CONSIDERATI

Cross-sectorale gegevensdeling tussen private partijen voor fraudebestrijding

Ministerie van Justitie en Veiligheid

13 mei 2019

mr. dr. Bart W. Schermer
Chief Knowledge Officer

mr. Tessa Schop, CIPM
Juridisch Adviseur

Inhoudsopgave

Managementsamenvatting

Probleemstelling

Al enige tijd wordt door de Tweede Kamer gesproken over de vraag of een fraudepreventiesysteem waarin private partijen cross-sectoraal gegevens uitwisselen ten behoeve van fraudebestrijding juridisch wenselijk en haalbaar is. Meer specifiek gaat het om de vraag hoe de belangen van fraudepreventie zich verhouden tot de bescherming van de privacy en persoonsgegevens van betrokkenen in een dergelijk systeem.

Om meer zicht te krijgen op de juridische mogelijkheden en onmogelijkheden van cross-sectorale gegevensdeling, heeft het Ministerie van Justitie en Veiligheid Considerati gevraagd een juridische analyse uit te voeren ten aanzien van de eisen aan private cross-sectorale gegevensdeling binnen het Nederlandse rechtsbestel.

In het maatschappelijk debat over fraudepreventie wordt het in het Verenigd Koninkrijk ('VK') bestaande cross-sectorale fraudepreventiesysteem 'Cifas' regelmatig aangehaald als inspiratiebron en geopperd om een vergelijkbaar systeem te implementeren in Nederland. Om die reden heeft het Ministerie van Justitie en Veiligheid Considerati ook gevraagd om het Cifas systeem te beschrijven en de Nederlandse situatie te vergelijken met de situatie van informatie-uitwisseling onder Cifas in het VK.

Juridisch kader

Wanneer private partijen cross-sectoraal gegevens delen ten behoeve van fraudebestrijding vinden allerlei verwerkingen van persoonsgegevens plaats. Indien persoonsgegevens worden verwerkt, is daarop de Algemene Verordening Gegevensbescherming ('AVG') van toepassing.

Wil een cross-sectorale gegevensdeling tussen private partijen ten behoeve van fraudebestrijding in lijn zijn met de AVG, dan moet er:

- Een duidelijk omschreven doel zijn voor de verwerking;
- Een rechtmatige grondslag op grond van artikel 6 AVG zijn; én
- Een uitzondering zijn op het verwerkingsverbod voor strafrechtelijke gegevens.

Indien aan de bovenstaande rechtmatigheidseisen is voldaan, dan moet de verwerking vervolgens voldoen aan de zorgvuldigheidsvereisten. Hierbij moet gedacht worden aan het treffen van voldoende beveiligingsmaatregelen, het vereiste van dataminimalisatie, het vereiste om transparant te zijn over de gegevensverwerking en de kwaliteit van de gegevens.

In het kader van fraudebestrijding worden veelal strafrechtelijke gegevens verwerkt. Voor deze verwerkingen bestaat een algemeen verwerkingsverbod. De uitzonderingen op dit verwerkingsverbod zijn primair nationaalrechtelijk in uitvoeringswetgeving geregeld. In Nederland is dit de Uitvoeringswet AVG ('UAVG') in het VK de UK Data Protection Act 2018. De regels voor de verwerking van strafrechtelijke gegevens verschillen daarmee tussen Nederland en het VK.

Cross-sectorale gegevensdeling in Nederland

Privaat - privaat

De AVG en UAVG bieden juridische mogelijkheden om cross-sectoraal gegevens te delen tussen private partijen ten behoeve van het bestrijden van fraude. De juridische mogelijkheden vereisen wel dat op grond van artikel artikel 33 lid 4 sub c en 5 UAVG een vergunning wordt aangevraagd bij de Autoriteit Persoonsgegevens. Deze vergunning dient aangevraagd te worden door de private partijen die gegevens willen gaan delen (de verwerkingsverantwoordelijken) (p. 12 – 18; 45 – 47).

Het kan zijn dat de private partijen de gegevensdeling graag wensen in te richten in samenwerking met een externe organisatie, die optreedt als beheerder. Deze beheerder deelt zelf geen persoonsgegevens met organisaties teneinde fraude te bestrijden, maar faciliteert de gegevensdeling.
De rol van beheerder als facilitator kan verschillend zijn ingericht. Zo kan de beheerder uitsluitend een verwerker zijn, maar kan het ook zijn dat de beheerder gezamenlijk met de andere organisaties verwerkingsverantwoordelijke is. Dit is afhankelijk van de wijze waarop de cross-sectorale gegevensdeling wordt ingericht (p. 16 – 17).

Privaat - publiek
Er bestaan ook mogelijkheden op grond van de AVG en UAVG om publieke organisaties te laten deelnemen aan de cross-sectorale gegevensdeling ten behoeve van het bestrijden van fraude. Nu in Nederland geen algemene wettelijke bepaling bestaat op grond waarvan publieke organisaties mogen deelnemen, dient per publieke partij beoordeeld te worden of conform artikel 6 lid 1 sub e AVG een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag in de wet aan de betreffende partij is toebedeeld. Beoordeeld dient te worden of deze taak ook zo ver reikt dat aan alle organisaties die deelnemen aan de cross-sectorale gegevensdeling gegevens verstrekt mogen worden en de publieke partij ook gegevens mag ontvangen van al deze organisaties. Indien de wens bestaat dat opsporingsdiensten als politie en bijzondere opsporingsdiensten als de FIOD gaan deelnemen aan de cross-sectorale gegevensdeling, dan dient aan de hand van de Wet politiegegevens beoordeeld te worden of een wettelijke basis bestaat om gegevens te verstrekken aan de organisaties die deelnemen aan de gegevensdeling (p. 19 – 21).

Op het moment wordt gewerkt aan de Wet gegevensverwerking door samenwerkingsverbanden ('WGS'). Dit conceptwetsvoorstel is nog in voorbereiding en dan ook nog niet aangenomen door de Kamer. Indien deze wet wordt aangenomen kan dit mogelijk een eenvoudigere juridische basis bieden dan op dit moment onder huidige wetgeving het geval is om een privaat-publiek samenwerkingsverband in te richten met het doel om fraude te bestrijden. De conceptwet biedt de mogelijkheid om een verband in te richten waarbij zowel private als publieke partijen kunnen deelnemen; een publieke partij dient wel altijd onderdeel te zijn van de samenwerking (p. 20).

Verstrekking aan opsporingsinstanties
Naast het in kaart brengen van het juridisch kader met betrekking tot het cross-sectoraal delen van gegevens tussen private partijen en daarnaast de mogelijke deelname van publieke partijen, is ook nader gekeken naar de juridische mogelijkheden voor politie en eventuele andere opsporingsinstanties, als de FIOD, om gegevens te ontvangen vanuit de cross-sectorale gegevensdeling ten behoeve van de bestrijding en opsporing van fraude. De opsporingsinstanties zijn in voornoemde situatie niet zelf deelnemer aan de cross-sectorale gegevensdeling tussen private partijen, maar ontvangen gegevens vanuit deze gegevensdeling. De UAVG biedt verwerkingsverantwoordelijken op grond van artikel 33 lid 2 sub b UAVG de mogelijkheid om gegevens te verstrekken aan politie en/of FIOD om aangifte te doen, danwel opsporingsinstanties op de hoogte te brengen van hetgeen is voorgevallen. Deze juridische basis is gericht aan de verwerkingsverantwoordelijke zelf en rechtvaardigt niet dat de gegevens vanuit de cross-sectorale gegevensdeling van alle organisaties gezamenlijk in één keer worden verstrekt aan politie en/of FIOD. Indien cross-sectoraal gegevens gedeeld gaan worden en dit mogelijk gebeurt door middel van een fraudepreventiesysteem, dient goed gekeken te worden hoe de verstrekking aan de opsporingsinstanties technisch wordt ingericht, zodat de verwerkingsverantwoordelijke degene is die de gegevens verstrekt aan politie en/of FIOD (p. 21 – 22).

Cross-sectorale gegevensdeling in het Verenigd Koninkrijk - het systeem Cifas

In het VK bestaat al ruim 30 jaar een fraudepreventiesysteem, dat wordt beheerd door de organisatie Cifas. Cifas beheert meerdere databases, waaronder een National Fraud database en een Internal Fraud database, waarin door zowel private als publieke organisaties gegevens gedeeld worden ten behoeve van fraudebestrijding. Circa 400 organisaties uit de private sector en enkele uit de publieke sector delen gegevens en inlichtingen met elkaar middels de databases van Cifas. Organisaties die afkomstig zijn uit allerlei

verscheidende sectoren kunnen 'lid' worden van deze databases en op deze manier gegevens met elkaar uitwisselen ten behoeve van het bestrijden van fraude.

Juridische basis Cifas
Op grond van de AVG en de Data Protection Act 2018 bestaat een juridische basis voor de gegevensverwerkingen die plaatsvinden in de databases van Cifas. In het VK is in de Data Protection Act 2018 een uitzondering opgenomen waaronder deelnemers van een 'anti-fraud organisation', als Cifas, strafrechtelijke persoonsgegevens mogen verwerken ten behoeve van het bestrijden van fraude, zonder dat daartoe een vergunning wordt aangevraagd bij de ICO, de toezichthouder in het VK. Met de term 'anti-fraud organisation' wordt gedoeld op dezelfde term als die gebruikt wordt in de Serious Crime Act 2007. In artikel 68 van de Serious Crime Act 2007 wordt een 'anti-fraud organisation' omschreven als een organisatie die het mogelijk maakt informatie te delen ten behoeve van het bestrijden van fraude of de bestrijding van een bepaalde vorm van fraude of die één van deze functies als doel of als één van zijn doelen heeft. In de Code of Practice die opgesteld is op grond van artikel 71 Serious Crime Act 2007 en gelezen dient te worden in samenhang met de Serious Crime Act, is Cifas expliciet benoemd als een 'anti-fraud organisation' (p. 32 – 33).

Publieke partijen
Zoals uit het voorgaande blijkt, nemen ook publieke organisaties deel aan de databases van Cifas. Naast dat publieke organisaties deelnemer kunnen zijn van Cifas, zijn er ook publieke organisaties die gegevens verstrekken aan Cifas zonder dat zij zelf deelnemer van Cifas zijn. De juridische basis voor deelname van deze publieke organisaties en voor de gegevensverstrekkingen van publieke organisaties die geen deelnemer zijn, is in het VK vastgelegd in de Serious Crime Act 2007. Op grond van de Serious Crime Act 2007 mogen gegevens verstrekt worden aan Cifas, de leden van Cifas of enig ander persoon aan wie de verstrekking op grond van de regelingen van Cifas is toegestaan (p. 33).

Verstrekking aan opsporingsinstanties
Vanuit de 'National Fraud' database, één van de databases van Cifas, worden daarnaast rechtstreeks gegevens verstrekt aan enkele opsporingsinstanties. Op dagelijkse basis worden automatisch rapporten doorgestuurd aan deze opsporingsinstanties waarin nieuwe fraudezaken zijn opgenomen, die zijn ingevoerd in de database door de deelnemende partijen. Cifas heeft aangegeven dat de grondslag voor de verstrekking aan de opsporingsinstanties plaatsvindt ten behoeve van het gerechtvaardigd belang, artikel 6 lid 1 sub f AVG. Daarnaast bestaat volgens Cifas voor deze verstrekking ook een grondslag in artikel 6 lid 1 sub e AVG, een taak van algemeen belang. Cifas heeft aangegeven dat deze taak van algemeen belang aan hen is toebedeeld in de Data Protection Act 2018 (p. 33 - 34).

Naast het hebben van een juridische basis, moeten op grond van de AVG ook altijd waarborgen worden getroffen om de persoonlijke levenssfeer van de betrokkenen te beschermen. De waarborgen die Cifas treft om de persoonlijke levenssfeer van de betrokkenen te beschermen zijn vastgelegd in acht principes die zij hebben ontwikkeld. Deze principes zijn nader uitgewerkt in een Handboek dat geldt voor alle deelnemende partijen aan Cifas. De deelnemers dienen naleving van de principes en het Handboek te waarborgen (p. 35 – 37).

Toepasbaarheid systeem Cifas in Nederland

Het fraudepreventiesysteem waarvan gebruik wordt gemaakt in het VK kan niet één-op-één overgenomen worden in Nederland. De belangrijkste reden waarom het fraudepreventiesysteem zoals dat gebruikt wordt in het VK niet overgenomen kan worden in Nederland, is omdat de uitzonderingsgronden voor het verwerken van strafrechtelijke persoonsgegevens in Nederland en het VK verschillend zijn ingericht. In het VK is in de Data Protection Act 2018 een specifieke bepaling opgenomen op basis waarvan het voor een 'anti-fraud organisation', als Cifas, en zijn deelnemers mogelijk is om strafrechtelijke gegevens te verwerken om fraude te bestrijden. In Nederland zijn de uitzonderingsgronden voor het verwerken van strafrechtelijke

persoonsgegevens anders ingeregeld. Op grond van de UAVG is het mogelijk om cross-sectoraal gegevens te delen ten behoeve van het bestrijden van fraude indien de organisaties, die mogelijk gegevens willen gaan delen, daartoe een vergunning aanvragen bij de Autoriteit Persoonsgegevens. Om cross-sectorale gegevensdeling in Nederland mogelijk te maken dient dan ook een vergunningstraject doorlopen te worden waarbij de Autoriteit Persoonsgegevens voorafgaand aan de verwerking toetst of deze in lijn is met de AVG. Door de wijze waarop de uitzonderingsgronden in het VK zijn ingericht, hebben de partijen daar voorafgaand aan de verwerking géén vergunning hoeven aanvragen bij de toezichthouder in het VK, de ICO, en hebben zij met elkaar en met de beheerder, Cifas, de gegevensdeling zelfstandig kunnen inrichten (p. 39 – 40).

Daarnaast is in het VK in de Serious Crime Act 2007 een wettelijke basis neergelegd op basis waarvan publieke organisaties als deelnemer gegevens mogen verstrekken aan de databases van Cifas ten behoeve van het bestrijden van fraude. Publieke organisaties, die zelf geen deelnemer zijn aan de databases van Cifas, mogen op basis van deze bepaling ook gegevens verstrekken aan Cifas. In Nederland kennen wij een dergelijke algemene juridische basis niet waardoor niet zonder meer gezegd kan worden dat in Nederland ook de mogelijkheid bestaat dat publieke organisaties mogen deelnemen aan een eventuele cross-sectorale gegevensdeling. Per publieke organisatie dient beoordeeld te worden of zij een grondslag, als bedoeld in art. 6 AVG hebben, om deel te kunnen nemen aan de cross-sectorale gegevensdeling. Voor politie en bijzondere opsporingsdiensten dient dit beoordeeld te worden op basis van de Wet politiegegevens. (p. 40 – 41).

Hoewel in het VK een wettelijke basis bestaat voor de inrichting van Cifas en de ICO (vooralsnog) geen aanleiding ziet tot handhaving, wil dat niet zeggen dat de wijze waarop Cifas is ingericht binnen de Nederlandse context ook automatisch rechtmatig is en tot een vergunning van de Autoriteit Persoonsgegevens leidt. De AVG is weliswaar een Europese verordening die voor alle lidstaten van de Europese Unie gelijk is, maar de AVG heeft de lidstaten wel op een aantal punten ruimte gelaten om specifieke bepalingen op te nemen of uitzonderingen te maken. Zo zijn de lidstaten, zoals hiervoor al aangegeven, vrij geweest om in hun nationale uitvoeringswetten bepalingen op te nemen waaronder bijzondere en strafrechtelijke persoonsgegevens verwerkt mogen worden. Politieke en maatschappelijke overwegingen die spelen in afzonderlijke lidstaten zullen bij de formulering van deze uitzonderingsgronden van belang zijn geweest. De AVG bevat daarnaast geen specifieke set aan regels, maar veeleer principes waaraan moet worden voldaan wanneer gegevens verwerkt worden. Deze principes zijn geformuleerd als open normen en kunnen daarom verschillend worden ingevuld. Het is aan de toezichthouder van een lidstaat om te bepalen of op juiste wijze invulling wordt gegeven aan deze principes en of er dan ook voldoende waarborgen zijn getroffen om de persoonlijke levenssfeer te beschermen. Vanuit de European Data Protection Board (EDPB), waarin alle toezichthouders zijn verenigd, zijn richtlijnen gegeven, dan wel worden richtlijnen gegeven hoe deze principes ingevuld dienen te worden, maar er blijft een bepaalde interpretatieruimte voor lidstaten bestaan. Het kan dan ook zijn dat het VK bepaalde waarborgen als afdoende beschouwt, terwijl de Nederlandse toezichthouder dat anders beoordeelt. Of de wijze waarop Cifas op dit moment is ingericht ook in Nederland rechtmatig is, moet zelfstandig worden beoordeeld. Hierbij is de specifieke Nederlandse situatie maatgevend, niet de situatie in het VK.

Mogelijkheden inrichting cross-sectorale gegevensdeling Nederland

Dat Cifas niet één-op-één overgenomen kan worden in Nederland, betekent echter niet dat in Nederland geen juridische mogelijkheden bestaan om tussen private partijen cross-sectoraal gegevens te delen om fraude te bestrijden (p. 41 – 42). Hieronder worden de mogelijkheden benoemd die in Nederland bestaan op welke wijze cross-sectorale gegevensdeling wel kan plaatsvinden. Hierbij wordt meegegeven dat onderstaande paragrafen opeenvolgend gelezen dienen te worden (p. 42 – 44).

Vergunningsaanvraag AVG, UAVG

Onder de huidige wetgeving is het mogelijk om cross-sectorale gegevensdeling tussen private partijen in te richten, maar daartoe dient wel eerst door de organisaties, die gezamenlijk gegevens willen gaan delen, een

vergunningstraject zoals bedoeld in artikel 33 lid 4 sub c en 5 UAVG, in te worden gegaan. De private partijen, mogelijk met een beherende partij, die willen gaan starten met de cross-sectorale gegevensdeling dienen dan ook een vergunning aan te vragen bij de Autoriteit Persoonsgegevens. Onderdeel van deze vergunningsaanvraag is dat de organisaties eerst gezamenlijk een DPIA uitvoeren waarin de risico's van de cross-sectorale gegevensdeling voor de betrokkenen in kaart worden gebracht, alsmede de maatregelen die genomen worden om deze risico's te verkleinen. Daarnaast dienen de organisaties ook gezamenlijk een privacy protocol op te stellen over de cross-sectorale gegevensdeling. Afhankelijk van de uitkomsten van de DPIA, kan vastgesteld worden hoe het vergunningstraject verder moet worden vervolgd. Zie voor meer informatie over de wijze waarop de gegevensdeling ingericht kan worden hoofdstuk 3 en de wijze waarop een vergunningsaanvraag dient plaats te vinden bijlage I - Aanvraag vergunning UAVG (p. 16- 27; p. 42 – 43; 46 – 47).

Oprichting privaat-publiek samenwerkingsverband onder WGS

Op het moment wordt nog gewerkt aan het conceptwetsvoorstel WGS. Indien deze wet wordt aangenomen en in werking treedt, kan op basis van deze wet ook gekozen worden om een privaat- publiekrechtelijk samenwerkingsverband in te richten ten behoeve van het algemeen belang om fraude te bestrijden. Bij AMvB dienen nadere regels gesteld te worden welke organisaties, privaat en publiek, deelnemen aan de samenwerking, ten behoeve van welk doel deze samenwerking plaatsvindt en onder welke voorwaarden en welke waarborgen getroffen worden bij deze samenwerking (p. 43).

Wetswijziging UAVG

Indien op termijn zou blijken dat bovenstaande juridische mogelijkheden verbetering behoeven en er een politieke en maatschappelijke wens bestaat deze verbeteringen door te voeren, dan kan bijvoorbeeld via een wetswijziging in de UAVG een zelfstandige wettelijke basis voor cross-sectorale gegevensdeling (p. 43 – 44) worden gecreëerd. Hierbij zijn twee verschillende wetswijzigingen mogelijk:

1. Een mogelijkheid is om in aanvulling op artikel 33 lid 4 sub c en lid 5 UAVG een specifiek kader te creëren dat van toepassing is wanneer een vergunning aangevraagd wordt teneinde (cross-sectoraal) gegevens te gaan delen ten behoeve van fraudebestrijding. In dit specifieke kader dient nader uitgewerkt te worden aan welke randvoorwaarden en waarborgen een vergunningaanvraag dient te voldoen wanneer organisaties (cross-sectoraal) gegevens willen gaan delen ten behoeve van fraudebestrijding. Deze randvoorwaarden en waarborgen geven organisaties de ruimte en geeft hen meer concrete handvatten om de gegevensdeling in te richten. De waarborgen die in dit specifieke kader zijn opgenomen zorgen ervoor dat, net als bij publiekrechtelijke samenwerkingsverbanden waarbij veelal een wet aan ten grondslag ligt, bij de gegevensdeling meer waarborgen worden getroffen om te spreken van een zorgvuldige verwerking. Het kader dwingt organisaties ertoe om deze waarborgen ook daadwerkelijk in de praktijk te verankeren. De Autoriteit Persoonsgegevens behoudt uiteraard de mogelijkheid van voorafgaande toetsing en dient te oordelen over de vergunningaanvraag.
2. Daarnaast kan overwogen worden om de UAVG te wijzigen en de uitzonderingsgrond, zoals die nu is opgenomen in de Data Protection Act 2018, over te nemen in de UAVG. De overname van deze bepaling in de Nederlandse UAVG, betekent dat een nieuwe uitzonderingsgrond wordt gecreëerd om strafrechtelijke gegevens te verwerken zonder dat een vergunningaanvraag bij de Autoriteit Persoonsgegevens nodig is. Net als in het VK wordt het aanbevolen om bij besluit of in een nadere regeling uit te werken welke organisaties deze gegevens mogen verwerken, zodat duidelijk is begrensd welke organisaties ten behoeve van welk doel strafrechtelijke gegevens mogen verwerken. De toevoeging van deze uitzonderingsgrond in de UAVG laat uiteraard onverlet dat de Autoriteit Persoonsgegevens te allen tijde de bevoegdheid behoudt om, zelfstandig of op verzoek van betrokkenen, toezicht te houden.

