraude te voorkomen of om informatie over fraude uit te wisselen.[15] Een organisatie kan wel een gerechtvaardigd belang hebben om persoonsgegevens te verwerken ter preventie van fraude aangaande zijn eigen organisatie. Dit volgt uit overweging 47 bij de AVG en artikel 33, tweede lid, UAVG. Het voorgaande betekent echter niet dat de organisatie deze gegevens ook met derden mag delen. De verwerking dient immers noodzakelijk te zijn met het oog op het zwaarwegend belang van derden. Bovendien moeten in zodanige waarborgen worden voorzien dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Als het zwaarwegend belang is aangetoond en in de waarborgen is voorzien, kan de verwerking waarmee persoonsgegevens van strafrechtelijke aard worden gedeeld met derden voor een vergunning in aanmerking komen.

5.2.1 Zwaarwegend belang van derden

40. De Nederlandse wetgever zegt ten aanzien van het zwaarwegend belang het volgende. "*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.*"[16]

41. Safecin heeft tot doel met de Fraudehelpdesk "de Nederlandse samenleving te behoeden en weerbaarder te maken tegen financieel-economische criminaliteit om daarmee (verdere) schade onder burgers en het bedrijfsleven te voorkomen". De wetgever noemt slechts bedrijven of ondernemingen die de 'derde' zijn die een zwaarwegend belang kunnen hebben; de wetstekst sluit burgers niet uit, de AP is van oordeel dat ook burgers de derde kunnen zijn met een zwaarwegend belang om fraude tegen te gaan.

42. Uit het doel van Safecin concludeert de AP dat dit doel dient om zwaarwegende belangen van derden te behartigen, in de zin van artikel 33, vijfde lid, UAVG.

5.2.2 Noodzakelijkheid

43. Een zwaarwegend belang alleen is niet voldoende. De verwerking dient immers noodzakelijk te zijn met het oog op dit zwaarwegend belang. Het is volgens de wetgever aan de AP om vooraf, dat wil zeggen via de vergunningaanvraag, noodzaak en evenredigheid te toetsen.[17]

[14] Zie respectievelijk artikel 124 Wet op de rechterlijke organisatie en artikel 3 Politiewet 2012.
[15] Dit kan wel het geval zijn bij specifieke gevallen met een wettelijke regeling, bijvoorbeeld in de Wet ter voorkoming van witwassen en financieren van terrorisme.
[16] Kamerstukken II 2017-18, 34 851, nr. 7, Nota naar aanleiding van het verslag, p. 54-56.
[17] Kamerstukken II 2017-18, 34 851, nr. 7, Nota naar aanleiding van het verslag, p. 55.

44. De noodzakelijkheid van een verwerking moet onder andere worden getoetst aan de proportionaliteit en de subsidiariteit. Met andere woorden: een verwerking dient noodzakelijk te zijn om het vastgestelde doel van de verantwoordelijke te bereiken, waarbij dient te worden nagegaan of het middel opweegt tegen de inbreuk op de persoonlijke levenssfeer en of er geen minder verstrekkend middel is waarmee het doel ook wordt bereikt.

45. Safecin betoogt dat het verzamelen c.q. vastleggen van meldingen met daarin persoonsgegevens van strafrechtelijke aard noodzakelijk is om de Nederlandse samenleving te behoeden en weerbaarder te maken voor financieel-economische criminaliteit. Dit doel wil Safecin bereiken met verschillende middelen. Deze middelen noemt Safecin 'verdere verwerkingen' en staan hiervoor omschreven in paragraaf 3.

46. De AP overweegt ten aanzien van de noodzaak in het algemeen als volgt.[18] Safecin had per verwerking en verwerkingsdoeleinde moeten onderbouwen hoe de verwerkingen door de noodzakelijkheidstoets komen. Zij heeft echter enkel voor de vastlegging van gegevens – zeer summier – onderbouwd waarom het noodzakelijk zou zijn gegevens vast te leggen.[19] De AP heeft Safecin er meermaals nadrukkelijk op gewezen een grondige onderbouwing van de noodzaak en proportionaliteit te documenteren in zowel het protocol als de DPIA.[20] Dit heeft Safecin nagelaten. Het niet of onvoldoende onderbouwen van de noodzaak is in strijd met het verantwoordingsplicht van artikel 5, tweede lid, van de AVG.