1 Inleiding

1.1 Aanleiding

Al enige tijd wordt in Nederland, onder andere door de Tweede Kamer, gesproken of een fraudepreventiesysteem, waarin private partijen gegevens uitwisselen, zoals dat in het Verenigd Koninkrijk ('VK') wordt gebruikt, ook dienstbaar zou zijn ten behoeve van de bestrijding van fraude in Nederland. In het VK bestaat al ruim 30 jaar een fraudepreventiesysteem, dat wordt beheerd door de organisatie Cifas. Cifas beheert meerdere databases, waaronder een National Fraud database en een Internal Fraud database, waarin door organisaties gegevens gedeeld worden ten behoeve van fraudebestrijding. Organisaties die afkomstig zijn uit allerlei verscheidende sectoren kunnen 'lid' worden van deze databases en op deze manier gegevens met elkaar uitwisselen.

Tijdens het Algemeen Overleg financieel-economische criminaliteit op 4 oktober 2018 is aan de orde gesteld in hoeverre het fraudepreventiesysteem Cifas ook mogelijkheden biedt voor de Nederlandse situatie.[1] Hierbij is een belangrijke voorwaarde dat een fraudebestrijdingssysteem naar het VK-model in lijn is met de Algemene Verordening Gegevensbescherming ('AVG') en de Uitvoeringswet Algemene Verordening Gegevensbescherming ('UAVG').

Om meer inzicht te verkrijgen in de juridische (on)mogelijkheden met betrekking tot het cross-sectoraal gegevens delen ten behoeve van het bestrijden van fraude naar het VK-model, heeft het Ministerie van Justitie en Veiligheid ('Ministerie') Considerati gevraagd een juridische analyse uit te voeren ten aanzien van de eisen aan private cross-sectorale gegevensdeling binnen het Nederlandse rechtsbestel en daarnaast het systeem in het VK, dat wordt beheerd door Cifas, in kaart te brengen. Meer specifiek heeft het Ministerie gevraagd om:

- Een juridische analyse te maken van de eisen aan cross-sectorale gegevensdeling binnen het Nederlandse rechtsbestel:
  a. tussen private partijen op het gebied van fraudebestrijding;
  b. tussen private partijen, zoals hiervoor omschreven, in het geval dat een publieke partij, met name de politie (eventuele uitbreiding met andere opsporingsinstanties zoals FIOD), gegevens/resultaten van genoemde cross-sectorale gegevensdeling tussen private partijen ontvangt.
- Het systeem in het VK, dat wordt beheerd door Cifas, te beschrijven;
- De Nederlandse situatie te vergelijken met de situatie van informatie-uitwisseling onder Cifas in het VK.

Daarnaast is op 13 maart 2018 de motie Koopmans c.s.[2] aangenomen waarin de regering wordt verzocht om een halfjaar na het van toepassing worden van de AVG en UAVG te berichten over de ervaringen met onder andere de privacyaspecten rondom het branchebreed aanleggen van zwarte lijsten van fraudeurs en over haar voornemens inzake de aanpak daarvan, zo nodig door middel van nieuwe wetgeving. Onderhavig rapport kan bijdragen aan het verkrijgen van inzicht omtrent de privacyaspecten die spelen rondom het branchebreed aanleggen van zwarte lijsten van fraudeurs.

[1] Kamerstukken II 2018/2019, 29911, nr. 210
[2] Kamerstukken II 2017/2018, 34851, nr. 19, *Motie Koopmans*

1.2 Aanpak

Om bovenstaande vragen te kunnen beantwoorden wordt in dit rapport de volgende aanpak gehanteerd:

1) Het Europeesrechtelijke kader voor het cross-sectoraal delen van persoonsgegevens tussen private partijen wordt in kaart gebracht (De AVG). Deze analyse wordt vervolgens toegespitst op de Nederlandse situatie (de UAVG). Hetzelfde wordt gedaan voor de situatie in het VK.
2) Vervolgens wordt gekeken hoe een cross-sectorale gegevensverwerking ingericht kan worden. Nu in Nederland nog geen concrete inrichting van cross-sectorale gegevensverwerking bestaat, is gekeken naar het in het VK geldende Cifas systeem en wordt beoordeeld in hoeverre het Cifas systeem toepasbaar is in Nederland.
3) Tenslotte wordt op basis van het onder 1 geschetste kader getoetst wat de juridische basis kan zijn voor het cross-sectoraal delen van gegevens binnen Nederland, uitgaande van verschillende mogelijkheden.

1.3 Methodologie

Dit rapport is gebaseerd op deskresearch aangevuld met interviews. Om het juridisch kader in Nederland zo goed mogelijk in kaart te brengen, zijn gesprekken gevoerd met vertegenwoordigers binnen het Ministerie van Justitie en Veiligheid en de Autoriteit Persoonsgegevens.

De informatie met betrekking tot het fraudepreventiesysteem in het VK is opgehaald tijdens een telefonisch overleg met medewerkers van de organisatie Cifas en tijdens daaropovolgende informatieuitvragen aan Cifas. Daarnaast heeft e-mailcontact met de Information Commissioner Office ('ICO'), de toezichthouder in het VK, plaatsgevonden. De informatie met betrekking tot de databases van Cifas en de juridische basis op grond waarvan de gegevens in deze databases verwerkt worden, is volledig aangeleverd door de organisatie Cifas zelf.

1.4 Leeswijzer

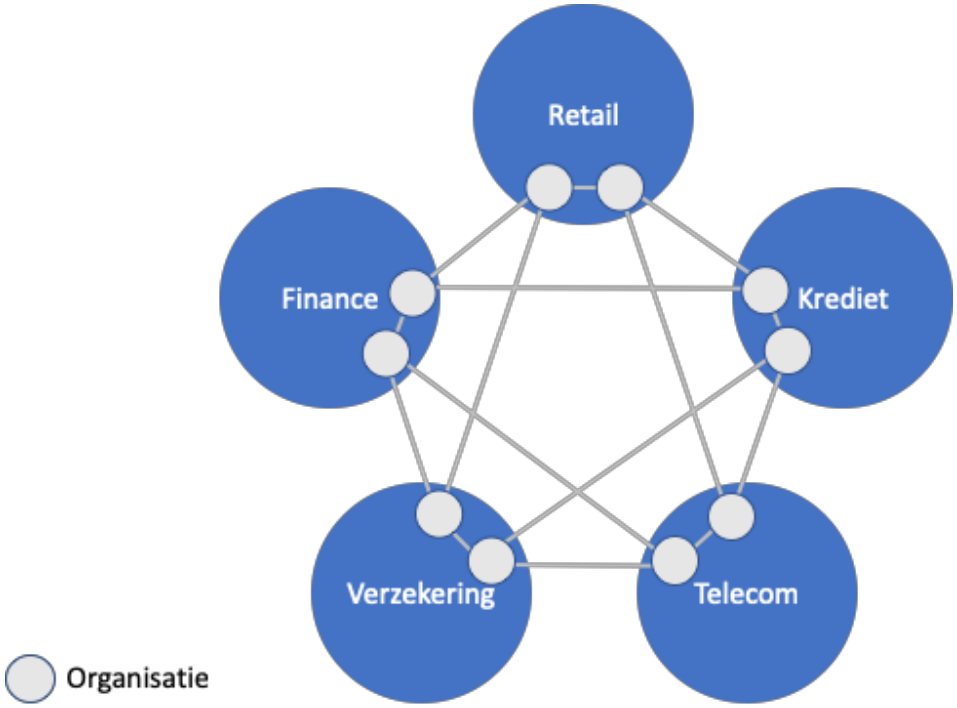
In het volgende hoofdstuk wordt kort ingegaan op de wetgeving die binnen de Europese Unie van toepassing is wanneer private partijen cross-sectoraal gegevens met elkaar delen. Daarna wordt dit juridisch kader toegepast op het Nederlandse rechtsbestel en wordt nader ingegaan op de eisen die gesteld worden aan cross-sectorale gegevensdeling tussen private partijen ten behoeve van het bestrijden van fraude. In hoofdstuk 4 wordt voorts een beschrijving gegeven van het fraudepreventiesysteem in het VK, dat beheerd wordt door Cifas, en wordt daarbij het juridisch kader beschreven. In hoofdstuk 5 wordt de vergelijking gemaakt tussen Cifas en de Nederlandse situatie en worden enkele scenario's geschetst hoe cross-sectorale gegevensdeling tussen private partijen in Nederland vormgegeven kan worden.

2 Juridisch kader

2.1 Algemene Verordening Gegevensbescherming

Zoals blijkt uit de aanleiding (1.1) staat in onderhavig rapport het cross-sectoraal delen van persoonsgegevens tussen private partijen ten behoeve van het bestrijden van fraude in zowel Nederland als het VK centraal. Met cross-sectoraal gegevens delen wordt bedoeld dat gegevens worden gedeeld tussen private partijen die afkomstig zijn uit allerlei verschillende sectoren; dus over de grenzen van de eigen sector heen. Indien private partijen cross-sectoraal gegevens delen kan deze deling verschillende vormen aannemen: het verstrekken van informatie aan organisaties, het bevragen van organisaties om informatie, het ontvangen van informatie van organisaties, het antwoorden aan organisaties en in sommige gevallen kan afstemming plaatsvinden tussen organisaties om bijvoorbeeld nadere informatie op te vragen.

Visueel gezien kan cross-sectorale gegevensdeling als volgt worden weergeven:



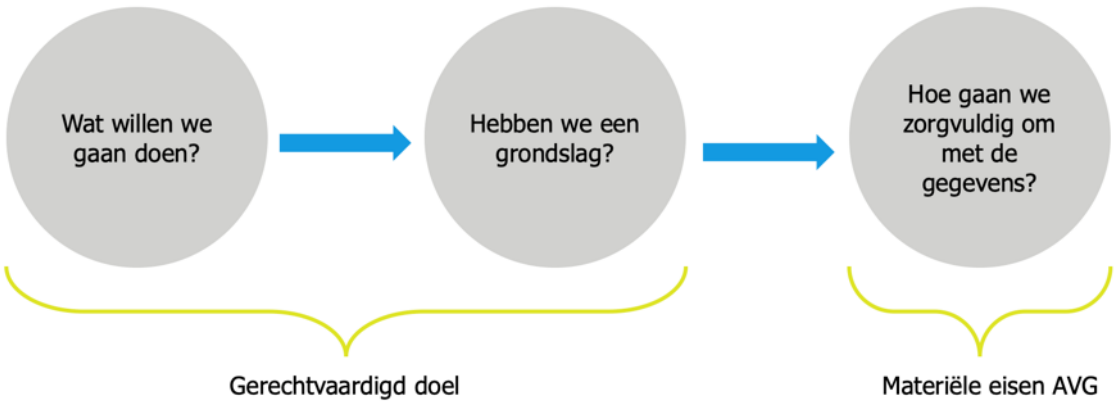
Wanneer private partijen cross-sectoraal gegevens delen ten behoeve van fraudebestrijding vinden allerlei verwerkingen van persoonsgegevens[3] plaats.

[3] Persoonsgegevens worden in de AVG gedefinieerd als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Een natuurlijk persoon is identificeerbaar wanneer deze direct of indirect kan worden geïdentificeerd aan de hand van één of meerdere gegevens. Dit betekent dat zowel gegevens die over een persoon gaan als gegevens die naar een natuurlijk persoon te herleiden zijn, onder de AVG vallen. Denk daarbij bijvoorbeeld aan NAW-gegevens, e-mailadressen, geboortedatum maar ook een IP-adres kan een persoonsgegevens zijn. Om te spreken van identificeerbaarheid is het niet noodzakelijk dat de naam van de persoon ook bekend is: als iemand uniek kan worden onderscheiden in een groep mensen, dan is deze persoon identificeerbaar en zijn de gegevens persoonsgegevens. De AVG is alleen van toepassing op de verwerking van gegevens over natuurlijke personen. Gegevens over rechtspersonen zijn géén persoonsgegevens, omdat zij geen betrekking hebben op een natuurlijke persoon. Dit is slechts anders wanneer de organisatie vereenzelvigd kan worden met een natuurlijke persoon. Zo zegt de omzet van een eenmanszaak iets over het inkomen van de eigenaar van de eenmanszaak. Wanneer u gegevens verwerkt van personen binnen een organisatie (bijvoorbeeld medewerkers), dan is er ook sprake van de verwerking van persoonsgegevens. De AVG is daarnaast ook niet van toepassing op overleden personen, omdat dit volgens de wet geen natuurlijke personen meer zijn.

Indien persoonsgegevens worden verwerkt, is daarop de AVG van toepassing en dient te worden voldaan aan de vereisten die daaruit voortvloeien. De AVG heeft rechtstreekse werking in de hele Europese Unie. De AVG is dan ook gelijk voor alle lidstaten van de Europese Unie. Hoewel de AVG rechtstreekse werking heeft, laat de AVG de lidstaten op bepaalde punten wel ruimte om specifieke bepalingen op te nemen of uitzonderingen te maken. Het gaat bijvoorbeeld om de regels over de verwerking van bijzondere categorieën van persoonsgegevens en strafrechtelijke persoonsgegevens.[4] In Nederland zijn deze specifieke bepalingen vastgelegd in de Uitvoeringswet AVG ('UAVG'). In het VK zijn deze uitzonderingen opgenomen in de Data Protection Act 2018. De AVG dient dan ook in samenhang gelezen te worden met deze nationale uitvoeringswetten.

De AVG vereist dat persoonsgegevens alleen mogen worden verwerkt voor welbepaalde, nadrukkelijk omschreven en gerechtvaardigde doeleinden. Voordat wordt begonnen met het verzamelen of anderszins verwerken van persoonsgegevens, moet vastgelegd worden waarvoor deze persoonsgegevens nodig zijn.[5]
Een doel is gerechtvaardigd als het gebaseerd kan worden op één van de grondslagen uit artikel 6 AVG. Wanneer een gerechtvaardigd doel bestaat, mogen gegevens verwerkt worden. Bij het verwerken van persoonsgegevens zelf moet vervolgens ook altijd voldaan worden aan de overige 'materiële' vereisten die voortvloeien uit de AVG. Hierbij moet gedacht worden aan het treffen van voldoende beveiligingsmaatregelen, het vereiste van dataminimalisatie, transparant zijn over de gegevensverwerking en de kwaliteit van de gegevens.[6]

Visueel kan de logica van de AVG als volgt worden weergegeven:



2.2 Doel

Zoals hierboven aangegeven mogen op grond van de AVG persoonsgegevens slechts verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. Persoonsgegevens mogen dan ook niet verwerkt worden zonder dat daarvoor een doel is bepaald; gegevens verzamelen omdat deze mogelijk in de toekomst nog weleens van pas kunnen komen is dan ook niet toegestaan. Wel mogen persoonsgegevens verwerkt worden voor meerdere doelen tegelijkertijd; de verschillende doelen dienen in dat geval wel duidelijk te zijn bepaald. Het doel of de doelen waarvoor de gegevens worden verwerkt moeten uitdrukkelijk

[4] Ministerie van Justitie en Veiligheid, Handleiding Algemene Verordening Gegevensbescherming en Uitvoeringswet Algemene Verordening Gegevensbescherming, p. 19.
[5] Artikel 5 lid 1 sub b AVG, overweging 39 AVG. Ministerie van Justitie en Veiligheid, Handleiding Algemene Verordening Gegevensbescherming en Uitvoeringswet Algemene Verordening Gegevensbescherming, p. 35.
6 Ministerie van Justitie en Veiligheid, Handleiding Algemene Verordening Gegevensbescherming en Uitvoeringswet Algemene Verordening Gegevensbescherming, p. 36.

omschreven zijn. Dit betekent dat, voordat gestart wordt met de verwerking, moet zijn vastgelegd waarvoor de persoonsgegevens nodig zijn.

2.3 Grondslag art. 6 AVG

Om het doel gerechtvaardigd te maken, dient het gebaseerd te kunnen worden op één van de grondslagen genoemd in artikel 6 AVG. Persoonsgegevens mogen volgens artikel 6 AVG worden verwerkt indien:

a) de ondubbelzinnige toestemming van de betrokkene is verkregen;
b) dit noodzakelijk is voor de uitvoering van een overeenkomst;
c) dit noodzakelijk is voor het voldoen aan een wettelijke verplichting;
d) dit noodzakelijk is ter vrijwaring van de vitale belangen van de betrokkene;
e) dit noodzakelijk is voor de uitvoering van een taak in algemeen belang of voor het uitoefenen van het openbaar gezag;
f) dit noodzakelijk is voor de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, die niet worden overstemd door de belangen, rechten en vrijheden van de betrokkene.

Ten aanzien van grondslag (a) geldt dat de toestemming vrij, specifiek en geïnformeerd moet zijn. Dit houdt in dat de toestemming vrijelijk gegeven moet kunnen worden, dat de toestemming ondubbelzinnig moet zijn en dat de betrokkene voorafgaand duidelijk geïnformeerd moet zijn ten aanzien waarvan hij toestemming geeft.

Vrije toestemming houdt in dat de betrokkene ook toestemming voor de verwerking kan weigeren zonder dat daar negatieve consequenties aan zijn verbonden. Toestemming wordt veelal niet geacht vrijelijk te zijn wanneer sprake is van een ongelijke verhouding tussen betrokkene en de verwerkingsverantwoordelijke. Hiervan is vaak sprake wanneer de verwerkingsverantwoordelijke een overheidsinstantie betreft, omdat mensen zich niet snel vrij zal voelen om toestemming te weigeren, dan wel omdat er toch negatieve consequenties verbonden zijn aan een weigering. Wanneer een overheidsinstantie een verwerking toch baseert op basis van toestemming van een betrokkene, dient goed beargumenteerd te worden waarom sprake is van een vrije toestemming en moeten hiervoor de juiste waarborgen worden getroffen.

Betrokkenen dienen daarnaast over alle informatie te beschikken om een goede keuze te kunnen maken. Dit houdt in dat de verantwoordelijke duidelijke informatie moet verschaffen over de redenen waarom de persoonsgegevens worden verwerkt, zodat de betrokkene goed in staat wordt gesteld om toestemming te geven ten aanzien van elk van de doelen waarvoor zijn gegevens worden verwerkt. De organisatie in kwestie moet voorts kunnen aantonen dat het toestemming heeft gekregen. Het is dan ook van belang dat de verkregen toestemming goed wordt gedocumenteerd, zodat indien nodig – aan de Autoriteit Persoonsgegevens – aangetoond kan worden dat de toestemming rechtsgeldig is verkregen en er dus een grondslag was om gegevens uit te wisselen. Ten slotte moet de betrokkene de gegeven toestemming altijd kunnen intrekken.

Met betrekking tot grondslag (b) geldt dat deze alleen kan worden gebruikt wanneer de betrokkene ook partij is bij de overeenkomst. De overeenkomst hoeft niet gericht te zijn op het verwerken van de persoonsgegevens, maar de verwerking moet wel een noodzakelijk uitvloeisel van de overeenkomst zijn. Persoonsgegevens mogen ook worden verwerkt als dit noodzakelijk is om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. In deze zogenoemde precontractuele fase kan het verwerken van persoonsgegevens namelijk noodzakelijk zijn.

Ten aanzien van de grondslag (c) geldt dat de wettelijke verplichting bij wet moet zijn vastgelegd, waaronder ook het doel van de verwerking van persoonsgegevens in dit kader. Om een verwerking op deze grondslag te baseren, moet de verantwoordelijke ook daadwerkelijk onderworpen zijn aan deze wettelijke verplichting.

Een beroep op de grondslag (d) is alleen mogelijk wanneer de verwerking noodzakelijk is om de vitale belangen van de betrokkene of van een ander natuurlijk persoon te beschermen. Denk hierbij bijvoorbeeld aan een situatie waarin hulpverleners acute noodzakelijke medische hulp aan de betrokkene moeten verlenen. Alleen wanneer het niet mogelijk is de verwerking te baseren op een andere grondslag, bijvoorbeeld omdat de betrokkene buiten bewustzijn is en dan ook niet om toestemming gevraagd kan worden, is een beroep op deze grondslag mogelijk.

Ten aanzien van de grondslag (e) geldt dat de taak van algemeen belang of het openbaar gezag bij wet moet zijn vastgelegd, waaronder ook het doel van de verwerking van persoonsgegevens in dit kader. Ook moet in die wet zijn bepaald welke organisatie is belast met deze taak of aan wie het gezag is opgedragen. Dit hoeven niet per definitie publiekrechtelijke partijen te zijn. De AVG vereist niet dat voor elke afzonderlijke verwerking specifieke wetgeving is vereist; er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen die noodzakelijk zijn voor de taak van algemeen belang of de uitoefening van het openbaar gezag.[7]

Persoonsgegevens mogen tenslotte worden verwerkt als dit noodzakelijk is voor de behartiging van het gerechtvaardigde belang (f) van de verwerkingsverantwoordelijke of een derde, mits de belangen, rechten en vrijheden van de betrokkene(n) niet zwaarder wegen. Om verwerkingen op deze grondslag te kunnen baseren moet een zorgvuldige beoordeling worden gemaakt om te bepalen of sprake is van een gerechtvaardigd belang, maar ook om te bepalen of de betrokkene, gelet op het moment en de context van de verzameling van de persoonsgegevens, redelijkerwijs mag verwachten dat zijn persoonsgegevens voor dit doel worden verwerkt. Deze grondslag kan niet worden gebruikt door overheidsinstanties voor de uitvoering van hun publieke taken. De achterliggende gedachte hierachter is dat het aan de wetgever is om de rechtsgrond te creëren voor overheidsinstanties wanneer zij persoonsgegevens verwerken voor de uitvoering van hun taken. Wanneer een overheidsinstantie gegevens verwerkt anders dan ter uitvoering van hun taken, bijvoorbeeld ten behoeve van bedrijfsvoeringsactiviteiten, is een beroep op het gerechtvaardigd belang wel mogelijk.[8]

Het hebben van één grondslag is voldoende om de verwerking gerechtvaardigd te maken. Dat betekent dat private partijen uitsluitend cross-sectoraal gegevens met elkaar mogen delen wanneer zij deze verwerking kunnen baseren op één van de grondslagen zoals hierboven uiteengezet.