47. Uit het doel van Safecin blijkt dat het informeren van burgers en bedrijfsleven nadat een mogelijk frauduleuze activiteit heeft plaatsgevonden een belangrijk onderdeel van dienstverlening is. De AP acht het voor dit doel niet noodzakelijk om gegevens herleidbaar naar personen te verzamelen. Slechts het vastleggen van de zogenaamde 'modus operandi', dat wil zeggen de manier waarop de fraude heeft plaatsgevonden zonder gegevens over de persoon achter de fraude, zou hiervoor voldoende zijn nu daarmee vermeende slachtoffers kunnen worden bijgestaan en worden geïnformeerd over te nemen vervolgstappen, zoals het doen van aangifte of een doorverwijzing naar bevoegde instanties. Er is naar oordeel van de AP voor dit doel een minder verstrekkend middel beschikbaar dan het vastleggen van persoonsgegevens van strafrechtelijke aard. De verwerking is dan ook in strijd met het subsidiariteitsbeginsel.

48. Uit het doel van Safecin blijkt ook dat zij in specifieke gevallen optreedt om burgers en het bedrijfsleven te behoeden en weerbaarder te maken voor fraude. Het gaat dan niet om algemene informatievoorziening en kennisuitwisseling over fraude, maar specifieke informatie-uitwisseling over specifieke fraudegevallen. In het protocol is echter niet onderbouwd hoe een specifiek middel, zoals de IBAN-check, verklaringen voor juridische procedures of uitwisseling met anderen, noodzakelijk is om dat doel te bereiken. Impliciet valt uit het protocol op te maken dat deze middelen kennelijk 'handig' zijn. Dat maakt echter niet dat de middelen noodzakelijk zijn of niet op een andere manier vorm gegeven kunnen worden. Safecin had dit nader dienen te onderbouwen.

[18] De noodzakelijkheidstoets in algemene zin omvat tevens de proportionaliteits- en subsidiariteitstoets en de noodzakelijkheidstoets in enge zin.
[19] Paragraaf 4.2 en de aanhef van paragraaf 5 van het protocol.
[20] Gesprekken in februari, maart en juli 2018 en de brief van de AP van 17 juli 2018.

49. Zoals hiervoor aangegeven is het voor de uitwisseling van gegevens van strafrechtelijke aard met derden van belang een goede afweging van de proportionaliteit te maken. Onder andere kunnen volgens de wetgever de volgende omstandigheden een rol in bij spelen bij de proportionaliteitstoets:[21]

- de mate waarin opname van een individu in het systeem waarop de gegevensuitwisseling betrekking heeft, kan betekenen dat betrokkene wordt uitgesloten van bijvoorbeeld eerste levensbehoeften of van goederen of diensten die betrekking hebben op een (klassiek of sociaal) grondrecht;
- de kwetsbaarheid van bepaalde groepen betrokkenen, zoals minderjarige klanten en werknemers, oudere werknemers en werknemers die geen mogelijkheid hebben om een eventueel ontslag aan te vechten;
- de reikwijdte van het systeem, in termen van zowel degenen die het systeem kunnen vullen, degenen die gegevens in het systeem kunnen raadplegen en degenen van wie persoonsgegevens in het systeem worden verwerkt. Hoe groter de reikwijdte, hoe ingrijpender de gevolgen voor opname van de betrokkene in het systeem kunnen zijn. Naarmate de reikwijdte van een systeem groter is, zullen derhalve de waarborgen voor betrokkenen zwaarder moeten zijn of zal het systeem in het geheel niet door de toetsing komen. Het beperken van de reikwijdte van het systeem (geografisch, sectoraal of anderszins) kan bijdragen aan een positieve uitkomst van de proportionaliteitsafweging.