2.4 Strafrechtelijke persoonsgegevens

Bij het cross-sectoraal delen van gegevens tussen private partijen ten behoeve van het bestrijden van fraude, is het aannemelijk dat de betrokken partijen naast 'gewone' persoonsgegevens ook strafrechtelijke gegevens verwerken. Strafrechtelijke gegevens zijn persoonsgegevens die betrekking hebben op strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen en persoonsgegevens die betrekking hebben op een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag. Bij veroordelingen gaat het om gegevens waarbij de rechter, al dan niet onherroepelijk, strafrechtelijk gedrag heeft vastgesteld. Bij gegevens over strafbare feiten gaat het om min of meer gegronde verdenkingen van strafrechtelijk gedrag gepleegd door een persoon. Hierbij is het geen vereiste dat de gegevens uitgewisseld worden door opsporingsinstanties. Ook wanneer private partijen gegevens uitwisselen over mogelijk gepleegde strafbare feiten, kan sprake zijn van strafrechtelijke gegevens.

Bij het vaststellen wanneer sprake is van strafrechtelijke persoonsgegevens, dient niet alleen gekeken te worden naar gegevens die direct betrekking hebben op strafrechtelijke gedragingen, maar ook naar de gegevens waaruit de aanwezigheid van een strafrechtelijke gedraging kan worden afgeleid. Dat betekent dat,

[7] Artikel 6 lid 1 sub e AVG, overweging 45.

[8] Artikel 6 AVG, overwegingen 40 – 47 AVG, Ministerie van Justitie en Veiligheid, Handleiding Algemene Verordening Gegevensbescherming en Uitvoeringswet Algemene Verordening Gegevensbescherming, p. 36 – 40.

naast de gegevens die direct zien op een strafbaar feit of een strafrechtelijke veroordeling, het ook kan zijn dat bijvoorbeeld enkel een naam een strafrechtelijk gegeven kan zijn. In beginsel is een naam een gewoon persoonsgegeven, maar indien organisaties in een samenwerkingsverband een naam van een persoon delen met elkaar ten behoeve van het bestrijden van fraude, kan uit het feit dat deze persoon onderdeel is van deze gegevensdeling worden opgemaakt dat zich (mogelijk) een strafrechtelijke gedraging heeft voorgedaan, namelijk het plegen van fraude. De gegevens die in dit geval gedeeld worden kunnen dan als strafrechtelijke gegevens worden aangemerkt omdat daaruit afgeleid kan worden dat de betrokkene verdacht wordt van een strafbaar feit. Wanneer cross-sectoraal gegevens gedeeld gaan worden tussen private partijen ten behoeve van het bestrijden van fraude, worden dus gegevens verwerkt die iets zeggen over een verdenking van een strafbaar feit gepleegd door een persoon en worden strafrechtelijke persoonsgegevens uitgewisseld.

Persoonsgegevens van strafrechtelijke aard mogen slechts verwerkt worden als hier een uitzondering voor is voorzien in artikel 10 AVG in samenhang met de nationale uitvoeringswetten. Voor Nederland dient gekeken te worden naar de UAVG en voor het VK naar de Data Protection Act 2018.

2.5 Zorgvuldige gegevensverwerking

Naast het hebben van een gerechtvaardigd doel en een grondslag, zijn in de AVG aanvullende beginselen opgenomen waaraan voldaan moet worden om van een zorgvuldige verwerking van persoonsgegevens te spreken; hierbij moet onder meer gedacht worden aan het vereiste van dataminimalisatie, juistheid van de gegevens, het treffen van beveiligingsmaatregelen en transparantie. Indien cross-sectoraal gegevens gedeeld worden moet dus, naast het hebben van een doel en grondslag, ook altijd worden voldaan aan de aanvullende beginselen om te spreken van een zorgvuldige gegevensverwerking.[9]

Dataminimalisatie en juistheid

Het is van belang dat niet meer gegevens worden verzameld en verwerkt dan noodzakelijk is voor het doel waarvoor deze worden verzameld (dataminimalisatie). De gegevens moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is om het doel te bereiken.

Opslagbeperking

Persoonsgegevens mogen niet langer mogen worden bewaard dan noodzakelijk is voor het doel waarvoor ze zijn verzameld of verder verwerkt. Nadat de bewaartermijn is verlopen dienen de gegevens te worden verwijderd of volledig geanonimiseerd.

Transparantie en informatieplicht

Op grond van de AVG, dienen betrokkenen geïnformeerd te worden over de hen betreffende gegevensverwerkingen; partijen dienen transparant te zijn over de verwerkingen die plaatsvinden. Hierbij is van belang dat de informatie en communicatie eenvoudig, toegankelijk en in begrijpelijke taal is. In de AVG is vastgelegd welke informatie verstrekt dient te worden aan betrokkenen.

Beveiligingsmaatregelen

Verwerkingsverantwoordelijken zijn verplicht om passende technische en organisatorische maatregelen te treffen om de persoonsgegevens die zij verwerken passend te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Bij het treffen van de maatregelen dient onder andere rekening gehouden te worden met de stand van de techniek, de aard en de context van de doeleinden en de waarschijnlijkheid en ernst van de risico's voor de rechten en vrijheden van de betrokkenen.

[9] Artikel 5 AVG (beginselen inzake verwerking van persoonsgegevens), artikelen 12 tot en met 23 AVG (rechten van betrokkenen).

Rechten van de betrokkenen
Betrokkenen hebben op grond van de AVG een aantal rechten die hen toekomen. De betrokkene heeft het recht op inzage in de gegevens die over hem of haar worden verwerkt. Daarnaast kan een betrokkene ook verzoeken om de hem of haar betreffende gegevens te verbeteren, aan te vullen of onder omstandigheden te verwijderen. De AVG kent daarnaast ook het recht op beperking van de verwerking, het recht op overdraagbaarheid en het recht op bezwaar.

2.5.1 Passende maatregelen en verantwoordingsplichten
Het is aan de verwerkingsverantwoordelijke om invulling te geven aan de bovenstaande beginselen voor een zorgvuldige verwerking van persoonsgegevens. Dit betekent dat de verwerkingsverantwoordelijke passende maatregelen van technische en organisatorische aard moet nemen om te garanderen dat de gegevens zorgvuldig worden verwerkt. De verwerkingsverantwoordelijke moet dit ook kunnen aantonen (verantwoordingsplicht). De AVG verplicht de verwerkingsverantwoordelijke (afhankelijk van de aard van de verwerking) om concrete beheersmaatregelen te nemen zoals het doen van gegevensbeschermingseffectbeoordelingen (ook wel DPIAs), het aanstellen van een Functionaris Gegevensbescherming (FG of DPO) en het bijhouden van een register van verwerkingen.[10]

2.6 Verantwoordelijkheidsverdeling
De hierboven beschreven verplichtingen uit de AVG zijn van toepassing op de 'verwerkingsverantwoordelijke'. De verwerkingsverantwoordelijke is degene die alleen of tezamen met anderen het *doel* en de *middelen* vaststelt voor de verwerking, met andere woorden de verwerkingsverantwoordelijke bepaalt waarom persoonsgegevens worden verzameld en hoe dat dan gebeurt.[11] Het is aan de verwerkingsverantwoordelijke om een rechtmatige grondslag voor het verwerken van de persoonsgegevens te hebben. Verder is het aan de verwerkingsverantwoordelijke om de gegevens zorgvuldig te verwerken zoals hierboven beschreven.

Zoals uit de definitie blijkt, ziet het begrip niet noodzakelijk op een enkele natuurlijke persoon of rechtspersoon, maar kan het betrekking hebben op meerdere deelnemers aan een verwerking. Wanneer twee of meer verantwoordelijken samen het doel en de middelen van een gegevensverwerking bepalen, zullen zij worden aangeduid als gezamenlijke verantwoordelijken (zie artikel 26 AVG). Dit is bijvoorbeeld het geval als twee of meer verantwoordelijken een gezamenlijke database opzetten waarin persoonsgegevens worden verwerkt en de verantwoordelijken gezamenlijk het doel van deze database bepalen. Bij cross-sectorale gegevensdeling kan ook sprake zijn van gezamenlijke verantwoordelijkheid tussen de private partijen die gegevens delen, afhankelijk van hoe de verwerkingen en de samenwerking concreet is ingericht. Indien de organisaties gezamenlijk het doel vaststellen voor de gegevensdeling en gezamenlijk bepalen op welke wijze, met welke middelen, de gegevensdeling wordt uitgevoerd, is er sprake van gezamenlijke verantwoordelijkheid. De verantwoordelijken worden dan niet voor al hun verwerkingen gezamenlijke verantwoordelijken, maar wel voor die verwerkingen waar ze gezamenlijk beslissingen over nemen, zoals ten aanzien van het doel, de middelen, de categorieën persoonsgegevens die worden gedeeld, de bewaartermijnen van de gegevens en ontvangers van de persoonsgegevens. Om te beoordelen of sprake is van gezamenlijke verantwoordelijkheid, dient goed gekeken te worden naar hoe de cross-sectorale gegevensdeling tussen de private partijen is ingericht.

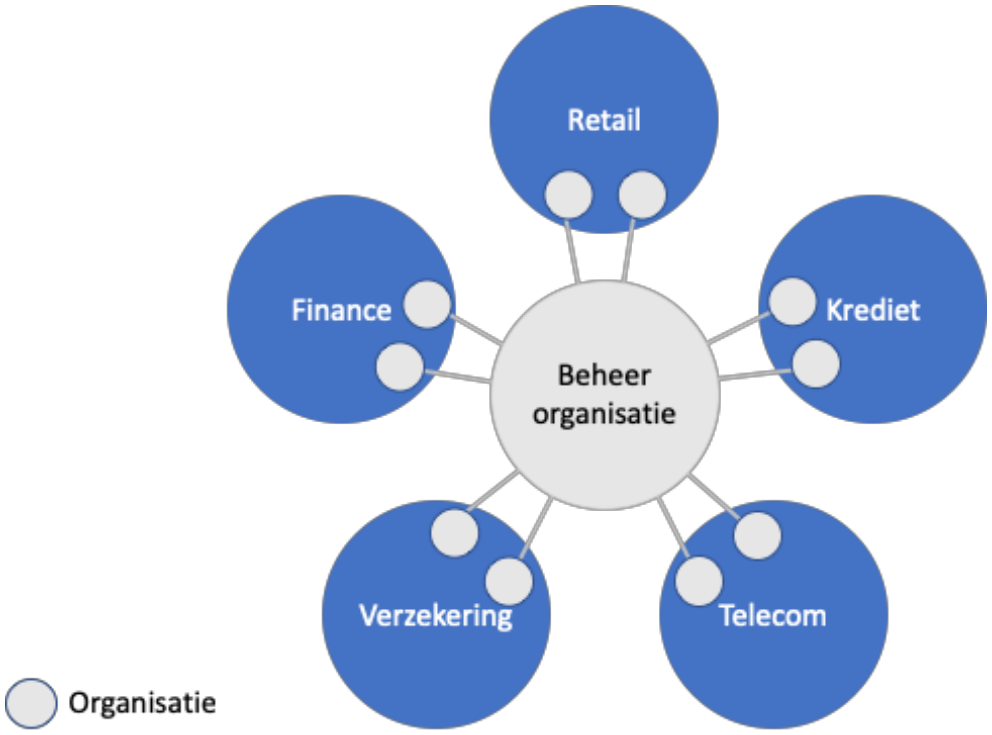
In het geval van gezamenlijke verantwoordelijken, moeten de betrokken partijen in navolging van artikel 26 AVG bepalen hoe zij de onderlinge verantwoordelijkheden en aansprakelijkheden verdelen en dienen ze de gemaakte afspraken op duidelijke en transparante wijze vast te leggen. Het moet voor betrokkenen namelijk

[10] Artikel 35 (gegevensbeschermingseffectbeoordelingen), artikel 37 (functionaris gegevensbescherming), artikel 30 (verwerkingsregister).
[11] Artikel 4 lid 7 AVG

duidelijk zijn bij wie ze hun rechten kunnen uitoefenen en van wie zij informatie ontvangen over de verwerking van hun persoonsgegevens.[12]

2.7 Verwerkerschap

De verwerkingsverantwoordelijke kan een derde partij inzetten om ten behoeve van hem persoonsgegevens te verwerken zonder dat deze partij aan diens rechtstreeks gezag is onderworpen, deze derde partij wordt dan een verwerker genoemd.[13] In het kader van cross-sectorale gegevensdeling tussen private partijen voor fraudebestrijding zou bijvoorbeeld gedacht kunnen worden aan een beheerorganisatie die de daadwerkelijke uitwisselingen faciliteert ten behoeve van de samenwerkende partijen (de verwerkingsverantwoordelijken).



Wanneer een dergelijke beheerorganisatie echter zelf doel en middelen voor de verwerking gaat bepalen, bijvoorbeeld door het vaststellen van toetredingscriteria, het bepalen welke gegevens worden uitgewisseld, of zelf het initiatief neemt tot de verwerkingen, dan moet de organisatie worden aangemerkt als een verwerkingsverantwoordelijke. Deze organisatie moet dan zelf een rechtmatige grondslag hebben voor het verzamelen en delen van persoonsgegevens.

2.8 Samenvatting

Wil een cross-sectorale gegevensdeling tussen private partijen ten behoeve van fraudebestrijding in lijn zijn met de AVG, dan moet er:

- Een duidelijk omschreven doel zijn voor de verwerking;
- Een rechtmatige grondslag op grond van artikel 6 AVG zijn; én
- Een uitzondering zijn op het verwerkingsverbod voor strafrechtelijke gegevens.

[12] Artikel 26 AVG
[13] Artikel 28 AVG

Het antwoord op de vraag of er een rechtmatige grondslag voor de verwerking en een uitzondering op het verwerkingsverbod is, hangt nauw samen met de vraag wie er als verwerkingsverantwoordelijke(n) worden aangemerkt: de individuele partijen voor de 1-op-1 uitwisselingen, een gezamenlijke verantwoordelijkheid voor alle uitwisselingen, of een beheerorganisatie voor het faciliteren van cross-sectorale gegevensdeling.

Indien aan de bovenstaande rechtmatigheidseisen is voldaan, dan moet de verwerking vervolgens voldoen aan de zorgvuldigheidsvereisten. In het volgende hoofdstuk wordt nader ingegaan op de Nederlandse situatie met betrekking tot de rechtmatige verwerking van persoonsgegevens voor cross-sectorale gegevensdeling tussen private partijen.

3 Cross-sectorale gegevensdeling ten behoeve van fraudebestrijding in het Nederlandse rechtsbestel

3.1 Rechtmatigheid gegevensdeling tussen private partijen

Zoals in hoofdstuk 1 aangegeven dient in kaart te worden gebracht welke juridische vereisten in Nederland gelden ten aanzien van cross-sectorale gegevensdeling tussen private partijen op het gebied van fraudebestrijding. In het voorgaande hoofdstuk is het kader van de AVG uiteengezet. In dit hoofdstuk wordt dit kader toegepast op de Nederlandse situatie en uiteengezet of cross-sectoraal gegevens gedeeld mogen worden tussen private partijen in het Nederlandse rechtsbestel. Voordat in wordt gegaan op de juridische analyse, wordt eerst kort uiteengezet wat in dit hoofdstuk wordt verstaan onder de term fraude.

3.1.1 Het begrip 'fraude'

Fraude is een wijdverbreid fenomeen waar velerlei verschijningsvormen onder geschaard kunnen worden. Ondanks dat fraude een veelvoorkomend begrip is, heeft het in zowel het Nederlandse strafrecht als het maatschappelijk verkeer geen vastomlijnde betekenis. Het Nederlandse Wetboek van Strafrecht (WvSr) kent geen bepaling waarin specifiek het plegen van fraude strafbaar is gesteld. Wel zijn in het WvSr meerdere bepalingen opgenomen die zich richten op het gedrag dat als fraude kan worden omschreven.[14]

Fraude is een vorm van bedrog waarbij bepaalde zaken anders voor worden gedaan 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 valse voorwendselen met het oogmerk om zich op basis van deze bedrieglijke gegevens ten koste van anderen te bevoordelen dan wel te verrijken.

Er is sprake van fraude wanneer:

- Opzettelijk is gehandeld;
- Een misleidende voorstelling van zaken is gegeven;
- Met het oogmerk economisch voordeel te behalen;
- Er een benadeelde is; en
- Sprake is van onrechtmatig of onwettig handelen.

Als aan deze elementen wordt voldaan is sprake van fraude. In dit hoofdstuk wordt fraude beperkt tot horizontale fraude waarbij het gaat om fraude die gericht is tegen burgers en bedrijven. Bij horizontale fraude moet bijvoorbeeld gedacht worden aan hypotheekfraude, fraude met betaalproducten (skimmimg, phishing, creditcard), verzekeringsfraude of assurantiefraude, telecomfraude, faillissementsfraude, acquisitiefraude, internet gerelateerde fraude (waaronder online handelsfraude), voorschotfraude, beleggingsfraude en identiteitsfraude.[15]

3.1.2 Doel

Zoals in hoofdstuk 2, juridisch kader, is aangegeven mogen persoonsgegevens op grond van de AVG slechts verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. Het doel of de

[14] F.G.H. Kristen, R.M.I. Lamp, J.M.W. Lindeman en M.J.J.P. Luchtman, *Bijzonder strafrecht:* Strafrechtelijke handhaving van sociaal-economisch en fiscaal recht in Nederland, Den Haag: Boom Juridische uitgevers 2011, blz. 41.
[15] F. Boerman, M. Grapendaal, F. Nieuwenhuis, E. Stoffers, *Nationaal dreigingsbeeld 2017 Georganiseerde criminaliteit,* Zoetermeer: 2017, p. 129-161.

doelen waarvoor de gegevens worden verwerkt moeten uitdrukkelijk omschreven zijn. Dit betekent dat, voordat gestart wordt met de verwerking van de gegevens, moet zijn vastgelegd waarvoor de persoonsgegevens nodig zijn.

Indien cross-sectoraal gegevens gedeeld gaan worden tussen private partijen ten behoeve van het bestrijden van fraude of mogelijk een fraudepreventiesysteem ingericht gaat worden, dient voorafgaand dan ook goed bepaald en vastgelegd te worden wat het precieze doel is van de gegevensdeling. Zodra private partijen gegevens gaan delen om fraude te bestrijden, is het voor de hand liggend dat de doelstelling voornamelijk ziet op het bestrijden van fraude teneinde de schade die private partijen oplopen door fraude te verminderen. De gegevensdeling kan echter ook een aanvullend publiek belang dienen als de gegevens (pro-actief) gedeeld gaan worden met opsporingsinstanties. Het is dan ook belangrijk dat de organisaties die mogelijk gegevens willen gaan delen voorafgaand goed vastleggen voor welke doelen de gegevens gedeeld kunnen worden.

Bij het verzamelen en uitwisselen van gegevens tussen meerdere private partijen bestaat het risico dat de verzamelde en uitgewisselde gegevens voor andere doelen worden gebruikt dan oorspronkelijk bedoeld. Dit heet ook wel function of mission creep. Het is daarom van belang dat er bij het verstrekken van persoonsgegevens op wordt gelet dat de persoonsgegevens alleen worden verwerkt voor het doel waarvoor ze in beginsel zijn verstrekt, in dit geval dus het bestrijden van fraude. Alle private partijen die betrokken zijn bij de cross-sectorale gegevensdeling, dan wel gegevens ontvangen vanuit de cross-sectorale gegevensdeling zullen te allen tijde het doeleinde waarvoor de persoonsgegevens verzameld zijn in de gaten moeten blijven houden. Er zullen maatregelen getroffen moeten worden om te zorgen dat de persoonsgegevens niet voor een ander doeleinde worden gebruikt.

3.1.3 Grondslag art. 6 AVG

Om het doel gerechtvaardigd te maken, dient het gebaseerd te kunnen worden op één van de grondslagen genoemd in artikel 6 AVG. Voor meer informatie over de betekenis van de grondslagen, wordt verwezen naar het juridisch kader. Persoonsgegevens mogen worden verwerkt indien:

a) de ondubbelzinnige toestemming van de betrokkene is verkregen;
b) dit noodzakelijk is voor de uitvoering van een overeenkomst;
c) dit noodzakelijk is voor het voldoen aan een wettelijke verplichting;
d) dit noodzakelijk is ter vrijwaring van de vitale belangen van de betrokkene;
e) dit noodzakelijk is voor de uitvoering van een taak in algemeen belang of voor het uitoefenen van het openbaar gezag;
f) dit noodzakelijk is voor de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, die niet worden overstemd door de belangen, rechten en vrijheden van de betrokkene.

Hieronder wordt nader gekeken naar de toepasbaarheid van de grondslagen indien cross-sectoraal gegevens gedeeld gaan worden tussen private partijen ten behoeve van het bestrijden van fraude.

Om van een rechtsgeldige **toestemming** te kunnen spreken, geldt dat sprake moet zijn van een vrije, specifieke en geïnformeerde toestemming. Indien cross-sectoraal gegevens gedeeld gaan worden tussen private partijen over potentiële fraudeurs, kan dit niet gebeuren op basis van toestemming van de betrokkene. Gezien de doelstellingen van de gegevensdeling en het feit dat organisaties elkaar door middel van de gegevensdeling willen waarschuwen voor potentiële fraudeurs, zal de betrokkene zich niet snel 'vrij' voelen om toestemming te weigeren. Het is aannemelijk dat aan het weigeren van toestemming negatieve consequenties verbonden kunnen zijn voor de betrokkene. Indien beargumenteerd wordt dat wel sprake is van een 'vrije' toestemming, biedt deze grondslag geen uitkomst om een dergelijke gegevensdeling effectief in te richten: een betrokkene verleent immers niet snel toestemming om onderdeel te worden van een dergelijke gegevensdeling.

De grondslag **uitvoering van een overeenkomst** biedt in dit geval ook geen uitkomst nu de betrokkene, van wie de gegevens worden verwerkt, geen partij zal zijn bij de overeenkomst die ziet op de gegevensdeling.

Om gegevens te mogen verwerken op basis van de grondslag **wettelijke verplichting,** dient deze verplichting bij wet te zijn vastgelegd en dient de verantwoordelijke te zijn onderworpen aan deze verplichting. Nu op het moment nog niet duidelijk is welke private partijen mogelijk cross-sectoraal gegevens willen gaan delen, kan nog niet beoordeeld worden of in specifieke materiewetgeving bepalingen zijn opgenomen die deze gegevensdeling rechtvaardigen. Er kan dan ook geen beroep op deze grondslag worden gedaan. Voor volledigheid is wel gekeken naar de Wet op het financieel toezicht en de Telecommunicatiewet[16]. In deze wetten zijn geen wettelijke verplichtingen opgenomen die organisaties in de financiële sector of in de telecomsector ertoe verplichten cross-sectoraal gegevens te gaan delen ten behoeve van het bestrijden van fraude.

Een gerechtvaardigd beroep op de grondslag **vitaal belang** kan uitsluitend worden gedaan wanneer sprake is van een acute situatie waarbij dringend noodzakelijke medische hulp aan de betrokkene moet worden verleend. Bij het cross-sectoraal delen van gegevens ten behoeve van het bestrijden van fraude, is daar geen sprake van. Er kan dan ook geen beroep op deze grondslag worden gedaan.

Ook voor een gerechtvaardigd beroep op de grondslag **taak van algemeen belang dan wel voor een taak in het kader van de uitoefening van het openbaar gezag** geldt dat de taak bij wet moet zijn vastgelegd. Deze taak dient in de wet ook specifiek aan de verwerkingsverantwoordelijke te zijn opgedragen; dit kunnen ook private partijen betreffen. Net als bij de wettelijke verplichting kan niet gezegd worden dat persoonsgegevens op basis van deze grondslag verwerkt mogen worden nu nog niet duidelijk is welke organisaties mogelijk deel gaan nemen aan de gegevensdeling. Voor de volledigheid is ook in dit geval gekeken naar de Wet op het financieel toezicht en de Telecommunicatiewet. Deze wetten bevatten geen dergelijke taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag op basis waarvan organisaties in de financiële sector of de telecomsector cross-sectoraal persoonsgegevens mogen verwerken ten behoeve van het bestrijden van fraude.

De enige mogelijke grondslag op basis waarvan de private partijen in het kader van fraudebestrijding cross-sectoraal gegevens kunnen delen, is het **gerechtvaardigd belang** van de organisatie als bedoeld in artikel 6 lid 1 sub f AVG.[17]

Voor een geslaagd beroep op de grondslag 'behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijk of een derde', dient aan drie vereisten te worden voldaan:

I. Aanwezigheid van een gerechtvaardigd belang;
II. De noodzakelijkheidseis, waaronder proportionaliteit en subsidiariteit; en
III. Het belang van de verantwoordelijke moet prevaleren boven het belang van de (potentiële) fraudeurs.

Indien private partijen cross-sectoraal gegevens willen gaan delen ten behoeve van het bestrijden van fraude, dienen zij goed na te gaan of voldaan kan worden aan de toets voor een geslaagd beroep op de grondslag gerechtvaardigd belang. Hieronder wordt een nadere toelichting op de vereisten gegeven.

[16] In de Telecommunicatiewet is wel een wettelijke bepaling opgenomen waaruit blijkt dat aanbieders gegevens verder mogen verwerken zonder toestemming van de betrokkene wanneer deze worden verwerkt om fraude op te sporen. Dee verplichting strekt echter niet zover dat daaronder ook gegevens cross-sectoraal gedeeld mogen worden teneinde fraude op te sporen in een samenwerkingsverband.

[17] Graag wordt opgemerkt dat indien het voornemen bestaat om te zijner tijd ook publieke organisaties te laten deelnemen aan het gegevensdelingssysteem, dit niet mogelijk is op basis van het gerechtvaardigd belang. Overheidsorganisaties kunnen geen beroep doen op deze grondslag wanneer zij gegevens verwerken ter uitvoering van hun taken. Indien publieke organisaties gaan deelnemen, dient dan ook nader onderzocht te worden op welke juridische basis het mogelijk is deel te nemen aan de het gegevensdelingssysteem.

I. Gerechtvaardigd belang

Om van een gerechtvaardigd belang te kunnen spreken, moet het belang rechtmatig zijn, duidelijk verwoord en daadwerkelijk aanwezig zijn; het mag geen speculatief belang betreffen. Bij een gerechtvaardigd belang moet gedacht worden aan een verwerking die noodzakelijk is om reguliere bedrijfsactiviteiten te verrichten of die de bedrijfsvoering in wezenlijke zin ondersteunt. De verwerking van persoonsgegevens die strikt noodzakelijk is voor fraudevoorkoming is ook een gerechtvaardigd belang als bedoeld in artikel 6 lid 1 sub f AVG.[18] In beginsel ziet het legitieme belang van de organisatie erop om de organisatie zelf te beschermen tegen de gevolgen die fraude met zich meebrengen ten aanzien van de bedrijfsactiviteiten.

In sommige gevallen kan een gerechtvaardigd belang van een organisatie echter ook samenvallen met een publiek belang. Dit kan bijvoorbeeld zijn wanneer organisaties gegevens gaan delen ten behoeve van het bestrijden van fraude. De organisatie kan dan een legitiem zakelijk belang hebben om ervoor te zorgen dat klanten geen misbruik maken van zijn diensten en de organisatie verlies leidt, terwijl anderzijds klanten van de organisatie, belastingbetalers en het grote publiek ook een legitiem belang hebben bij deze gegevensdeling doordat frauduleuze activiteiten worden ontmoedigd en fraude wordt opgespoord.

In dergelijke gevallen kan het feit dat de organisatie niet alleen handelt ten behoeve van zijn eigen legitieme bedrijfsbelang, maar ook ten behoeve van het algemeen belang, meer gewicht geven aan dat belang. Hoe groter het algemeen belang is dat gediend wordt en als ook van de organisatie verwacht mag worden dat zij een rol spelen bij het nastreven van dit algemene belang, hoe zwaarder dit mee kan wegen in de belangenafweging die gemaakt dient te worden.[19]

Bij de belangenafweging (zie III) mag dus meegenomen worden dat het legitiem belang dat de organisatie heeft met het bestrijden van fraude ook een algemeen belang dient. Het mag echter niet zover gaan dat praktijken die niet door overheidsorganisaties mogen worden uitgevoerd omdat zij in strijd zijn met het recht op privacy, via deze weg alsnog door private partijen uitgevoerd kunnen worden.[20]

II. Noodzakelijkheidseis

De gegevensverwerking moet ook noodzakelijk (waaronder proportionaliteit en subsidiariteit) zijn voor het doel dat daarmee wordt beoogd. Hierbij moet worden beoordeeld of het doel van de verwerking in redelijke verhouding staat tot de inbreuk op de persoonlijke levenssfeer van betrokkenen en of het belang anderszins of met minder ingrijpende middelen kan worden gediend. Indien het belang met andere of minder ingrijpende middelen kan worden gediend, is de verwerking niet toegestaan.[21] Indien private partijen cross-sectoraal gegevens gaan delen dient dan ook goed onderbouwd worden waarom voor de organisaties de noodzaak bestaat om cross-sectoraal gegevens te delen ten behoeve van het bestrijden van fraude; waar bestaat de toegevoegde waarde van deze manier van gegevens delen uit ten opzichte van het delen van gegevens in een bepaalde branche, zoals al wordt gedaan in het Incidentenwaarschuwingssysteem financiële instellingen.[22] Goed onderbouwd dient te worden wat de effectiviteit is van cross-sectorale gegevensdeling en of het niet mogelijk is deze resultaten te bereiken op een alternatieve, minder ingrijpende manier.

---

[18] Artikel 6 lid 1 sub f AVG, overweging 47.

[19] Working Party 29 WP/217, Opinion 06/2-14 on the notion of legitimate interests of the data controller, 09-04-2014, p. 35.

[20] Deze onderbouwing staat los van de vraag of een dergelijke taak bij private partijen belegd kan worden. Dit is een politieke en maatschappelijke keuze die gemaakt dient te worden.

[21] Ministerie van Justitie en Veiligheid, Handleiding Algemene Verordening Gegevensbescherming en Uitvoeringswet Algemene Verordening Gegevensbescherming, p. 39 – 40.

[22] Financiële instellingen (verzekeraars, hypothecaire instellingen, financieringsondernemingen en banken) delen gegevens met elkaar middels het incidentenwaarschuwingssysteem (zwarte lijst) teneinde fraude en criminaliteit tegen te gaan. Deze zwarte lijst is goedgekeurd door de AP. https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/register-zwarte-lijsten/zwarte-lijst-financiele-instellingen

III. Belangenafweging

Daarnaast dient ook een afweging plaats te vinden waarbij de belangen van de betrokkenen afgewogen worden tegenover het belang dat de organisaties hebben met het bestrijden van fraude. Bij het uitvoeren van de belangenafweging dient goed gekeken te worden naar de impact die de verwerking heeft op de rechten en vrijheden van betrokkenen. Elementen die van belang zijn bij deze afweging zijn onder meer de gevoeligheid van de gegevens die verwerkt worden, de manier waarop de gegevens verwerkt worden en of de verwerking voorzienbaar is voor betrokkenen: mogen betrokkenen verwachten dat hun gegevens op deze wijze en voor dit doel verwerkt worden. Het is daarnaast belangrijk de mogelijke gevolgen van de verwerking mee te nemen in de belangenafweging; kan de verwerking leiden tot uitsluiting van een betrokkene of tot stigmatisering. Naast de impact op de betrokkenen, dient meegenomen te worden welke waarborgen getroffen worden om de rechten en vrijheden van betrokkenen te beschermen. Hoe groter de impact, hoe meer waarborgen getroffen dienen te worden.[23]

Uit beslissingen van de Autoriteit Persoonsgegevens ten aanzien van goedgekeurde zwarte lijsten, kan worden afgeleid dat het onder meer belangrijk is om bij de inrichting van (cross-sectorale) gegevensdeling goed te kijken naar de wijze waarop de bewijslast wordt ingeregeld. Aan welke voorwaarden dient te zijn voldaan, voordat een organisatie een fraudezaak met daarbij de persoonsgegevens van de fraudeur mag inbrengen in de gegevensdeling. Bij het bepalen hiervan, moet de impact goed voor ogen worden gehouden. De impact van deze sector-overstijgende deling zal groter zijn dan wanneer de deling plaatsvindt tussen enkele private partijen of binnen een bepaalde branche.

Een ander belangrijk punt is het proces van raadpleging. Welke personen krijgen toegang tot de gegevens en op welke wijze kunnen de gegevens geraadpleegd worden. Om de inbreuk op de persoonlijke levenssfeer te beperken, kan bijvoorbeeld overwogen worden de toegang zodanig in te richten dat uitsluitend enkele medewerkers van een deelnemende organisatie, die belast zijn met geheimhouding, de gegevens mogen raadplegen of dat het raadplegen uitsluitend is voorbehouden aan een specifiek team binnen een organisatie, zoals bij het Incidentenwaarschuwingssysteem financiële instellingen is gedaan.[24] Naast het toegangsvereiste, dient ook goed bekeken te worden op welke wijze de gegevens geraadpleegd kunnen worden; op welke wijze mogen de deelnemende organisaties inzage verkrijgen in gegevens. Om de inbreuk zo veel mogelijk te beperken, kan gedacht worden aan een hit/no-hit systeem waarbij de deelnemende organisaties enkel respons krijgen dat persoonsgegevens die zij willen verifiëren overeenkomen met gegevens die al bij een andere organisatie bekend zijn en zij op basis daarvan nader onderzoek moeten doen in plaats van dat zij inzage krijgen in de inhoud van de zaak. Voor meer informatie over waarborgen die getroffen dienen te worden wordt verwezen naar 2.5 en 3.1.6.

Het is ook belangrijk om voorafgaand goed de scope te bepalen van de gegevensdeling. Dit betreft zowel de omvang van de partijen die kunnen deelnemen, maar ook de scope van de zaken die kunnen worden ingediend. Op dit moment wordt gesproken van mogelijke cross-sectorale gegevensdeling tussen private partijen, maar is niet helder welke branches kunnen deelnemen aan de gegevensdeling. Om de impact op de betrokkene goed te duiden moet helder zijn wie deelneemt, wat gedeeld wordt, hoe lang gegevens beschikbaar blijven, onder welke omstandigheden gedeeld wordt en welke consequenties daaraan verbonden worden. Een klein vergrijp moet bijvoorbeeld niet de toekomst van betrokkenen ruïneren omdat zij (voor altijd) te boek staan als fraudeur in al hun toekomstige interacties met publieke en private instanties. Gezien de impact die cross-sectorale gegevensdeling met zich mee kan brengen op de rechten en vrijheden van betrokkenen, is het van belang dat over bovenstaande punten goed wordt nagedacht.

---

[23] Working Party 29 WP/217, Opinion 06/2-14 on the notion of legitimate interests of the data controller, 09-04-2014, p. 33 – 43.

[24] Zie 3.2 en 4.2 Protocol Incidentenwaarschuwingssysteem financiële instellingen. https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/zw_lijsten_protocollen/zwarte-lijst-fi-2013-protocol.pdf. Op het moment wordt door de aangesloten organisaties gewerkt aan een nieuw protocol. Totdat een nieuw protocol door de AP is goedgekeurd is dit protocol uit 2013 van toepassing.

3.1.4 Strafrechtelijke persoonsgegevens

Zoals uitgelegd onder 2.4 worden bij het cross-sectoraal delen van gegevens tussen private partijen ten behoeve van het bestrijden van fraude strafrechtelijke gegevens verwerkt. Persoonsgegevens van strafrechtelijke aard mogen slechts worden verwerkt als hier een uitzondering voor voorzien is in artikel 32 – 33 van de UAVG, in navolging van artikel 10 AVG. In artikel 32 zijn de algemene uitzonderingsgronden opgenomen en in artikel 33 de specifieke uitzonderingsgronden.

De enige mogelijke uitzonderingsgrond in de AVG, UAVG waaronder de private partijen in het kader van cross-sectorale gegevensdeling strafrechtelijke gegevens kunnen verwerken, kan thans gevonden worden in artikel 10 AVG jo. art. 33 lid 4 sub c en lid 5 UAVG.

Op basis van art. 33 lid 4 sub c UAVG mogen persoonsgegevens van strafrechtelijke aard ten behoeve van derden worden verwerkt indien de Autoriteit Persoonsgegevens met inachtneming van het vijfde lid een vergunning voor de verwerking heeft verleend. In artikel 33 lid 5 is vervolgens vastgelegd dat een vergunning als bedoeld in lid 4 sub c slechts kan worden verleend, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Aan de vergunning kunnen voorschriften worden verbonden. De vergunning dient aangevraagd te worden door de verwerkingsverantwoordelijke(n); dit betekent dat de private partijen, die voornemens zijn cross-sectoraal gegevens te gaan delen, daartoe gezamenlijk een vergunning dienen aan te vragen. Op welke wijze een vergunning aangevraagd dient te worden en uit welke stappen het vergunningstraject bestaat, is nader uitgewerkt in bijlage I. Voor meer informatie wordt verwezen naar bijlage I.

3.1.5 Vergunningstraject

Zoals uit het voorgaande blijkt, dient een vergunning aangevraagd te worden willen private partijen cross-sectoraal gegevens gaan delen ten behoeve van fraudebestrijding. Deze vergunning dient door de verwerkingsverantwoordelijken aangevraagd te worden. Dit betekent in dit geval dat de private partijen, die van plan zijn te starten met de gegevensdeling gezamenlijk een vergunning bij de Autoriteit Persoonsgegevens moeten aanvragen.[25]

Inschakelen beheerder

Het kan zijn dat de private partijen de gegevensdeling graag wensen in te richten in samenwerking met een externe organisatie, die optreedt als beheerder. Deze externe organisatie ('beheerder') deelt zelf geen persoonsgegevens met organisaties teneinde fraude te bestrijden, maar faciliteert de gegevensdeling. De rol van beheerder kan verschillend worden ingericht. Hieronder wordt daar kort op ingegaan.

Beheerder als verwerker

Indien de beheerder in opdracht van en onder instructies van de andere organisaties de gegevensdeling voor hen verricht, treedt de beheerder op als verwerker. Een verwerker is een derde die ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder dat deze derde onder rechtstreeks gezag staat van de verwerkingsverantwoordelijke.[26] De beheerder heeft als verwerker geen zeggenschap over de gegevensverwerkingen die plaatsvinden. De verwerker mag alleen handelen onder de verantwoordelijkheid en naar instructies van de organisaties. Dat betekent dat de organisaties vaststellen voor welk doel de gegevens worden verwerkt en op welke wijze, met welke middelen, deze verwerkingen worden uitgevoerd. De beheerder voert enkel de verwerking uit die door de organisaties is uitbesteedt. Ingeval voor een dergelijke

[25] Artikel 33 lid 4 sub c en lid 5 UAVG, Memorie van Toelichting artikel 33 UAVG.

[26] Artikel 28 AVG.

constructie wordt gekozen, dient in de vergunningaanvraag duidelijk te worden aangegeven dat gebruik gemaakt gaat worden van een verwerker en dient aangegeven te worden hoe dit wordt ingericht.

Beheerder als gezamenlijk verantwoordelijke
Indien de beheerder ook zelfstandig beslissingen gaat nemen over de doelen van de verwerking en de middelen waarmee de gegevensdeling wordt uitgevoerd, dan kan de beheerder niet enkel gezien worden als verwerker en bestaat ook verantwoordelijkheid voor de beheerder ten aanzien van de gegevensverwerkingen. Zoals in het juridisch kader uiteengezet, kan bij cross-sectorale gegevensdeling vaak gesproken worden van gezamenlijke verantwoordelijkheid omdat de organisaties gezamenlijk het doel van de samenwerking vaststellen en ook gezamenlijk bepalen op welke wijze de gegevensdeling wordt uitgevoerd. Indien de beheerder ook beslissingen neemt ten aanzien van het doel en de middelen van de gegevensdeling kan gezegd worden dat de beheerder ook verwerkingsverantwoordelijke is en met de andere organisaties gezamenlijk verantwoordelijk is voor de verwerking. Indien gekozen wordt voor deze constructie, dient de beheerder goed te kunnen onderbouwen dat zij een grondslag hebben, in dit geval het gerechtvaardigd belang, om als beheerder gegevens van de organisaties te verwerken ten behoeve van het bestrijden van fraude. Indien de beheerder optreedt als gezamenlijk verantwoordelijke, dient de beheerder ook onderdeel te zijn van het vergunningstraject en samen met de organisaties de vergunningaanvraag te doen.

Een vergunning dient aangevraagd te worden door de verwerkingsverantwoordelijke(n). Indien een beherende partij zelfstandig de vergunningsaanvraag zou doen, moet de beheerder kunnen aantonen dat een grondslag bestaat, in dit geval het gerechtvaardigd belang, om een dergelijke gegevensdeling in te richten en te faciliteren voor de private partijen. Hoewel het niet op voorhand is uitgesloten dat een dergelijke aanvraag succesvol is, is naar het oordeel van de onderzoekers, gegeven de mogelijke impact op de rechten en vrijheden van de betrokkene, het gerechtvaardigd belang van de beherende partij snel ondergeschikt. Het belang van de beherende partij bestaat namelijk niet uit het voor zichzelf voorkomen van fraude, maar het (commercieel) faciliteren van een samenwerking gericht op fraudebestrijding. Zonder de betrokkenheid van verwerkingsverantwoordelijken die daadwerkelijk potentieel slachtoffer zijn van fraudebestrijding is het voor een beherende partij moeilijk om de noodzakelijkheid van de verwerking aan te tonen.

Concluderend
De AVG en UAVG bieden juridische mogelijkheden om cross-sectoraal gegevens te delen tussen private partijen ten behoeve van het bestrijden van fraude. De juridische mogelijkheden vereisen wel dat een vergunning wordt aangevraagd bij de Autoriteit Persoonsgegevens voor de gegevensdeling. Deze vergunning dient aangevraagd te worden door de private partijen die gegevens willen gaan delen. Zoals hierboven aangegeven bestaat er dus een juridische mogelijkheid, maar het is niet gezegd dat cross-sectorale gegevensdeling tussen private partijen ook daadwerkelijk kan plaatsvinden. Daartoe dient eerst het vergunningstraject in te worden gegaan. Zie voor meer informatie over het vergunningstraject, bijlage I – Aanvraag vergunning UAVG.

3.1.6 Zorgvuldige gegevensverwerking
Zoals blijkt uit het juridisch kader dient bij het verwerken van persoonsgegevens, naast het hebben van een gerechtvaardigd doel en een grondslag, ook altijd te worden voldaan aan de aanvullende beginselen die in de AVG zijn opgenomen; hierbij moet onder meer gedacht worden aan het vereiste van dataminimalisatie, juistheid van de gegevens, het treffen van beveiligingsmaatregelen en transparantie.

Indien cross-sectoraal gegevens gedeeld gaan worden tussen private partijen, is het van belang dat voorafgaand goed wordt nagedacht over de waarborgen die getroffen worden om de inbreuk op de persoonlijke levenssfeer zo beperkt mogelijk te houden. Aan de gegevensdeling in publiekrechtelijke samenwerkingsverbanden ligt veelal een wettelijke regeling ten grondslag waarin de waarborgen al zijn verankerd. In het wetgevingstraject is voorafgaand al goed nagedacht onder welke voorwaarden de

bevoegdheden mogen worden ingezet, welke waarborgen daarbij getroffen worden en dit wordt voorts ook geborgd in de wetgeving zelf. Aan een privaatrechtelijk samenwerkingsverband ligt geen wetgeving ten grondslag waardoor mogelijk meer vragen bestaan of wel voldoende waarborgen worden getroffen en of deze voorts in de praktijk ook goed geborgd worden. Indien cross-sectoraal gegevens gedeeld gaan worden, is het dan ook van belang goed te bekijken onder welke voorwaarden deze deling kan worden ingericht. Hieronder wordt nader ingegaan op algemene aandachtspunten die voornamelijk van belang zijn bij het cross-sectoraal delen van gegevens ten behoeve van het bestrijden van fraude.