50. De AP overweegt ten aanzien van de proportionaliteit als volgt. Hiervoor is reeds opgemerkt dat onterechte opname in gegevensbestanden zoals zwarte lijsten over bijvoorbeeld frauduleus handelen vergaande gevolgen voor betrokkenen kunnen hebben, zoals stigmatisering of maatschappelijke uitsluiting. Uit de wetsgeschiedenis blijkt dat de wetgever in beginsel gegevensuitwisselingen binnen een bepaalde branche of in een afgebakend geografisch gebied voor ogen heeft die voor een vergunning in aanmerking komen. De Fraudehelpdesk is cross-sectoraal opgezet. Dat betekent dat de gegevens van betrokkenen waarover meldingen van fraude in een bepaalde sector zijn binnengekomen onverschillig van die sector worden opgeslagen. Dit maakt de reikwijdte van de verwerking in sectorale zin zeer breed. Safecin legt met de Fraudehelpdesk meldingen van 13 soorten frauduleuze activiteiten vast.[22] De reikwijdte van deze types fraude is groot en zien op een groot deel van het economisch verkeer. Deze reikwijdte in inhoudelijke zin heeft tot gevolg dat de impact voor betrokkene groot kan zijn. Daarbij merkt de AP op dat Safecin niet heeft voorzien in waarborgen die deze reikwijdte beperken met betrekking tot de toegang van betrokkenen tot primaire levensbehoeften of tot goederen of diensten die betrekking hebben op een (klassiek of sociaal) grondrecht. Zo blijkt uit de voorgenomen verwerking dat er geen onderscheid wordt gemaakt in partijen die zich als deelnemer kunnen aansluiten bij de Fraudehelpdesk. Ter illustratie: aanbieders van sociale huurwoningen (een sociaal grondrecht) kunnen zo ongeclausuleerd aansluiten en betrokkenen weigeren op grond van gegevens verkregen van Safecin.

51. Een zeer streng opnamebeleid zou een belangrijke waarborg in de proportionaliteitstoets kunnen zijn. De AP is van oordeel dat er echter geen sprake is van een zeer streng opnamebeleid. In het toetsingsproces van het meldingensysteem FM blijkt dat opname altijd plaatsvindt als een

[21] Kamerstukken II 2017-18, 34 851, nr. 7, Nota naar aanleiding van het verslag, p. 54-56.
[22] Tabel op pagina 13-17 van het Protocol. Voorbeelden hiervan zijn acquisitiefraude, beleggingsfraude, merkenfraude, identiteitsfraude.

melding gaat over een betrokkene die reeds in het meldingensysteem staat.[23] Als de betrokkene niet bekend is en het gerede vermoeden van een frauduleuze activiteit volgt uit de melding, doet de Fraudehelpdesk nader onderzoek in openbare bronnen. Niet gespecificeerd is wanneer er sprake is van het 'gerede vermoeden'. Evenmin is limitatief opgesomd wat 'openbare bronnen' zijn en hoe de verwerking van de Fraudehelpdesk zich verhoudt met de doelbinding van die openbare bronnen.[24] Voorts is niet gespecificeerd of en hoe wordt beoordeeld of de betrokkenen tot een kwetsbare groep behoren. Voor de verschillende types fraude zijn daarnaast aanvullende criteria opgesteld, deze criteria zijn echter niet aan te merken als voorwaarden voor opname in de systemen, maar fungeren als classificatie voor het type fraude. Tevens zijn er geen bepalingen opgenomen waaruit blijkt dat opname in het systeem pas na het voldoen van een bepaalde verplichting plaatsvindt: bijvoorbeeld de eis dat er ten minste aangifte bij de politie van de frauduleuze handeling is gedaan door of namens de melder. Uit het voorgaande concludeert de AP dat er onvoldoende waarborgen zijn voor opname van de meldingen in de systemen en de opnamecriteria te lichtvaardig zijn.

52. Daarnaast heeft ook de bewaartermijn invloed op de proportionaliteitsafweging. Daarover overweegt de AP als volgt. De hoofdbewaartermijn in het protocol is 8 jaar: voor meldingen waarbij volgens Safecin is 'vastgesteld' dat er sprake is van financieel-economische criminaliteit. Er is niet onderbouwd waarom 8 jaar een redelijke termijn is. Voor betrokkene is 8 jaar evenwel een behoorlijke tijd die impactvol kan zijn. Er wordt geen heroverweging van opname gedaan na bijvoorbeeld strafrechtelijke vrijspraak of sepot of een civielrechtelijke afwijzing van aansprakelijkheid van de betrokkene. De AP is daarom van oordeel dat de bewaartermijn disproportioneel is.

53. Uit het voorgaande concludeert de AP dat Safecin niet heeft voldaan aan de verantwoordingsplichten van artikel 5, tweede lid, AVG. Daarnaast oordeelt de AP dat het niet noodzakelijk en proportioneel is om persoonsgegevens van strafrechtelijke aard te verwerken en dat de voorgenomen verwerking in strijd is met het subsidiariteitsbeginsel. De voorgenomen verwerking voldoet daarmee niet aan de eisen van artikel 33, vijfde lid, UAVG en daarmee kan geen vergunning worden verleend.

5.3 Zodanige waarborgen dat de persoonlijke levenssfeer van betrokkenen niet onevenredig wordt geschaad

54. Als blijkt dat de verwerking noodzakelijk is voor een zwaarwegend belang voor derden, vereist artikel 33, vijfde lid, van de AVG dat er moet worden voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van betrokkenen niet onevenredig wordt geschaad. Uit het voorgaande volgt dat de voorgenomen verwerking van de Fraudehelpdesk niet noodzakelijk is met het oog op een zwaarwegend belang van derden, op grond waarvan een vergunning niet kan worden verleend. De AP komt daarom niet toe aan de beoordeling van eventuele waarborgen, de evenredigheidstoets en de grondslag van de verwerking.

55. Ten overvloede wenst de AP wel het volgende op te merken met betrekking tot de waarborgen. Safecin heeft in het protocol onvoldoende aandacht geschonken aan de gevolgen die opname kan

[23] Paragraaf 4.3 en 5.1 van het protocol.
[24] Er wordt alleen ter illustratie verwezen naar het handelsregister van de Kamer van Koophandel en social media, paragraaf 4.5 van het protocol.

hebben op de persoonlijke levenssfeer van betrokkenen. De aandacht in het protocol ligt voornamelijk op de impact die mogelijke frauduleuze handelingen hebben op het slachtoffer. Er is geen bepaling opgenomen waarin de betrokkene op de hoogte wordt gesteld van het feit dat hij/zij is opgenomen in de gegevensbestanden van de Fraudehelpdesk en daardoor heeft de betrokkene geen mogelijkheden verweer te voeren tegen (een al dan niet onterechte) opname.[25] Er is weliswaar een klachtenregeling opgenomen en de rechten van betrokkene zijn in het protocol opgenomen, maar die zijn illusoir als de betrokkene niet van opname op de hoogte is. Ter illustratie: als het rekeningnummer van een betrokkene in de IBAN-check database is opgenomen en de betrokkene hiervan niet op de hoogte is, kan het zijn dat potentiële zakelijke relaties van de betrokkene geen zaken met de betrokkene doet. Door het ontbreken van waarborgen rond de opname in de systemen kan de betrokkene ook onterecht zijn opgenomen, bijvoorbeeld omdat kwaadwillenden onterechte (maar overtuigende) meldingen hebben gedaan. Zonder dat de betrokkene het weet is hij dan benadeeld. Dit is in strijd met de verplichting van verwerkingsverantwoordelijken de juistheid van gegevens te waarborgen.