Dataminimalisatie en juistheid
Indien cross-sectoraal gegevens gedeeld gaan worden, dient het vereiste van dataminimalisatie goed in acht genomen te worden. Uitsluitend die gegevens die nodig zijn om het doel, het bestrijden van fraude, te bereiken mogen gedeeld worden met elkaar. Het is dan ook van belang om voorafgaand aan de verstrekking, dan wel bij de inrichting van een mogelijk systeem goed te beoordelen van welke gegevens het noodzakelijk is deze te delen. Hierbij dient het vereiste van 'need to know' gehanteerd te worden in plaats van 'nice to have'. De organisaties dienen er daarnaast zorg voor te dragen dat de gegevens die gedeeld worden actueel en correct zijn. Gegevens die dat niet (meer) zijn, dienen te worden gewist of gecorrigeerd.[27]

Bewaartermijn
Voorafgaand aan de inrichting van de gegevensdeling moet door de organisaties goed worden nagedacht hoe lang het nodig is de gegevens te bewaren teneinde het doel van de verwerking te bereiken. Gelet op de mogelijke impact die het cross-sectoraal delen van gegevens voor een betrokkene met zich mee kan brengen, dient goed overwogen te worden hoe lang de gegevens onderdeel mogen zijn van deze deling en hoe lang het gerechtvaardigd is gegevens betreffende een bepaalde fraudezaak te bewaren.[28]

Transparantie, informatieplicht en rechten van betrokkenen
Indien cross-sectoraal gegevens gedeeld gaan worden tussen private partijen, is het van belang dat de betrokkenen voorafgaand aan de gegevensdeling goed geïnformeerd worden over de gegevens die over hen verwerkt worden. De betrokkenen moeten goed op de hoogte zijn van hetgeen plaatsvindt met hun gegevens. In de AVG staat opgenomen welke informatie de betrokkenen dienen te ontvangen. Het is daarnaast van belang dat een procedure ingericht wordt op welke wijze de betrokkenen uitvoering kunnen geven aan de rechten die hen toekomen op grond van de AVG. De betrokkenen moeten goed in staat worden gesteld inzage te verkrijgen in de gegevens die over hen worden verwerkt, maar moeten ook een verzoek tot rectificatie en/of verwijdering kunnen indienen. Zie 2.5 juridisch kader.[29]

Beveiligingsmaatregelen
Ook dient voorafgaand aan de inrichting van de gegevensdeling goed gekeken te worden naar de beveiligingsmaatregelen die getroffen moeten worden om de gegevens passend te beveiligen. Indien cross-sectoraal gegevens worden gedeeld tussen private partijen, worden daarbij strafrechtelijke gegevens tussen organisaties uitgewisseld. Gezien de gevoelige aard van deze gegevens, is het van belang dat goed wordt nagedacht op welke wijze deze gegevens beveiligd gaan worden.[30]

3.1.7 Passende maatregelen en verantwoordingsplichten
Zoals blijkt uit 2.5.1 is het aan de verwerkingsverantwoordelijken, in dit geval de private partijen, om invulling te geven aan de bovenstaande beginselen. De organisaties dienen passende maatregelen te treffen om ervoor te zorgen dat de gegevens zorgvuldig worden verwerkt. De organisaties moeten dit ook kunnen aantonen

[27] Artikel 5 lid 1 sub c en d AVG
[28] Artikel 5 lid 1 sub e AVG
[29] Artikel 12 – 22 AVG
[30] Artikel 5 lid 1 sub f AVG

(verantwoordingsplicht). De AVG verplicht om concrete beheersmaatregelen te nemen, zoals onder meer het doen van gegevensbeschermingseffectbeoordelingen ook wel *Data Protection Impact Assessment* genoemd (verder: 'DPIA') in artikel 35 AVG. Een DPIA dient te worden uitgevoerd bij verwerkingen die waarschijnlijk een groot risico meebrengen voor de rechten en vrijheden van betrokkenen. Hiervan is onder meer sprake wanneer het voornemen bestaat om op grote schaal strafrechtelijke gegevens te verwerken. Ook wanneer het voornemen bestaat om een zwarte lijst bij te houden en te delen, dient een DPIA te worden uitgevoerd. Voordat de private partijen een vergunningsaanvraag kunnen doen bij de Autoriteit Persoonsgegevens, dienen zij gezamenlijk een DPIA uit te voeren teneinde de risico's voor de betrokkenen in kaart te brengen. Hieronder wordt kort ingegaan op wat een DPIA inhoudt.

DPIA
Een DPIA is een instrument om van voorgenomen regelgeving of bij projecten waarbij persoonsgegevens worden verwerkt, de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. Op basis hiervan worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of te verkleinen. Een DPIA dient een systematische beschrijving te bevatten van de voorgenomen gegevensverwerking, waarbij ook ingegaan moet worden op de noodzaak en de evenredigheid van de gegevensverwerking. Ook dienen eventuele privacyrisico's voor de betrokkenen in kaart te worden gebracht en de maatregelen die worden genomen om die risico's te beperken.

3.2 Deelname publieke partijen

Hierboven is het juridisch kader in kaart gebracht ten aanzien van cross-sectorale gegevensdeling tussen private partijen. In deze paragraaf wordt kort ingegaan op de juridische grondslag wanneer ook publieke partijen deelnemen aan de cross-sectorale gegevensdeling.

Zoals in 2.3, het juridisch kader, uiteen is gezet kunnen overheidsinstanties geen beroep doen op de grondslag gerechtvaardigd belang wanneer zij gegevens verwerken ter uitvoering van hun taken. Indien publieke partijen ook cross-sectoraal gegevens willen gaan delen, kan dit dan ook niet op grond van het gerechtvaardigd belang. Er dient dan ook beoordeeld te worden of publieke partijen op basis van een andere grondslag in art. 6 AVG cross-sectoraal gegevens kunnen delen ten behoeve van het bestrijden van fraude. Een grondslag waar publieke partijen in dit kader naar waarschijnlijkheid een beroep op kunnen doen is de taak van algemeen belang of openbaar gezag, artikel 6 lid 1 sub e AVG. Om een gerechtvaardigd beroep te kunnen doen op deze grondslag, dient deze taak bij wet aan de betreffende partij te zijn toebedeeld. Dat betekent dat de publieke partij uitsluitend gegevens kan delen wanneer bij wet een taak aan de publieke partij is toebedeeld op basis waarvan de deling gebaseerd kan worden. Nu thans nog niet bekend is of en zo ja welke publieke partijen mogelijk deel willen gaan nemen aan een eventuele cross-sectorale gevensdeling, kan niet gezegd worden of een dergelijke taak van algemeen belang of openbaar gezag bestaat. Per partij dient beoordeeld te worden of een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag in de wet is vastgelegd en of deze taak ook zo ver reikt dat aan alle organisaties die deelnemen aan de cross-sectorale gegevensdeling gegevens verstrekt mogen worden en de publieke partij ook gegevens mag ontvangen van al deze organisaties.

Graag wordt opgemerkt dat de taak van de publieke partijen die willen gaan deelnemen aan de gegevensdeling, niet expliciet hoeft te zien op de opsporing en bestrijding van fraude. Het kan goed zijn dat het voor een publieke partij nodig is om deel te nemen aan de gegevensdeling teneinde te weten dat bepaalde personen verdacht worden van fraude, maar dat fraudebestrijding niet de 'core business' van deze partij is. Hierbij kan bijvoorbeeld gedacht worden aan een publieke partij die leningen verstrekt aan studenten. Ter voorkoming van fraude, kan het raadzaam zijn dat deze partij deelneemt aan de gegevensdeling en zo kan controleren of een persoon die een aanvraag voor een studentenlening indient, bekend is binnen het gegevensdelingsverband. De 'core business' van deze organisatie ziet echter niet zozeer op fraudebestrijding. Zoals hiervoor aangegeven dient wel altijd bij wet een taak aan deze partij te zijn toebedeeld op basis waarvan

de partij kan deelnemen aan de gegevensdeling. Zonder wettelijke basis kan een publieke partij niet deelnemen aan de gegevensdeling. Indien de wens bestaat dat opsporingsinstanties als politie of de FIOD ook als partij willen deelnemen aan het gegevensdelingsverband en dan ook gegevens willen inbrengen, dient aan de hand van de Wet politiegegevens beoordeeld te worden of een grondslag bestaat om gegevens te verstrekken aan de private organisaties die deelnemen aan de gegevensdeling.

Indien tevens publieke partijen willen gaan starten met de gegevensdeling, dient dus voorafgaand goed beoordeeld te worden of zij een grondslag hebben voor deze deelname en of deze grondslag ook zover reikt dat zij gegevens aan alle organisaties van het gegevensdelingsverband mogen verstrekken, dan wel mogen ontvangen. Privaat- en publieke samenwerkingsverbanden worden veelal vormgegeven in een Convenant waarin alle nadere afspraken worden vastgelegd omtrent de gegevensdeling. Indien tevens publieke partijen gaan deelnemen bij de gegevensdeling, kan het raadzaam zijn de samenwerking vast te leggen in een Convenant. Graag wordt wel opgemerkt dat een Convenant niet de juridische basis schept om gegevens te mogen delen. De publieke partijen dienen in dit geval altijd een juridische basis te hebben om gegevens te mogen delen.

3.2.1 Wet gegevensverwerking door samenwerkingsverbanden

Op het moment wordt gewerkt aan de Wet gegevensverwerking door samenwerkingsverbanden ('WGS'). Dit conceptwetsvoorstel is op het moment nog in voorbereiding en dan ook nog niet aangenomen door de Kamer. Indien deze wet wordt aangenomen kan dit een juridische basis bieden om een privaat-publiek samenwerkingsverband in te richten met het doel om fraude te bestrijden. De conceptwet biedt de mogelijkheid om een verband in te richten waarbij zowel private als publieke partijen kunnen deelnemen; een publieke partij dient wel altijd onderdeel te zijn van de samenwerking. De deelnemers van de samenwerking, het doel van het samenwerkingsverband en de waarborgen dienen bij AMvB te worden uitgewerkt. Het samenwerkingsverband moet worden opgericht ten behoeve van een zwaarwegend algemeen belang.
Dit kan bestaan uit:

- De voorkoming van onrechtmatig gebruik van overheidsgelden en het bevorderen dat aan wettelijke verplichtingen wordt voldaan tot betaling van belastingen,
- De uitoefening van toezicht op de naleving van wettelijke voorschriften,
- De handhaving van de openbare orde en veiligheid,
- De voorkoming, opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

In de toelichting bij het conceptwetsvoorstel wordt de voorkoming en bestrijding van fraude expliciet benoemd als een dergelijk belang en zelfs genoemd als één van de aanleidingen voor het opstellen van het conceptwetsvoorstel. Indien deze wetgeving wordt aangenomen, kan dit dus een basis bieden om een privaat-publiek samenwerkingsverband op te richten ten behoeve van het bestrijden van fraude. Indien een samenwerkingsverband wordt opgericht onder de WGS dient dit verband een algemeen belang te dienen en wordt het verband minder vanuit het perspectief van de private partijen om bedrijfsschade te verminderen, zoals hiervoor meer centraal heeft gestaan.

Concluderend
De AVG/UAVG laten mogelijkheden bestaan voor publieke partijen om tevens deel te nemen aan de cross-sectorale gegevensdeling t.b.v. fraudebestrijding. Er bestaat echter geen algemene wettelijke bepaling op basis waarvan allerlei publieke partijen mogen deelnemen aan de gegevensdeling. Er dient dan ook per partij beoordeeld te worden of een taak van algemeen belang of openbaar gezag in de wet is vastgelegd en of deze taak ook zo ver reikt dat aan alle organisaties die deelnemen aan de cross-sectorale gegevensdeling gegevens verstrekt mogen worden en de publieke partij ook gegevens mag ontvangen van al deze organisaties. Indien tevens publieke partijen gaan deelnemen bij de gegevensdeling, kan het raadzaam zijn de samenwerking vast te leggen in een Convenant. Graag wordt wel opgemerkt dat een Convenant niet de juridische basis schept om gegevens te mogen delen. De publieke partijen dienen in dit geval altijd een juridische basis te hebben om gegevens te mogen delen. Indien de wens bestaat dat ook politie en/of FIOD gaan deelnemen aan de gegevensdeling, dient aan de hand van de Wet politiegegevens beoordeeld te worden of een wettelijke grondslag bestaat om gegevens te verstrekken aan de organisaties die deelnemen aan de gegevensdeling.

Indien de WGS wordt aangenomen, kan deze wet mogelijk een eenvoudigere juridische basis bieden, dan op dit moment het geval is, om een privaat- publiek samenwerkingsverband op te richten om fraude te bestrijden. Nu deze wet nog in voorbereiding is en de definitieve wettekst nog niet beschikbaar is, is het nog afwachten hoe de WGS in de praktijk vorm gaat krijgen.

3.3 Verstrekken aan politie en/of andere opsporingsinstanties

Naast het in kaart brengen van het juridisch kader met betrekking tot het cross-sectoraal delen van gegevens tussen private partijen is, nu dit ook plaatsvindt in het systeem Cifas, ook gevraagd nader te kijken naar de juridische mogelijkheden voor politie en eventuele andere opsporingsinstanties, als de FIOD, om gegevens te ontvangen vanuit de cross-sectorale gegevensdeling ten behoeve van de bestrijding en opsporing van fraude. De opsporingsinstanties zijn in dit geval niet zelf deelnemer aan de gegevensdeling, maar ontvangen gegevens vanuit de gegevensdeling. Hieronder wordt nader ingegaan op de juridische basis voor deze situatie. Let er daarnaast op dat ook hierbij voldoende waarborgen getroffen moeten worden.

Als vanuit de cross-sectorale gegevensdeling gegevens verstrekt worden aan de politie of eventuele andere opsporingsinstanties als de FIOD, dient deze verstrekking in overeenstemming te zijn met de AVG en UAVG. Nu het verstrekken van gegevens uit de gegevensdeling een verwerking van strafrechtelijke gegevens is aan een ontvanger (de politie of FIOD), moet allereerst het verwerkingsverbod voor deze gegevens worden opgeheven. Een mogelijke opheffing waaronder de strafrechtelijke gegevens in dit geval door een organisatie doorgegeven kunnen worden aan de politie en de FIOD kan gevonden worden in artikel 33 lid 2 sub b UAVG:

'Persoonsgegevens van strafrechtelijke aard mogen worden verwerkt door de verwerkingsverantwoordelijke die deze gegevens ten eigen behoeve verwerkt ter bescherming van zijn belangen, voor zover het gaat om strafbare feiten die zijn of op grond van feiten en omstandigheden naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn'.

Op grond van deze bepaling mag een verwerkingsverantwoordelijke strafrechtelijke gegevens verwerken wanneer het vermoeden bestaat dat strafbare feiten jegens hem of jegens zijn personeel gepleegd zullen gaan worden, dan wel reeds gepleegd zijn. Beargumenteerd kan worden dat de verwerkingsverantwoordelijke op basis van deze opheffing voorts ook aangifte mag doen en dan ook de opsporingsinstanties op de hoogte mag brengen van hetgeen is voorgevallen.

Als het verwerkingsverbod is opgeheven, dient vervolgens een grondslag voor de verstrekking te worden gevonden in artikel 6 AVG. In dit kader, kan artikel 6 lid 1 sub f AVG een grondslag bieden voor de verstrekking. Het is in het gerechtvaardigd belang van de organisatie om gegevens te verstrekken aan opsporingsinstanties

om deze op de hoogte brengen, dan wel aangifte te doen van een strafbaar feit dat jegens hem of zijn personeel is gepleegd of vermoed wordt dat deze gepleegd gaat worden.

Het bovenstaande biedt een juridische mogelijkheid voor een organisatie die deelneemt aan de gegevensdeling om gegevens betreffende een fraudezaak te verstrekken aan politie en/of FIOD. Let wel: deze uitzondering is van toepassing voor een verwerkingsverantwoordelijke zelf, wat betekent dat de betreffende organisatie zelf de gegevens dient te verstrekken aan de politie en of eventuele andere opsporingsinstanties. Indien cross-sectoraal gegevens gedeeld gaan worden, dient hiermee rekening gehouden te worden. Er bestaat een juridische mogelijkheid voor een organisatie zelf om gegevens aan opsporingsinstanties te verstrekken, maar deze juridische basis rechtvaardigt volgens ons niet dat alle gegevens vanuit het samenwerkingsverband rechtstreeks worden doorgezonden aan opsporingsinstanties. Wanneer de cross-sectorale gegevensdeling wordt ingericht middels een fraudepreventiesysteem, kan bij de technische inrichting hiermee rekening gehouden worden. Het dient zo ingeregeld te worden dat de betreffende organisatie zelf de zaak invoert en bijvoorbeeld vanuit zijn account de zaak automatisch wordt doorgestuurd naar politie en/of FIOD. Het valt lastig te beargumenteren dat de verstrekking zo kan worden ingericht dat vanuit het fraudepreventiesysteem zelf een scan gemaakt wordt van alle nieuwe zaken die bijvoorbeeld die betreffende dag zijn ingevoerd door alle organisaties en op automatische wijze worden doorgestuurd naar politie en/of andere opsporingsinstanties. Een mogelijkheid die wel kan bestaan is dat door politie of FIOD een vordering wordt ingediend op basis van het Wetboek van Strafvordering ('WvSv') (art. 126nc WvSv e.v.) bij het fraudepreventiesysteem op basis waarvan in een specifiek geval gegevens verstrekt dienen te worden. Indien een dergelijke vordering door politie of de FIOD wordt ingediend, dienen – in overeenstemming met hetgeen hierover gesteld in het WvSv – de gegevens door de betreffende verwerkingsverantwoordelijke verstrekt te worden aan de opsporingsinstanties. Dit betreft dus echter een specifieke verstrekking en rechtvaardigt niet dat op automatische wijze alle nieuw toegevoegde zaken middels een scan door worden gestuurd. Dit kan juridisch gezien alleen worden ingericht zoals hiervoor omschreven.

3.3.1 Ontvangst door politie en/of andere opsporingsinstanties

Op verwerkingen door de politie is de Wet politiegegevens ('Wpg') en hieraan gelieerde wetgeving van toepassing. Dat betekent dat de AVG en UAVG niet van toepassing zijn op verwerkingen door politie voor zover het gaat over de opsporing van strafbare feiten. De verwerkingen die verricht worden door de FIOD (een bijzondere opsporingsdienst) ter uitvoering van de politietaken vallen tevens onder het regime van de Wpg. Indien gegevens vanuit de cross-sectorale gegevensdeling worden doorgegeven aan de politie en/of FIOD, baseren zij de ontvangst van deze gegevens op de Wpg en verwerken zij deze ter uitvoering van hun taken.

Concluderend
De AVG en UAVG bieden juridische mogelijkheden om vanuit de organisaties die deelnemen aan de cross-sectorale gegevensdeling gegevens te verstrekken aan de politie en eventuele andere opsporingsinstanties als de FIOD. Deze juridische mogelijkheden zien er echter op dat de organisaties zelf de gegevens verstrekken aan de opsporingsinstanties en rechtvaardigt niet dat vanuit de gegevensdeling alle gegevens van alle organisaties tezamen in één keer worden verstrekt aan politie en/of FIOD. Indien cross-sectoraal gegevens gedeeld gaan worden en dit mogelijk gebeurt door middel van een fraudepreventiesysteem, dient dus goed gekeken te worden hoe de verstrekking aan de opsporingsinstanties technisch wordt ingericht.

4 Cifas: het systeem voor cross-sectorale gegevensdeling ten behoeve van fraudebestrijding in het Verenigd Koninkrijk

4.1 Algemene beschrijving Cifas

Zoals in hoofdstuk één is aangegeven worden in het VK cross-sectoraal gegevens gedeeld tussen private- en publieke partijen ten behoeve van fraudebestrijding. In het VK wordt deze gegevensdeling gefaciliteerd door de organisatie Cifas. Cifas heeft meerdere databases opgericht waarin gegevens betreffende bepaalde vormen van fraude gedeeld kunnen worden tussen organisaties die aangesloten zijn als deelnemer bij de databases van Cifas. In het vervolg zullen deze organisaties worden aangeduid als deelnemers of deelnemende organisaties. Circa 400 organisaties uit de private sector en enkele uit de publieke sector delen gegevens en inlichtingen met elkaar middels de databases van Cifas.

Cifas voorziet in drie verschillende databases; de 'National Fraud' database, de 'Internal Fraud' database en het 'Immigration portal'.

De **'National Fraud'** database is bedoeld om gegevens uit te wisselen tussen de aangesloten organisaties ten behoeve van de bestrijding van fraude die wordt gepleegd door individuen of bedrijven. Fraude is, zoals reeds uit hoofdstuk 3 blijkt een veelomvattend begrip. De fraudezaken die in de National Fraud database worden opgenomen zien op:

- Identity Fraud: het indienen van een aanvraag voor een lening middels een gestolen identiteit;
- Facility Takeover Fraud: onbevoegde derden die bestaande accounts gebruiken om producten te bestellen of abonnementen af te sluiten;
- Application Fraud: aanvragers die bij een aanvraag voor een product of dienst valse documenten verstrekken;
- Asset Conversion Fraud: derden die goederen, veelal auto's, verkopen terwijl zij geen eigenaar zijn van het betreffende goed;
- Misuse of Facility Fraud: derden die rechtmatig een bankaccount of rekening openen, maar voorts deze rekening of dit account misbruiken door daarop leningen te laten storten die zij op frauduleuze wijze hebben verkregen;
- False Insurance Claim: het indienen van valse documenten om een verzekeringsclaim uitgekeerd te krijgen.

Nieuwe vormen van fraude kunnen toegevoegd worden indien dit nodig is om aan de behoeften van de deelnemende organisaties te voldoen.