5.4 Zorgvuldig ontwerp voorgenomen verwerking

56. De AP heeft over een langere periode voorlichting geboden aan Safecin over het protocol.[26] In die periode is de AVG van toepassing geworden en zijn aanvullende bepalingen van kracht geworden om verwerkingsverantwoordelijken zorgvuldig gegevensverwerkingen te laten ontwerpen. De AP heeft Safecin erop gewezen dat de voorgenomen verwerking DPIA-plichtig is. De AP is van oordeel dat de DPIA die onderdeel uitmaakt van de vergunningaanvraag niet voldoet aan de eisen van artikel 35, zevende lid, AVG. In de DPIA worden geen verwerkingsdoeleinden beschreven en worden evenmin verwerkingsgrondslagen, waaronder de gerechtvaardigde belangen die de verwerkingsverantwoordelijke beoogt de behartigen, uitgewerkt. Tevens ontbreekt een beoordeling van de noodzaak en de evenredigheid van de verwerkingen. De risico's voor de rechten en vrijheden van betrokkenen worden wel beschreven, maar niet beoordeeld. Daardoor is niet duidelijk waarom bepaalde risico's als 'hoog' of 'zeer hoog' worden benoemd en andere (kennelijk) als 'laag' of 'normaal'. Tot slot worden er wel technische en organisatorische beveiligingsmaatregelen uitgewerkt, maar worden er geen maatregelen uitgewerkt die strekken ter bescherming van de rechten en vrijheden van betrokkenen. Dit betekent dat niet duidelijk is of en op welke wijze de als 'hoog' of 'zeer hoog' benoemde risico's worden weggenomen. De AP kan daarom de conclusie uit de DPIA niet volgen dat er geen hoge restrisico's meer zijn voor betrokkenen. De AP is dan ook van oordeel dat Safecin, alvorens een vergunning aan te vragen, de AP formeel om advies in de vorm van een voorafgaande raadpleging conform artikel 36 AVG had moeten vragen.

6 Conclusie

57. Safecin heeft naar aanleiding van de wens om informatie over fraude uit te wisselen de Fraudehelpdesk in het leven geroepen. Hiermee beoogt zij de Nederlandse samenleving te behoeden en weerbaarder te maken voor financieel-economische criminaliteit en om daarmee (verdere) schade onder burgers en het bedrijfsleven te voorkomen. De aangedragen grondslag voor de voorgenomen verwerking van persoonsgegevens van strafrechtelijke aard is gelegen in het zwaarwegende belang van derden, zijnde burgers en bedrijfsleven, om fraude tegen te gaan. De AP is van oordeel dat Safecin de noodzaak en proportionaliteit van de voorgenomen verwerking

[25] Een dergelijke informatieplicht volgt uit de artikelen 12-14 van de AVG.
[26] Zie paragraaf 2 'Procedureverloop'.

onvoldoende heeft aangetoond. Daarnaast heeft Safecin niet voldaan aan de verantwoordingsplichten in de AVG.

58. De AP wijst de aanvraag ter verlening van een vergunning 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.

7 Afsluiting en rechtsmiddel

Indien u het niet eens bent met dit besluit kunt u binnen zes weken na de datum van verzending van het besluit ingevolge de Awb een bezwaarschrift indienen bij de Autoriteit Persoonsgegevens. U kunt een bezwaarschrift indienen per post door deze te zenden naar Postbus 93374, 2509 AJ Den Haag, onder vermelding van "Awb-bezwaar" op de envelop. U kunt ook een digitaal bezwaarschrift indienen, zie www.autoriteitpersoonsgegevens.nl. onder het kopje "Bezwaar maken tegen een besluit". Het indienen van een bezwaarschrift schort de werking van dit besluit niet op.

Den Haag, 19 juni 2019

Autoriteit Persoonsgegevens,
Overeenkomstig het door de Autoriteit Persoonsgegevens genomen besluit,

ir. C.M. Schut
Directeur Systeemtoezicht, Beveiliging en Technologie