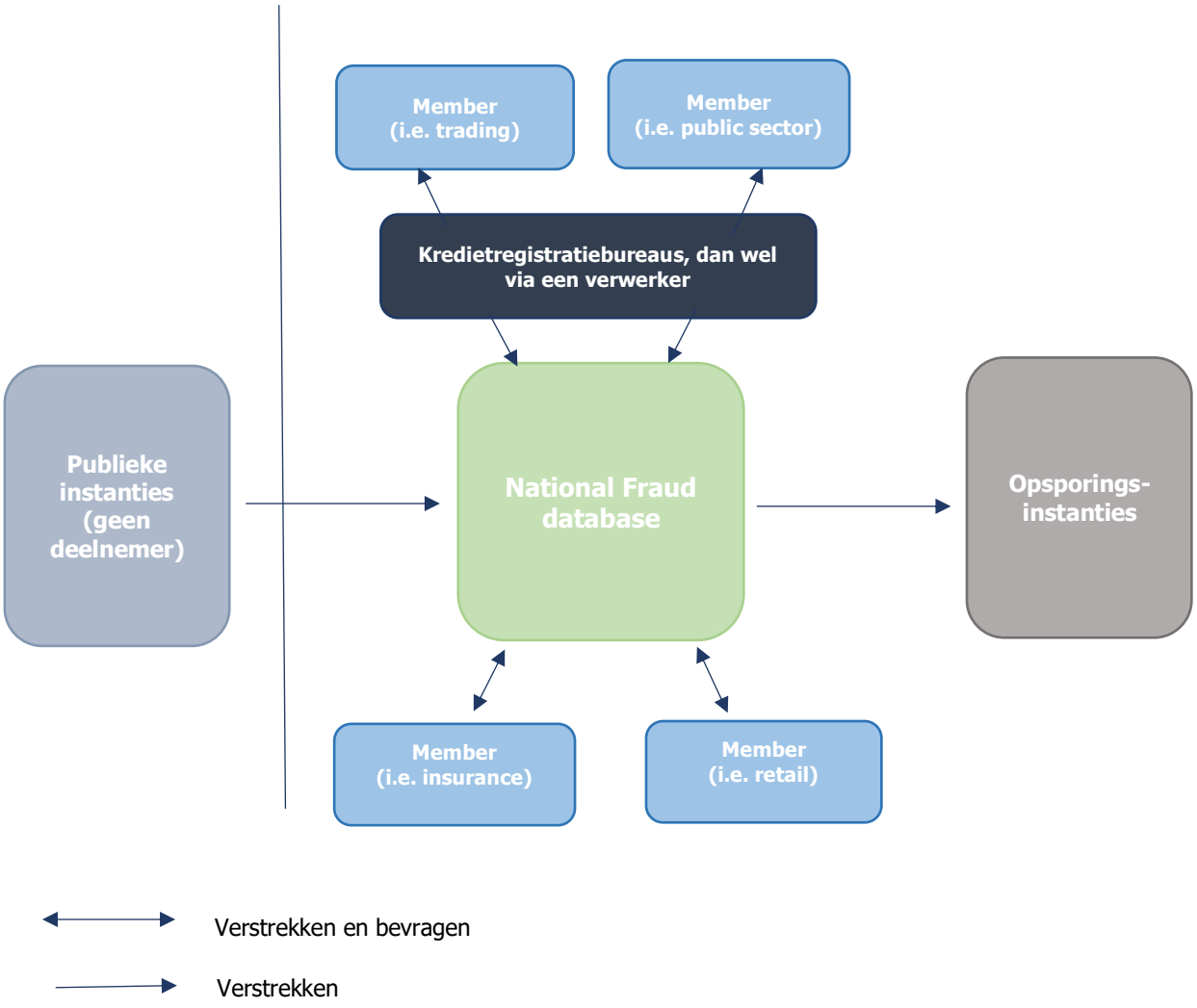
De deelnemers kunnen gegevens op verschillende manieren (laten) invoeren in de database. Zo kunnen de deelnemende organisaties de gegevens rechtstreeks invoeren, maar kunnen zij – indien ze daar reeds bij aangesloten zijn – de gegevens ook middels een kredietwaardigheidsbureau laten invoeren of middels een verwerker.

De 'National Fraud' database kenmerkt zich doordat de deelnemende organisaties degene zijn die de fraudezaken invoegen in de database. Naast de gegevens van de deelnemende organisaties, worden ook vanuit publieke organisaties gegevens toegevoegd aan de database. Deze publieke organisaties verstrekken dus gegevens aan de databases van Cifas, maar zijn zelf geen deelnemer van de databases. Zo verstrekken de 'General Register Office', de 'Royal Mail', de 'Metropolitan Police', het 'Department for Work and Pensions',

'Her Majesty's Revenu and Customs' en de 'National Trading Standards' gegevens aan de database zonder dat zij zelf een deelnemende organisatie zijn van de databases van Cifas.

Tenslotte worden vanuit de database automatisch gegevens verstrekt aan opsporingsinstanties als het National Fraud Intelligence Bureau ('NFIB'), de National Crime Agency ('NCA") en de politie. Vanuit Cifas worden dagelijks de nieuw binnengekomen zaken doorgestuurd aan de opsporingsinstanties teneinde hen te ondersteunen bij het doen van onderzoek naar en de opsporing van fraudezaken.

Visueel kan de werking van de 'National Fraud' database als volgt worden weergeven:



De '**Internal Fraud'** database ziet op het delen van gegevens ten behoeve van het bestrijden van fraude gepleegd door personeel. Deze database stelt werkgevers in staat om gevallen van fraude door personeel te registreren en beoogt te voorkomen dat personen ongestoord in dienst kunnen treden bij een nieuwe organisatie.

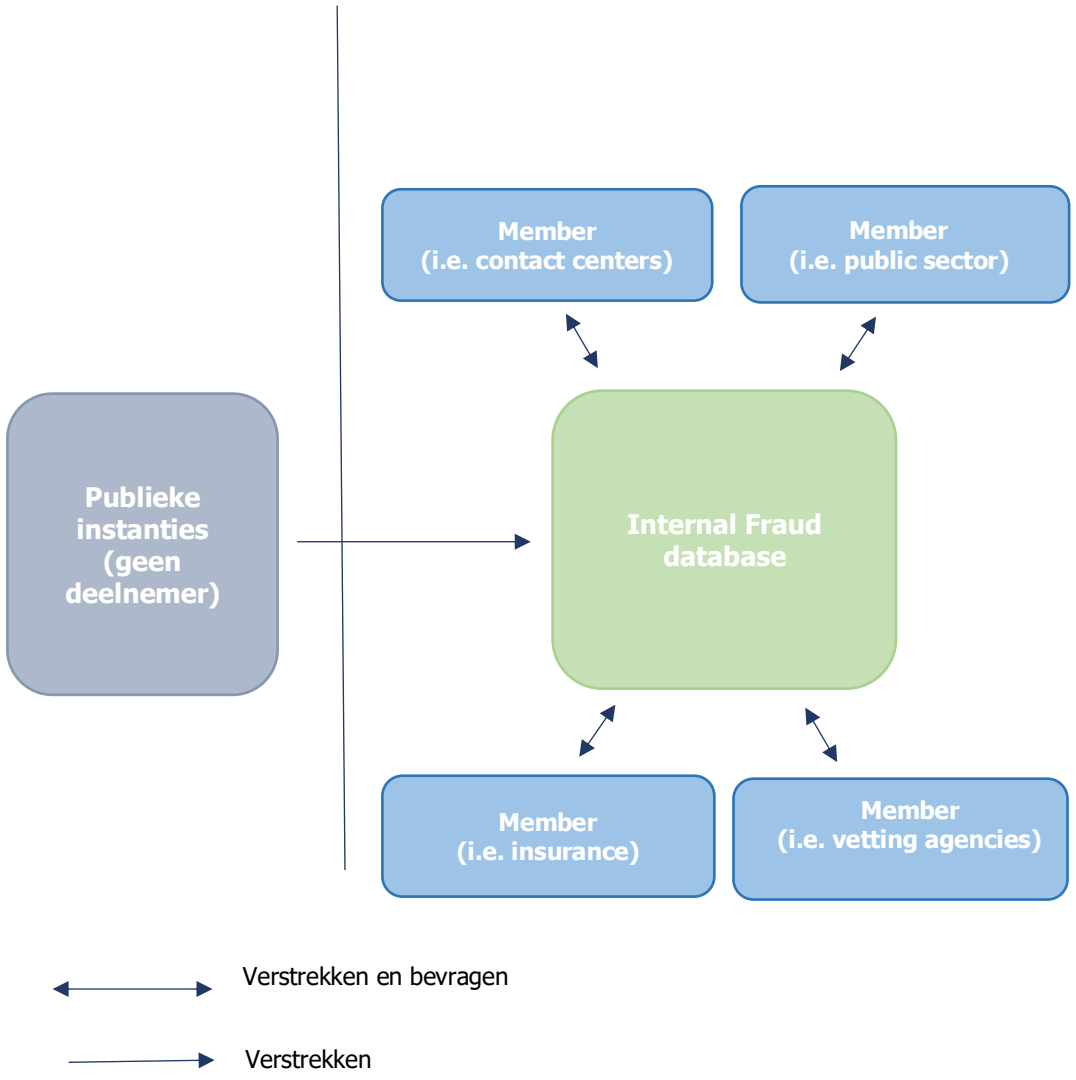
In de 'Internal Fraud' database staan zaken opgenomen die zien op:

- medewerkers die diefstal hebben gepleegd;
- medewerkers die onrechtmatig klantgegevens voor eigen (commercieel) gewin hebben gebruikt;

- medewerkers die substantiële verliezen hebben veroorzaakt, dan wel aanzienlijke reputatieschade hebben aangericht;
- medewerkers die bij hun sollicitatie valse documenten, als diploma's/certificaten hebben aangeleverd;
- medewerkers die ziekteverlof hebben geclaimd op grond van valse documenten.

Deelnemers hebben toegang tot de database om te controleren of een betreffend persoon aangemeld is in de database door andere deelnemende organisaties. Dit kan onder meer worden gedaan om sollicitanten te screenen of om huidige werknemers te screenen. Niet alleen vast personeel kan toegevoegd worden aan de database, maar ook uitzendkrachten kunnen ingevoerd worden in de database.

Visueel kan de werking van de 'Internal Fraud' database als volgt worden weergeven:



Het **'Immigration Portal'** is in 2014 naar aanleiding van de Immigration Act 2014 opgericht. Dit portaal is niet vanuit Cifas opgericht, maar is bij Cifas ondergebracht omdat zij, aldus Cifas, met de 'National Fraud' en 'Internal Fraud' databases, aangetoond hebben over goede, betrouwbare systemen te beschikken en dan ook goed in staat zijn een dergelijk portaal te faciliteren. Op grond van artikel 40 van de Immigration Act 2014, dienen banken middels het 'Immigration Portal' te controleren, zodra zij een aanvraag voor een bankrekening hebben ontvangen, of de aanvrager rechtmatig in het VK verblijft. In tegenstelling tot de twee andere

databases wordt de informatie in het 'Immigration portal' uitsluitend aangeleverd door het Home Office[31]. Nu dit portaal is opgericht op basis van een wettelijke verplichting binnen het VK en het portaal niet zozeer ziet op cross-sectorale gegevensdeling tussen private partijen ten behoeve van fraudebestrijding, wordt de werking van dit portal niet meegenomen in de verdere bespreking van dit hoofdstuk.

4.1.1 Oprichting Cifas

Cifas bestaat inmiddels meer dan dertig jaar en is opgericht in 1988. Zeven kredietorganisaties zijn destijds begonnen met het delen van gegevens teneinde fraude te bestrijden. Aangegeven vanuit Cifas is dat vanuit de Engelse overheid, alsmede opsporingsinstanties weinig prioriteit werd gegeven aan fraudebestrijding en de opsporing van fraudezaken, onder andere omdat de instrumenten van de opsporingsdiensten, aldus Cifas, hier wellicht niet het meest effectief waren. Private partijen werden vanuit de overheid dan ook geadviseerd gezamenlijk te bekijken op welke wijze zij actie konden ondernemen tegen fraude. Nu vele organisaties door fraudezaken, en het ontbreken van een gestructureerde aanpak daarin, veel financieel verlies leden, bestond voor deze organisaties de noodzaak dit gezamenlijk op te pakken.

In beginsel zijn zeven kredietorganisaties gestart met de gegevensdeling ten behoeve van de bestrijding van fraude waarvan zij zelf, als organisaties zijnde, in beginsel schade door hadden. Nadat bleek dat de gegevensdeling daadwerkelijk een meerwaarde had bij de aanpak van fraudezaken en deze organisaties minder verlies leden door fraude, nam het aantal deelnemende organisaties toe. Omstreeks twintig jaar na de oprichting van de 'National Fraud' database, is – vanuit de wens van de deelnemers – ook de 'Internal Fraud' database opgericht.

Cifas is opgericht door private partijen zonder enige vorm van overheidsondersteuning. De organisatie is thans een non-profit organisatie die volgens de organisatie zelf nog steeds volledig onafhankelijk opereert. Cifas wordt volledig gefinancierd door de bijdragen die de deelnemende organisaties jaarlijks dienen te betalen en ontvangt geen overheidssubsidies.

Nota bene:
Nu Cifas een naar privaatrecht opgerichte instantie is en volledig onafhankelijk van de overheid opereert, is door Cifas aangegeven dat vanuit de Engelse overheid geen ministeriële verantwoordelijkheid bestaat ten aanzien van de databases van Cifas en de gegevensverwerkingen die daarin plaatsvinden.

Dit kan anders zijn met betrekking tot de eventuele verantwoordelijkheid ten aanzien van specifieke publieke instanties die deelnemende organisaties zijn van de databases van Cifas, maar voor Cifas als beheerder en het geheel van gegevensverwerkingen die verricht worden door middel van de databases van Cifas bestaat geen ministeriële verantwoordelijkheid.

4.1.2 Governance

Cifas staat onder leiding van het Bestuur. Het Bestuur is verantwoordelijk voor het bepalen van de strategische richting en doelstellingen van de organisatie, alsook het meten van de behaalde resultaten ten opzichte van de gestelde doelstellingen. Daarnaast onderzoekt het Bestuur mogelijke risico's en voert het controles uit. De bestuursleden zijn voorts verantwoordelijk voor het bepalen van de visie, missie en waarden van Cifas. Het houdt toezicht op de Adviesraad en de werkzaamheden die de Adviesraad uitvoert. Het Bestuur wordt geleid door de voorzitter.

De Adviesraad heeft de verantwoordelijkheid om toezicht te houden op de operationele doeltreffendheid van Cifas. De Adviesraad behartigt daarnaast de belangen van de belangrijkste stakeholders van Cifas: de

[31] Ministerie van Binnenlandse Zaken

deelnemende organisaties, maar ook andere partijen die gebruik maken van diensten van Cifas zoals publieke organisaties, dan wel opsporingsinstanties. Ten behoeve van het behartigen van de belangen van deze stakeholders, adviseert de Adviesraad zowel de Executive Group als het Bestuur. De Adviesraad bestaat uit afgevaardigden van deelnemende organisaties uit de verschillende sectoren die vertegenwoordigd zijn in de databases.

De dagelijkse leiding van Cifas is in handen van de Executive Group. De Executive Group staat onder leiding van de Chief Executive en de Chief Operating Officer.

4.1.3 Budget

Cifas wordt gefinancierd door bijdragen die de deelnemende organisaties jaarlijks betalen. Afhankelijk van de grootte van de organisatie en de hoeveelheid omzet die een organisatie heeft, wordt vastgesteld hoeveel de organisatie jaarlijks dient bij te dragen. Zoals reeds eerder uiteengezet is Cifas een non-profit organisatie; de bijdragen die de deelnemende organisaties jaarlijks betalen worden geïnvesteerd in de werkzaamheden van Cifas en niet uitgekeerd aan aandeelhouders. Naast de jaarlijkse bijdrage dienen de deelnemende organisaties ook een jaarlijkse verzekeringspremie te betalen. Deze verzekeringspremie beschermt een deelnemende organisatie onder meer tegen claims van derden wanneer de deelnemende organisatie een beslissing heeft genomen ten aanzien van een derde op basis van foutief ingediende informatie door een andere deelnemende organisatie. Indien een deelnemende organisatie dus foutieve informatie heeft ingediend en een andere organisatie op basis daarvan een beslissing heeft genomen jegens een persoon, kan deze laatste organisatie een beroep doen op de verzekering indien een claim wordt ingediend.

Zodra een organisatie zich aanmeldt bij Cifas, dienen zij eenmalig 'inschrijfgeld' te betalen; dit bedraagt 50% van de jaarlijkse bijdrage. Deze eenmalige inschrijfkosten dekken alle kosten die gemaakt dienen te worden om deelnemer te worden bij Cifas en bevatten daarnaast een training voor het personeel dat Cifas gaat gebruiken.

Zodra je als organisatie je hebt aangemeld voor de 'National Fraud database' betekent dit dat je ook kan deelnemen aan de 'Internal Fraud database'. Er zijn voor deelnemers van de nationale database geen extra kosten verbonden aan de deelname van de interne database.

4.1.4 Deelnemende partijen

Inmiddels zijn circa 400 organisaties aangesloten als deelnemer bij (één van de) databases van Cifas. Dit zijn voornamelijk private organisaties, maar ook enkele (lokale) publieke organisaties. Op dit moment zijn circa 98% van de organisaties afkomstig uit de private sector en 2% van de deelnemende organisaties publiek. Cifas streeft ernaar het aantal publieke deelnemers te verhogen naar 5%.

Deelnemende organisaties

De organisaties die deelnemen aan Cifas zijn afkomstig uit verscheidene sectoren, zoals de financiële sector, kredietsector, retail sector, verzekeringssector, telecommunicatiesector en handelssector. Ook nemen verscheidene postorderbedrijven en callcenters aan de samenwerking deel. Vanuit de publieke sector neemt onder meer de organisatie deel die zich bezighoudt met het verstrekken van leningen aan studenten, maar ook Home office is deelnemer van Cifas.

Hieronder is aangegeven hoeveel organisaties (absoluut en procentueel) per sector deelnemen aan de National Fraud database. Een dergelijk overzicht kan door Cifas niet aangeleverd worden voor de Internal Fraud database.

Sector:	Aantal organisaties:	Percentage[32]:
Bankwezen	83	26%
Financiering	54	17%
Alternatieve leningen	47	14%
Hypotheek	34	10%
Anders	26	8%
Verzekering	21	6%
Retail	16	5%
Publieke sector	10	3%
Krediet- en bouwmaatschappijen	9	3%
Creditcard	9	3%
Factoring	8	2%
Telecom	8	2%

Zaken toegevoegd door publieke organisaties

De zaken die in de databases van Cifas staan worden ingevoerd door de deelnemers zelf. Daarnaast verstrekken enkele publieke organisaties ook gegevens aan Cifas, zonder dat zij zelf deelnemer zijn aan de databases van Cifas. Zo verstrekken het 'General Register Office' (gegevens betreffende overledenen), de 'Royal Mail' (gegevens betreffende frauduleuze doorverwijzingen), 'Metropolitan Police' (gegevens betreffende valse en frauduleuze identiteitsdocumenten), 'Department for Work and Pensions and Her Majesty's Revenu and Customs' (gegevens betreffende veroordelingen voor belastingfraude) en 'National Trading Standards' (gegevens betreffende individuen en bedrijven die betrokken zijn bij fraude- en/of scamactiviteiten) gegevens aan Cifas en aan deelnemers van Cifas teneinde bij te dragen aan de bekendwording van fraudezaken en de voorkoming daarvan.

Verstrekking aan opsporingsinstanties

Daarnaast worden vanuit de 'National Fraud' database rechtstreeks gegevens verstrekt aan de NFIB, NCA en de politie. Op dagelijkse basis worden automatisch rapporten doorgestuurd aan deze organisaties waarin nieuwe fraudezaken zijn opgenomen, ingevoerd in de database door de deelnemende partijen. Deze rapporten worden verstrekt ten behoeve van de ondersteuning in de opsporing van (omvangrijke) fraudezaken, maar onder meer ook teneinde specifieke opsporingsoperaties te ondersteunen naar vermoedens van witwassen, corrupte professionals en andersoortige criminaliteit. Het is daarnaast voor politie ook mogelijk om een specifiek verzoek om informatie betreffende een verdachte in te dienen bij Cifas. Met de partijen aan wie Cifas gegevens verstrekt is een overeenkomst afgesloten waarin afspraken zijn gemaakt over de manier waarop en het doel waarvoor de opsporingsinstanties gebruik mogen maken van de gegevens die Cifas aan hen verstrekt.

4.1.5 Toetreding

In beginsel kunnen allerlei organisaties uit verscheidene sectoren zich aanmelden als deelnemer bij Cifas. De deelname is niet beperkt tot bepaalde sectoren, maar kenmerkt zich juist door sectoraal overstijgend samen te werken. Dat betekent dat alle organisaties kunnen toetreden tot Cifas.

Om toe te kunnen treden tot Cifas, dienen de organisaties wel aan de volgende vereisten te voldoen:

- Organisaties dienen zelf te beschikken over de persoonsgegevens: *'they need to 'own' the data.'* Om aan dit vereiste te voldoen dienen organisaties die willen deelnemen aan Cifas aan te tonen

[32]Het overzicht met daarin aangegeven hoeveel organisaties (absoluut en procentueel per sector deelnemen aan de National Fraud database is aangeleverd door Cifas. Het is bij onderzoekers bekend dat het totale percentage van alle sectoren totaal uitkomt op 99%. Nu de cijfers afkomstig zijn van Cifas, kan niet gezegd worden waar de 1% foutmarge zich bevindt.

dat zij geregistreerd staan bij de Information Commissioner's Office (ICO) als verwerkingsverantwoordelijke en dan ook een fee betalen aan de ICO.[33];
- Organisaties dienen in hun eigen verwerkingsregister op te nemen dat zij gegevens delen met Cifas en de deelnemende partijen van Cifas;
- Organisaties moeten procedures ingericht hebben om fraude te kunnen identificeren en te classificeren. Voorts dienen organisaties de geïdentificeerde fraudegevallen ook toe te voegen aan de database(s);
- Organisaties dienen de door Cifas opgestelde procedures, die bestaan uit de basisprincipes en het handboek (zie 4.5), teneinde te voldoen aan de wetgeving op het gebied van de bescherming van persoonsgegevens te accepteren en ook na te leven. Organisaties dienen te accepteren dat jaarlijks een audit kan plaatsvinden ten aanzien van de naleving van deze procedures.
- Organisaties dienen, middels een 'fair processing notice' betrokkenen te informeren over de raadpleging van en verstrekking van gegevens aan Cifas en de wijze waarop hun gegevens gebruikt kunnen worden;
- Organisaties dienen een vrijwaring te verstrekken aan de andere deelnemende organisaties en aan Cifas tegen claims van derden. Zie 4.1.3 over de verzekeringspremie.

Indien organisaties aan bovenstaande elementen voldoen, kunnen zij deelnemen aan Cifas. Via de website van Cifas kunnen organisaties een verzoek tot deelname doen.

4.1.6 Toegevoegde waarde van de databases

Vanuit Cifas is aangegeven, alsmede op basis van de stukken op de website kan worden opgemaakt, dat de deelnemende organisaties daadwerkelijk voordeel behalen uit hun deelname aan de databases van Cifas. Uit het jaarrapport van 2017 is gebleken dat halverwege het jaar 2017 reeds £ 1,3 miljard was bespaard door de cross-sectorale gegevensdeling tussen de deelnemende partijen.[34] Dit betekent voor een deelnemende organisatie voor iedere pond die zij betalen een return on investment van £ 239. Naast het feit dat deelnemende organisaties minder financiële schade hebben door de fraude die gedetecteerd is middels de gegevensdeling, heeft Cifas ook een preventieve werking voor de deelnemende organisaties. Eventuele kwaadwillenden zijn op de hoogte van de databases van Cifas en hebben ook inzicht in de organisaties die deelnemen aan de samenwerking; het doen van fraudepogingen bij deze organisaties is minder effectief, nu door deelname aan de samenwerking in Cifas de kans hoger is dat de poging tot fraude opgemerkt wordt.

Vanuit Cifas is de toegevoegde waarde vooral geënt op de return on investment die de organisaties behalen uit hun deelname aan de databases van Cifas. Uit de 'Code of Practice for public authorities disclosing information to a specified 'anti-fraud organisation"[35] blijkt echter dat de verstrekking van gegevens vanuit publieke organisaties aan Cifas, dan wel deelnemers van Cifas meer een algemeen belang dient. Daarin wordt aangegeven dat overheidsinstanties een bijzondere verantwoordelijkheid hebben om de publieke middelen die zij beheren te beschermen en er zorg voor te dragen dat het geld van de belastingbetaler niet gebruikt wordt voor frauduleuze activiteiten. Gelet op deze verantwoordelijkheid is in de Serious Crime Act de mogelijkheid neergelegd om gegevens te verstrekken aan (deelnemers van) een 'anti-fraud organisation' teneinde fraude te bestrijden.

[33] Een registratie bij de ICO houdt kort gezegd in dat iedere organisatie die gegevens verwerkt en daarmee verwerkingsverantwoordelijke is een vergoeding dient te betalen aan de ICO. Deze verplichting dient niet verward te worden met het aanvragen van een vergunning en ziet ook niet specifiek op de deelnemers van Cifas. Deze verplichting geldt ten aanzien van alle verwerkingverantwoordelijken in het VK.

[34] Cifas, Annual report and financial statements for the year ended 31 December 2017, p. 1-4.

[35] Code of practice for public authorities disclosing information to a specified anti-fraud organisation under sections 68 to 72 of the Serious Crime Act 2007

4.2 Feitelijke werking van het systeem

4.2.1 Wanneer komt een zaak in aanmerking voor de databases van Cifas?

De deelnemende organisaties dienen zelf te bepalen of een zaak in aanmerking komt om toegevoegd te worden aan (één van de) databases van Cifas. Organisaties dienen zelf te beoordelen of een potentiële fraudezaak voldoet aan de vier pijlers van bewijslast. Indien dit het geval is, dient de zaak te worden toegevoegd aan de databases.

Deelnemers die zaken toevoegen aan de databases van Cifas dienen deze te kunnen onderbouwen met bewijs. Hierbij dienen de volgende 'vier pijlers' in acht te worden genomen:

1. Er zijn redelijke gronden om aan te nemen dat fraude is gepleegd, dan wel dat gepoogd is fraude te plegen;
2. Er moet voldoende bewijsmateriaal zijn om het feit te onderbouwen. Dit bewijsmateriaal moet zodanig zijn dat voldoende grond bestaat om aangifte te doen bij de politie;
3. Het strafbare feit moet identificeerbaar zijn en vallen onder één van de vormen van fraude die onderdeel is van de databases (zie 4.1);

'National Fraud' database:

4. Voordat de zaak wordt ingediend, moet de deelnemende organisatie het aangevraagde product hebben afgewezen, de aanvraag hebben ingetrokken of beëindigd wegens de gepoogde of gepleegde fraude, tenzij de deelnemer verplicht is het product te leveren of de aanvrager het volledige voordeel reeds heeft ontvangen.

'Internal Fraud' database:

5. Voordat de zaak wordt ingediend, moet de deelnemende organisatie de sollicitant hebben afgewezen, de dienstbetrekking hebben opgezegd of fraude hebben geïdentificeerd, dan wel ander relevant gedrag nadat de werknemer de werkgever heeft verlaten.

De compliance afdeling van Cifas controleert op maandelijkse basis één of twee van de zaken die toegevoegd zijn door een deelnemer. Deze controle vindt plaats teneinde te checken of de deelnemende organisatie bij toevoeging van de zaak de bewijslast op juiste wijze in acht heeft genomen.

De deelnemers dienen betrokkenen te informeren over de verwerkingen die plaatsvinden middels de databases van Cifas. De informatieplicht is ook één van de principes die ontwikkeld zijn om zorg te dragen voor een zorgvuldige gegevensverwerking (zie 4.5). De wijze waarop betrokkenen geïnformeerd worden verschilt per database. Cifas vereist niet dat betrokkenen die opgenomen worden in de '**National Fraud' database** voorafgaand specifiek geïnformeerd worden over de opname in de database. Bij de nationale database wordt volstaan met een 'Fair processing notice' die de deelnemende organisaties verstrekken aan betrokkenen wanneer zij een aanvraag doen voor een lening of product of die opgenomen staan op de websites van de deelnemende organisaties, waarin onder meer uitgelegd wordt dat Cifas geraadpleegd wordt op het moment dat bijvoorbeeld een aanvraag wordt ingediend en dat gegevens verstrekt kunnen worden aan Cifas, voor welke doelen deze gegevens worden verstrekt en welke beslissingen voorts op basis van deze gegevens genomen kunnen worden.

Op het moment dat een betrokkene bij een andere organisatie een aanvraag indient en de aanvraag voorts wordt afgewezen omdat de betreffende betrokkene opgenomen staat in de database, raakt de betrokkene op de hoogte dat hij of zij opgenomen staat in de database. Een betrokkene kan dan te allen tijde een inzageverzoek doen bij Cifas of bij de organisatie die het verzoek heeft afgewezen. Cifas handelt zelf het inzageverzoek van de betrokkene af of geleidt het inzageverzoek door aan de juiste organisatie. De betrokkene kan naar aanleiding van het inzageverzoek een klacht indienen tegen opname van zijn gegevens in de

database. De klacht wordt in beginsel afgehandeld door de deelnemende organisatie die de gegevens van de betrokkene heeft vastgelegd. Indien de klacht niet naar tevredenheid wordt afgehandeld, kan de betrokkene de klacht voorleggen aan Cifas. Cifas gaat na of de betreffende organisatie op juiste wijze ten aanzien van de betrokkene heeft gehandeld. Indien de registratie onjuist is, wordt de betrokkene verwijderd uit de database. Mocht betrokkene van mening zijn dat Cifas de ingediende klacht niet op juiste wijze heeft afgehandeld, dan kan betrokkene de klacht voorleggen aan de instantie die bevoegd is klachten af te handelen in de sector waar de organisatie, tegen wie de klacht is gericht, onder valt. In de financiële sector betreft dit een ombudsman, maar dit kan per sector verschillen.

Voordat een zaak ingediend wordt bij de **'Internal Fraud database'** dient de betrokkene, naast de 'fair processing notice' hierover ook specifiek geïnformeerd te worden. Om de betrokkenen te informeren is een standaard notificatie opgesteld. Deze notificatie is opgesteld in samenspraak met de ICO, waarbij wordt opgemerkt dat de ICO de notificatie niet expliciet heeft goedgekeurd maar wel een bijdrage heeft geleverd aan het opstellen daarvan.

4.2.2 Hoe werken de databases van Cifas?

Als voldoende bewijs bestaat om een zaak toe te voegen aan (één van de) databases, dient een deelnemende organisatie de zaak te registreren in de database. Bij registratie van een nieuwe zaak is niet exact voorgeschreven welke gegevens een deelnemende organisatie betreffende een zaak moet registreren. In elk geval de naam, het adres en de geboortedatum van de betreffende persoon dienen geregistreerd te worden. Daarnaast bestaan nog extra velden die de registrerend deelnemer kan invullen (denk hierbij aan het e-mailadres van de betrokkene of het bankrekeningnummer). Hoe meer gegevens ingevuld kunnen worden, hoe beter dat voor de kwaliteit en effectiviteit van het systeem is.

Om de juistheid van de gegevens te waarborgen en te voorkomen dat deelnemende organisaties te veel gaan registreren, zijn de velden ingericht als 'drop down' velden en betreffen het geen open velden. Bij de registratie van een nieuwe zaak, zijn slechts een aantal open velden waar deelnemende organisaties vrij zijn informatie op te nemen. In het Handboek zijn richtlijnen gegeven voor de registratie van nieuwe zaken.

Wanneer een organisatie controleert of een betreffend persoon of organisatie is opgenomen in de database en of er dan ook een match is, kan de deelnemer in de database zoeken op naam, telefoonnummer, geboortedatum of adres. De deelnemer hoeft slechts één van deze gegevens in te voeren om te controleren of deze gegevens al zijn opgenomen in de database. Wel is het zo dat je uitsluitend resultaat krijgt als er een match is. Cifas tracht hiermee te voorkomen dat deelnemende partijen een 'phishing expedition' doen en de gehele database doorlopen. Er moet een gegeven worden ingevoerd en er komt uitsluitend resultaat als een match bestaat. Daarnaast dient bij iedere bevraging van de database aangegeven te worden voor welk doel de check wordt gedaan (screening sollicitant, aanvraag voor lening et cetera). Indien een match bestaat, krijgt de bevragende organisatie inzicht in de details die opgenomen zijn over de betreffende persoon. Dit betreffen zowel details over hetgeen is voorgevallen als gegevens over de persoon zelf (dit kunnen onder andere zijn de naam, de geboortedatum, het adres, financiële gegevens en contactgegevens). Ook krijgt de bevragende organisatie gegevens over de organisatie die de zaak heeft ingediend en waarom de zaak is ingediend. De bevragende organisatie kan contact opnemen met de organisatie die de zaak heeft ingediend om meer informatie te verkrijgen, maar vanuit Cifas is aangegeven dat de bevragende organisatie veelal al voldoende informatie krijgt uit de database en contact met de andere organisatie vaak niet nodig is.

Indien sprake is van een match dient de deelnemende organisatie, die de database heeft bevraagd teneinde een mogelijke fraudeur te controleren, onderzoek uit te voeren naar de aanvraag (of enige andere vorm waarmee fraude is gepleegd) die de bevragende deelnemende organisatie van de mogelijke fraudeur heeft ontvangen. Als blijkt dat ook bij deze aanvraag frauduleus is gehandeld, identificeert de deelnemende organisatie om welk soort type fraude het gaat en voegt deze zaak ook toe aan de database als zijnde een

nieuwe zaak. Op deze manier wordt de informatie die opgenomen is in de database betreffende een bepaald persoon steeds omvangrijker en sterker. Blijkt geen sprake van fraude te zijn dan vervolgt de bevragende deelnemende organisatie het proces met de gecontroleerde persoon in principe gewoon volgens normale bedrijfsprocedures.

Zodra een zaak geregistreerd wordt in de 'National Fraud' database blijft de zaak voor zes jaar geregistreerd staan. Na zes jaar worden de gegevens uit de database verwijderd. In de 'National Fraud' database worden ook gegevens betreffende slachtoffers geregistreerd; deze gegevens worden twee jaar bewaard. De zaken in de 'Internal Fraud' database blijven drie jaar geregistreerd staan; na drie jaar worden de zaken verwijderd uit de database.

4.3 Rechtmatigheid gegevensdeling

4.3.1 Gegevensdeling in databases Cifas

De AVG is een Europese wet die rechtstreeks van toepassing is binnen de Europese lidstaten. Dat betekent dat het VK, totdat zij de Europese Unie verlaat,[36] onder de werking van de AVG valt en verwerkingen van persoonsgegevens dan ook in overeenstemming dient plaats te vinden met de AVG. De verwerkingen die plaatsvinden middels Cifas dienen dan ook aan het wettelijk kader te voldoen als uiteengezet in hoofdstuk twee.

Zoals reeds in hoofdstuk twee is uiteengezet, laat de AVG op bepaalde punten ruimte om specifieke bepalingen op te nemen of uitzonderingen te maken. In het VK zijn deze specifieke bepalingen vastgelegd in de Data Protection Act 2018. Voor de beoordeling van de gegevensverwerkingen die plaatsvinden middels de databases van Cifas dient dan ook gekeken te worden naar de AVG in samenhang met de Data Protection Act 2018.

De gegevens die verwerkt worden in de databases van Cifas kunnen aangemerkt worden als strafrechtelijke gegevens. Strafrechtelijke gegevens mogen op grond van artikel 10 AVG uitsluitend worden verwerkt onder toezicht van de overheid of wanneer dit specifiek bij wet is geregeld. In de Data Protection Act 2018 zijn de uitzonderingen opgenomen op grond waarvan strafrechtelijke gegevens alsnog verwerkt mogen worden.

Vanuit Cifas is aangegeven dat zij, alsmede de deelnemende organisaties, op grond van section 10, part 1 jo. Schedule 1, section 14 Data Protection Act 2018 strafrechtelijke gegevens mogen verwerken wanneer dit:

a. *'Is necessary for the purposes of preventing fraud or a particular kind of fraud, and*
b. *Consists of:*
    I. *The disclosure of personal data by a person as a member of an anti-fraud organisation;*
    II. *The disclosure of personal data in accordance with arrangements made by an anti-fraud organisation; or*
    III. *The processing of personal data disclosed as described in sub-paragraph (I) or (II).'*

Met de term 'anti-fraud organisation' wordt gedoeld op dezelfde term als die gebruikt wordt in de Serious Crime Act 2007. In artikel 68 van de Serious Crime Act 2007 wordt een 'anti-fraud organisation' omschreven als een organisatie die het mogelijk maakt informatie te delen ten behoeve van het bestrijden van fraude of de bestrijding van een bepaalde vorm van fraude of die één van deze functies als doel of als één van zijn doelen heeft. In de Code of Practice[37] die opgesteld is op grond van artikel 71 Serious Crime Act 2007 en

[36] Met betrekking tot de Brexit wordt graag nog het volgende opgemerkt. Zodra het VK de EU verlaat, dan wel aan het einde van de overeengekomen overgangsperiode, zal de GDPR worden verwerkt in een nieuwe wet (waarschijnlijk in de wet waarin de gehele intrekking uit de EU geregeld zal worden). Dit is echter nog zeer afhankelijk van de wijze waarop de Brexit geregeld zal worden.
[37] Code of practice for public authorities disclosing information to a specified anti-fraud organization under sections 68 to 72 of the Serious Crime Act 2007

gelezen dient te worden in samenhang met de Serious Crime Act, is Cifas expliciet benoemd als een 'anti-fraud organisation'.
Om de gegevensverwerking(en) gerechtvaardigd te maken, dienen de verwerkingen altijd gebaseerd te kunnen worden op één van de grondslagen uit artikel 6 AVG. Cifas heeft aangegeven dat zowel zij als organisatie als de deelnemende organisaties gegevens verwerken ten behoeve van hun gerechtvaardigd belang conform artikel 6 lid 1 sub f AVG om fraude te bestrijden.

4.3.2 Deelname publieke partijen

Zoals uit de algemene beschrijving blijkt zijn ook publieke organisaties lid van Cifas, dan wel verstrekken zij gegevens aan de databases van Cifas teneinde bij te dragen aan de bestrijding van fraude zonder dat zij lid zijn van Cifas. In de Serious Crime Act 2007 is de juridische basis neergelegd voor de verstrekking van gegevens door publieke organisaties aan Cifas. Op grond van artikel 68 Serious Crime Act 2007 mogen publieke organisaties als lid van een 'anti-fraud organisation' gegevens verstrekken ten behoeve van het bestrijden van fraude of het bestrijden van een bepaalde vorm van fraude of in het geval zij geen lid zijn wanneer dit plaatsvindt in overeenstemming met de regels die de 'anti-fraud organisation' heeft opgesteld. De Serious Crime Act 2007 biedt zowel een juridische basis voor publieke organisaties die deelnemer zijn van Cifas als publieke organisaties die geen deelnemer zijn om gegevens te verstrekken. De gegevens mogen verstrekt worden aan de 'anti-fraud organisation', de leden van deze organisatie of enig ander persoon aan wie de verstrekking op grond van de regelingen van de 'anti-fraud organisation' is toegestaan. Zoals hierboven aangegeven is op grond van de Serious Crime Act 2007 een Code of Practice opgesteld, waarin aanvullende regels zijn opgenomen waar publieke organisaties zich aan dienen te houden bij een verstrekking zoals bedoeld hierboven. In deze Code of Practice is Cifas expliciet benoemd als 'anti-fraud organisation'.
De juridische basis die is opgenomen in de Serious Crime Act 2007 schept voor de publieke organisaties een taak van algemeen belang of openbaar gezag als bedoeld in artikel 6 lid 1 sub e AVG op grond waarvan zij gegevens mogen verstrekken aan Cifas. In beginsel ziet het doel van Cifas voornamelijk op het bedrijfsbelang van organisaties teneinde het verlies dat zij leiden door fraude te verlagen. Zoals blijkt uit 3.1.3.1 kan een gerechtvaardigd bedrijfsbelang van organisaties, om fraude te bestrijden, samenvallen met een publiek belang. Dit kan bijvoorbeeld zijn wanneer organisaties gegevens delen ten behoeve van het bestrijden van fraude. De organisaties hebben dan een legitiem zakelijk belang om ervoor te zorgen dat klanten geen misbruik maken van hun diensten en de organisaties verlies leiden, terwijl anderzijds klanten van de organisatie, belastingbetalers en het grote publiek ook een legitiem belang hebben bij deze gegevensdeling doordat frauduleuze activiteiten worden ontmoedigd en fraude wordt opgespoord. Vanuit Cifas is de toegevoegde waarde van de gegevensdeling vooral geënt op de return on investment die de organisaties behalen uit hun deelname aan de databases van Cifas. Uit de 'Code of Practice for public authorities disclosing information to a specified anti-fraud organisation'[38] blijkt echter dat de verstrekking van gegevens vanuit publieke organisaties aan Cifas, dan wel deelnemers van Cifas meer een algemeen belang dient. Daarin wordt aangegeven dat overheidsinstanties een bijzondere verantwoordelijkheid hebben om de publieke middelen die zij beheren te beschermen en er zorg voor te dragen dat het geld van de belastingbetaler niet gebruikt wordt voor frauduleuze activiteiten. Gelet op deze verantwoordelijkheid is in de Serious Crime Act 2007 een taak van algemeen belang toebedeeld aan publieke organisaties op grond waarvan zij gegevens kunnen verstrekken aan de databases van Cifas, dan wel zelf deelnemer kunnen zijn aan de databases.

4.3.3 Verstrekken aan politie en/of andere opsporingsinstanties

Vanuit de 'National Fraud' database worden rechtstreeks gegevens verstrekt aan de NFIB, NCA en de politie. Op dagelijkse basis worden automatisch rapporten doorgestuurd aan deze opsporingsinstanties waarin nieuwe fraudezaken zijn opgenomen, ingevoerd in de database door de deelnemende partijen. Op basis van informatie

[38] Code of practice for public authorities disclosing information to a specified anti-fraud organisation under sections 68 to 72 of the Serious Crime Act 2007

van de website van Cifas en tevens door medewerkers van Cifas zelf aangeleverd, worden deze gegevens verstrekt om de opsporingsinstanties te helpen bij het voorkomen van fraude en andersoortige financiële criminaliteit. Cifas werkt met hen samen om de Britse economie en de maatschappij te beschermen tegen de schadelijke gevolgen van economische misdaden. Cifas heeft aangegeven dat de grondslag voor de verstrekking aan de opsporingsinstanties dezelfde grondslag is als gehanteerd voor de gegevensdeling in de databases zelf. Gegevens worden vanuit de databases verstrekt op grond van artikel 6 lid 1 sub f AVG, het gerechtvaardigd belang. De opheffing voor de verstrekking van strafrechtelijke gegevens kan gevonden worden in section 10, part 1 jo. Schedule 1, section 14 Data Protection Act 2018.

Cifas heeft daarnaast aangegeven dat de grondslag tevens gevonden kan worden in artikel 6 lid 1 sub e AVG, een taak van algemeen belang. Om een gerechtvaardigd beroep te kunnen doen op de grondslag 'taak van algemeen belang', dient deze taak bij wet aan de verantwoordelijke te zijn toebedeeld. Cifas heeft aangegeven dat zij, alsmede de deelnemende organisaties, deze taak hebben op grond van part 2 jo. chapter 2, section 8 Data Protection Act 2018:

'In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for:

a) the administration of justice,
b) the exercise of a function of either House of Parliament,
c) the exercise of a function conferred on a person by an enactment or rule of law,
d) the exercise of a function of the Crown, a Minister of the Crown or a government department, or
e) an activity that supports or promotes democratic engagement.'

De opheffing voor de verstrekking van strafrechtelijke gegevens kan ook hierbij gevonden worden in section 10, part 1 jo. Schedule 1, section 14 Data Protection Act 2018.

De politie, NFIB en NCA verwerken de ontvangende gegevens ter uitvoering van hun taken.

Concluderend
In Cifas bestaat op grond van de AVG en de Data Protection Act 2018 een juridische basis voor de gegevensverwerkingen die plaatsvinden in de databases van Cifas. Dit geldt zowel voor deelname van publieke – als private partijen aan Cifas. Ook voor de verstrekking van de gegevens aan de opsporingsinstanties bestaat een juridische basis volgens Cifas. Door de wijze waarop de uitzonderingsgronden in het VK gecreëerd zijn in de Data Protection Act 2018 om strafrechtelijke gegevens te mogen verwerken, is het niet nodig geweest voorafgaand aan de start van de gegevensdeling een vergunning aan te vragen bij de ICO.

Voor de publieke organisaties, die niet deelnemen aan de databases van Cifas, is het op grond van de Serious Crime Act 2007 ook juridisch mogelijk om gegevens te verstrekken aan de databases.

Naast het hebben van een juridische basis, moeten op grond van de AVG ook altijd waarborgen worden getroffen om de persoonlijke levenssfeer van de betrokkenen te beschermen. In 4.5 wordt nader ingegaan op de waarborgen die Cifas biedt om de impact op de persoonlijke levenssfeer te beperken.

4.4 Verantwoordelijkheidsverdeling

4.4.1 Verantwoordelijkheden Cifas

Cifas is de verwerkingsverantwoordelijke, zoals bedoeld in de AVG, voor de databases die Cifas aanbiedt en is met de deelnemende partijen gezamenlijk verwerkingsverantwoordelijk voor de zaken die worden ingevoerd in de databases van Cifas.

Zoals blijkt uit het juridisch kader, 2.6, is de verwerkingsverantwoordelijke degene die alleen of tezamen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Het begrip verwerkingsverantwoordelijke ziet niet noodzakelijk op één (rechts)persoon, maar kan betrekking hebben op meerdere deelnemers. Dat betekent dan ook dat sprake kan zijn van gezamenlijke verwerkingsverantwoordelijkheid. Ten aanzien van het begrip 'gezamenlijke verwerkingsverantwoordelijkheid' wordt meegegeven dat het bestaan van gezamenlijke verantwoordelijkheid niet noodzakelijkerwijs leidt tot een gelijkwaardige verantwoordelijkheid van de verschillende deelnemers aan de verwerking. Deze deelnemers kunnen in verschillende stadia en in verschillende mate bij de verwerking betrokken zijn.

Zoals hiervoor aangegeven is Cifas eigenstandig verwerkingsverantwoordelijke voor de databases van Cifas, maar bestaat gezamenlijke verwerkingsverantwoordelijkheid tussen de deelnemende partijen en Cifas ten aanzien van die zaken die worden ingevoerd in de databases van Cifas. Dat betekent dat voor de zaken die ingevoerd worden zowel Cifas als de deelnemers verantwoordelijk zijn om de vereisten die voortvloeien uit de AVG en de Data Protection Act 2018 na te leven.

Gelet op de informatie die is aangeleverd door Cifas en na bestudering van de stukken op de website van Cifas, kan opgemaakt worden dat Cifas, ten aanzien van de gezamenlijke verwerking, optreedt als een gemeenschappelijk verwerkingsverantwoordelijke; Cifas fungeert vaak als aanspreekpunt voor de ICO en treedt veelal ook op als aanspreekpunt voor vragen van betrokkenen, dan wel bieden zij ondersteuning als organisaties vragen krijgen van betrokkenen. Daarnaast hebben zij procedures en regelingen opgesteld waaraan de deelnemende partijen moeten voldoen om gebruik te mogen maken van de databases van Cifas. Cifas is ISO gecertificeerd[39] en de databases van Cifas zijn goedgekeurd voor publieke organisaties om gegevens aan te verstrekken.

Het beheer van de databases van Cifas is uitbesteed aan CGI IT UK Ltd ('CGI'). Zij treden op als verwerker voor de databases van Cifas. Cifas hecht er veel waarde aan dat de gegevens binnen de EU opgeslagen staan en geen doorgifte buiten de EU plaatsvindt. Vanuit Cifas is aangegeven dat CGI, alsmede de servers van CGI zijn gevestigd in het VK. Dat betekent dat thans geen doorgifte buiten de EU plaatsvindt. Cifas is zich bewust van de mogelijke veranderingen die optreden met betrekking tot de doorgifte zodra het VK de EU verlaat en tracht hier zoveel mogelijk rekening mee te houden.

4.4.2 Verantwoordelijkheden deelnemende partijen

Zoals hiervoor aangegeven bestaat volgens Cifas gezamenlijke verwerkingsverantwoordelijkheid tussen de deelnemende partijen en Cifas ten aanzien van die zaken die worden ingevoerd in de databases van Cifas. Cifas en de deelnemers zijn gezamenlijk verantwoordelijk voor de kwaliteit van de gegevens, een adequate bescherming van de gegevens en rechtmatig gebruik van de gegevens die in de databases staan opgenomen. Voor deelnemende organisaties betekent dit in elk geval dat zij verantwoordelijk zijn voor de juistheid van de gegevens die zij toevoegen aan de databases en daarnaast ook dat zij verantwoordelijk zijn dat rechtmatig gebruik wordt gemaakt van de gegevens die door een zoekopdracht worden geretourneerd.

[39] ISO 27001 is een standaard die gaat over informatiebeveiliging. In deze standaard staat hoe je procesmatig met het beveiligen van informatie kan omgaan, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen een organisatie zeker te stellen.

4.5 Zorgvuldige gegevensverwerking

Cifas heeft acht principes geïntroduceerd en een handboek opgesteld waarin de regels staan opgenomen waaraan deelnemende partijen moeten voldoen op het gebied van de bescherming van persoonsgegevens. De principes waaraan organisaties moeten voldoen zijn openbaar te raadplegen. Het handboek is echter niet openbaar, omdat dit relevante informatie voor kwaadwillenden kan bevatten over de werking van de systemen van Cifas en het gestelde beveiligingsniveau.[40] Om deelnemer te kunnen worden van Cifas, moet een deelnemer akkoord gaan met en werken volgens deze opgestelde principes en het handboek waarin de richtlijnen zijn opgenomen. Deze principes en richtlijnen beschrijven onder meer welke waarborgen getroffen moeten worden om de gegevens in de databases te beschermen, zorgen ervoor dat organisaties uitsluitend zaken toevoegen waarvoor voldoende bewijslast aanwezig is en dat organisaties transparant zijn over de verwerkingen die plaatsvinden. Is een deelnemende organisatie gevestigd buiten de EU, dan zijn deze organisaties zelf verplicht te controleren of zij passende waarborgen hebben getroffen voor de doorgifte buiten de EU. In het handboek zijn concrete handvatten opgenomen die de deelnemende organisaties helpen om de principes op juiste wijze te waarborgen en na te leven. Het handboek geeft dus een nadere invulling aan de opgestelde principes, zo is bijvoorbeeld het template 'fair processing notice' opgenomen in het handboek en zijn voorbeelden gegeven die de deelnemende organisaties meer aanknopingspunten geeft om te controleren of voldaan wordt aan de bewijslast. De maatregelen die opgenomen zijn in het handboek zijn onderverdeeld in verplichte maatregelen, zeer aanbevolen maatregelen en maatregelen waarbij organisaties ruimte hebben om te bepalen of zij deze doorvoeren.

De principes waaraan deelnemende organisaties zich dienen te houden, zijn hierna uiteengezet.

Wederkerigheid

De databases functioneren bijna volledig op basis van de input van de deelnemers. Naast de input van de deelnemers leveren ook publieke partijen, niet zijnde deelnemers, gegevens aan de databases van Cifas. Om als deelnemer voordeel te behalen uit de door andere deelnemers geregistreerde zaken, dien je als deelnemer ook zelf bij te dragen aan de registratie van fraudezaken.

Doelbinding (legitieme redenen om te zoeken)

Gegevens uit de databases mogen uitsluitend worden gebruikt met het oog op het voorkomen, opsporen en onderzoeken van fraude en financiële criminaliteit.

Transparantie

Betrokkenen hebben het recht geïnformeerd te worden over de wijze waarop de op hen betreffende gegevens worden gebruikt en hoe op basis van deze gegevens beslissingen zijn genomen of genomen kunnen worden waaraan voor hen gevolgen zijn verbonden. Om betrokkenen te informeren dient gebruik gemaakt te worden van de 'fair processing notice' die door Cifas aan de deelnemende organisaties is verstrekt. Er bestaat een verschil ten aanzien van de wijze waarop betrokkenen geïnformeerd dienen te worden met betrekking tot opnamen in de National Fraud database en de Internal Fraud database. Voor meer informatie over de wijze waarop betrokkenen geïnformeerd dienen te worden, wordt verwezen naar 4.2.1 'informeren betrokkenen'.

[40] Het handboek is, onder voorwaarde van ondertekening van een 'non-disclosure agreement', verstrekt aan de onderzoekers. Dat betekent dat de onderzoekers het handboek hebben ingezien.

Rechtmatigheid (zaken toevoegen en zoeken)

Deelnemende organisaties mogen uitsluitend gegevens aan de databases toevoegen en de databases uitsluitend raadplegen nadat de betrokkenen zijn geïnformeerd – middels een 'fair processing notice' – over de wijze waarop hun gegevens worden gebruikt (zie 4.2.1.1).

Rechtmatigheid (bewijslast)

Deelnemers die zaken toevoegen aan de databases van Cifas dienen deze te kunnen onderbouwen met bewijs. Hierbij dienen de volgende 'vier pijlers' in acht te worden genomen:

1. Er zijn redelijke gronden om aan te nemen dat fraude is gepleegd, dan wel dat gepoogd is fraude te plegen;
2. Er moet voldoende bewijsmateriaal zijn om het feit te onderbouwen. Dit bewijsmateriaal moet zodanig zijn dat voldoende grond bestaat om aangifte te doen bij de politie;
3. Het strafbare feit moet identificeerbaar zijn en vallen onder één van de vormen van fraude die onderdeel is van de databases (zie 4.1);

National Fraud database:

4. Voordat de zaak wordt ingediend, moet de deelnemende organisatie het aangevraagde product hebben afgewezen, de aanvraag hebben ingetrokken of beëindigd wegens de gepoogde of gepleegde fraude, tenzij de deelnemer verplicht is het product te leveren of de aanvrager het volledige voordeel reeds heeft ontvangen.

Internal Fraud database:

4. Voordat de zaak wordt ingediend, moet de deelnemende organisatie de sollicitant hebben afgewezen, de dienstbetrekking hebben opgezegd of fraude hebben geïdentificeerd, dan wel ander relevant gedrag nadat de werknemer de werkgever heeft verlaten.

Proportionaliteit

Deelnemers dienen bij het raadplegen van informatie uit de databases het proportionaliteitsbeginsel in acht te nemen; wat inhoudt dat de deelnemende organisatie bij een match altijd een afweging dient te maken. In deze afweging dient meegenomen te worden waar de aanvraag van de betrokkene op ziet en wat de risicobereidheid is van de organisatie. De deelnemende organisatie moet naar aanleiding van een match altijd onderzoek uitvoeren.

Aanvulling National Fraud database:
Deelnemende organisaties dienen bij het toevoegen van zaken – voor bescherming van deze partijen – tevens de slachtoffers te vermelden. Deze partijen dienen duidelijk te worden onderscheiden van de betrokkenen in de zaak.

Juistheid

De deelnemers dienen ervoor zorg te dragen dat de gegevens die zij indienen in de databases juist zijn. Zaken dienen binnen één dag, nadat is voldaan aan de bewijslast, te zijn toegevoegd aan de betreffende database.

Integriteit

De deelnemende partijen dienen over adequate technische en organisatorische maatregelen te beschikken teneinde de gegevens die zij verkrijgen vanuit Cifas passend te beveiligen. Toegang tot de databases van Cifas dient voorbehouden te zijn aan de werknemers van de deelnemende organisaties voor wie dat noodzakelijk is voor hun taakuitoefening.

Dataminimalisatie

Deelnemers moeten over het bewijsmateriaal beschikken ter ondersteuning van een zaak die zij hebben ingediend in de databases. Dit betekent echter niet zij dat gegevens voor onbepaalde tijd mogen bewaren. Zodra het doel van de verwerking is bereikt, dienen de gegevens veilig en permanent verwijderd te worden.

4.6 Rol Information Commissioner's Office

De ICO is in het VK de onafhankelijke toezichthouder die onder meer toezicht houdt op de naleving van de AVG en de Data Protection Act 2018. De ICO is dan ook bevoegd toezicht te houden op de naleving van de wetgeving op het gebied van de bescherming van persoonsgegevens door Cifas.

Vanuit Cifas is aangegeven dat de relatie met de ICO zeer goed is. De ICO heeft niet formeel goedkeuring gegeven aan de databases van Cifas, maar de ICO is goed op de hoogte van de (werking van deze) databases en is ook betrokken geweest bij de inrichting van de hiervan. De ICO heeft Cifas begeleid bij de inrichting van de databases en was, aldus Cifas, deelnemer van de werkgroep die zich bezighield met de oprichting van de databases.

Op dit moment wordt halfjaarlijks overleg gevoerd met de ICO. Cifas kan de ICO middels deze overleggen op de hoogte houden van eventuele nieuwe ontwikkelingen die zij voornemens zijn door te voeren. Daarnaast kan de ICO in deze overleggen Cifas bijsturen waar nodig. Door de goede relatie tussen de ICO en Cifas kan ook snel geschakeld worden wanneer klachten tegen Cifas worden ingediend. De ICO brengt Cifas hiervan op de hoogte en Cifas pakt deze klachten voorts adequaat op.

Vanuit de ICO is daarbij benadrukt dat zij wel advies gegeven hebben bij de oprichting ten aanzien van relevante aspecten die spelen bij de bescherming van persoonsgegevens, maar dat zij geen formele goedkeuring gegeven hebben aan de databases van Cifas, dan wel anderszins betrokken geweest zijn bij de oprichting. De ICO heeft wel, zoals ook aangegeven door Cifas, contact met Cifas over eventuele nieuwe ontwikkelingen die Cifas wenst door te voeren zodat de ICO hen van advies kan voorzien. Graag wordt wel meegegeven dat dit contact bestaat met alle erkende 'anti-fraud organisations' binnen het VK en dat de ICO dan ook geen speciale rol heeft met de Cifas boven deze andere organisaties. In het VK zijn namelijk meerdere instanties erkend als zijnde 'anti-fraud organisations', zoals Callcredit Information Group Limited, Equifax Limited, Experian Limited, Insurance Fraud Investigators Group en Synectics Solutions Limited. In totaal zijn 11 organisaties in het VK erkend als 'anti-fraud organisation'.[41] Deze organisaties houden zich, net als Cifas, bezig met het bestrijden van fraude. Enkele van deze organisaties werken ook met een systeem waar deelnemers gegevens met elkaar kunnen uitwisselen ten behoeve van het bestrijden van fraude. Cifas kenmerkt zich wel als 'anti-fraud organisation' door branche overstijgende (geen beperkingen) gegevensdeling tussen publieke en private partijen mogelijk te maken over allerhande fraudezaken (zie 3.1).

[41] Zie voor alle 'anti-fraud organisations' de Code of practice for public authorities disclosing information to a specified anti-fraud organisation under sections 68 to 72 of the Serious Crime Act 2007.

Nota bene:
Door de wijze waarop de uitzonderingsgronden in het VK gecreëerd zijn in de Data Protection Act 2018 om strafrechtelijke gegevens te verwerken, heeft Cifas, dan wel de organisaties die zijn gestart met de gegevensdeling, **geen** vergunning hoeven aanvragen bij de ICO om te mogen starten met de gegevensdeling. Dat betekent dan ook dat de ICO geen vergunning heeft verleend voor de databases van Cifas en dan ook niet voorafgaand een toetsing heeft hoeven uitvoeren ten aanzien van de werking van de databases en of deze in overeenstemming met de geldende wetgeving zijn ingericht.

5 Toepasbaarheid fraudepreventiesysteem Cifas in Nederland

Nadat in de voorgaande hoofdstukken het Nederlands juridische kader met betrekking tot het cross-sectoraal delen van gegevens uiteen is gezet en een beschrijving van Cifas, het fraudepreventiesysteem in het VK, is gegeven, wordt in dit hoofdstuk ingegaan op de toepasbaarheid van Cifas in Nederland. Na uitwerking van de twee vorige hoofdstukken, kan geconcludeerd worden dat het fraudepreventiesysteem in het VK, zoals dat nu wordt gebruikt in het VK, *niet* één-op-één overgenomen kan worden in Nederland. Hieronder wordt uiteengezet waarom het systeem niet overgenomen kan worden in Nederland.

5.1 Toepasbaarheid Cifas in Nederland

5.1.1 Juridische basis

De belangrijkste reden waarom het fraudepreventiesysteem zoals dat gebruikt wordt in het VK niet overgenomen kan worden in Nederland, is omdat de uitzonderingsgronden voor het verwerken van strafrechtelijke gegevens in Nederland en het VK verschillend zijn ingericht. Zoals blijkt uit het juridisch kader, uitgewerkt in H2, is zowel in Nederland als het VK de AVG van toepassing wanneer cross-sectoraal persoonsgegevens gedeeld worden ten behoeve van het bestrijden van fraude.

De AVG heeft rechtstreekse werking in de hele Europese Unie. De AVG is dan ook gelijk voor alle lidstaten van de Europese Unie. Hoewel de AVG rechtstreekse werking heeft, laat de AVG de lidstaten op bepaalde punten wel ruimte om specifieke bepalingen op te nemen of uitzonderingen te maken. In Nederland zijn deze specifieke bepalingen en uitzonderingen vastgelegd in de UAVG. In het VK zijn deze uitzonderingen opgenomen in de Data Protection Act 2018. De AVG dient dan ook altijd in samenhang gelezen te worden met deze nationale uitvoeringswetten.

Bij het cross-sectoraal delen van persoonsgegevens tussen organisaties worden strafrechtelijke persoonsgegevens uitgewisseld. Op grond van de AVG mogen strafrechtelijke persoonsgegevens uitsluitend worden verwerkt wanneer daarvoor een uitzondering in de AVG en nationale uitvoeringswetten kan worden gevonden. De lidstaten hebben op grond van de AVG ruimte gekregen om in de nationale uitvoeringswet bepalingen op te nemen waaronder strafrechtelijke persoonsgegevens verwerkt mogen worden.

In het VK is in de Data Protection Act 2018 specifiek een bepaling opgenomen op basis waarvan het voor een 'anti-fraud organisation', als Cifas, en zijn deelnemers mogelijk is om strafrechtelijke gegevens te verwerken om fraude te bestrijden. In Nederland zijn de uitzonderingsgronden voor het verwerken van strafrechtelijke persoonsgegevens anders ingeregeld. Op grond van de UAVG is het mogelijk om cross-sectoraal gegevens te delen ten behoeve van het bestrijden van fraude indien de organisaties, die mogelijk gegevens willen gaan delen, daartoe een vergunning aanvragen bij de Autoriteit Persoonsgegevens. Om cross-sectorale gegevensdeling in Nederland mogelijk te maken dient dus een vergunningstraject doorlopen te worden waarbij de Autoriteit Persoonsgegevens voorafgaand aan de verwerking toetst of deze in lijn is met de AVG. Of een dergelijke vergunning verleend wordt, hangt af van de concrete inrichting van het systeem en de onderbouwing van de noodzaak, proportionaliteit en subsidiariteit.

Door de wijze waarop de uitzonderingsgronden in het VK zijn ingericht, hebben de partijen daar voorafgaand aan de verwerking géén vergunning hoeven aanvragen bij de ICO en hebben zij met elkaar en met de beheerder, Cifas, de gegevensdeling zelfstandig in kunnen richten. De ICO heeft dan ook geen voorafgaande toetsing uitgevoerd ten aanzien van de rechtmatigheid van de databases van Cifas.

Ondanks dat in het VK geen vergunning hoeft te worden aangevraagd en dan ook geen voorafgaande toetsing heeft plaatsgevonden is de ICO wel bevoegd om – op eigen initiatief of naar aanleiding van klachten van betrokkenen – onderzoek uit te voeren naar de databases van Cifas. Op dit moment heeft een dergelijk onderzoek nog niet plaatsgevonden en zijn dan ook geen verdere beleidsstukken beschikbaar waarin meer informatie is opgenomen over de rechtmatigheid van de databases van Cifas.

Nu door de toezichthouder geen voorafgaande toetsing van de databases van Cifas aan de AVG heeft plaatsgevonden en voorts ook nog geen onderzoek vanuit de toezichthouder heeft plaatsgevonden, is geen informatie beschikbaar waaruit blijkt dat de databases van Cifas volledig zijn ingericht in overeenstemming met de AVG en dezelfde inrichting dan ook overgenomen kan worden in Nederland. In Nederland kan cross-sectorale gegevensdeling op grond van de AVG en UAVG uitsluitend worden ingericht wanneer daartoe een vergunning bij de Autoriteit Persoonsgegevens wordt aangevraagd. In Nederland zal eerst een voorafgaande toetsing moeten worden uitgevoerd door de Autoriteit Persoonsgegevens of de cross-sectorale gegevensdeling in overeenstemming is met de AVG en dan ook plaats mag vinden in Nederland. Dit in tegenstelling tot het VK waar gestart mocht worden met de verwerking zonder dat daartoe een vergunning is aangevraagd en waar de partijen dan ook zelf de waarborgen hebben ingericht om in overeenstemming met de AVG te handelen.

5.1.2 Deelname publieke organisaties

Naast private partijen nemen aan de databases van Cifas ook publieke partijen deel aan de samenwerking. Daarnaast is het bij Cifas ook zo dat enkele publieke partijen, die zelf geen deelnemer zijn van de databases, ook gegevens verstrekken aan Cifas om zo bij te dragen aan de bestrijding van fraude. In het VK is in de Serious Crime Act 2007 en de op basis daarvan opgestelde Code of Practice for Public Authorities[42], een juridische basis neergelegd voor publieke partijen om als deelnemer gegevens te verstrekken aan een 'anti fraud-organisation' en de andere deelnemende organisaties. Daarnaast is het op grond van deze juridische basis mogelijk om als publieke partij gegevens te verstrekken aan een 'anti-fraud organisation' en zijn deelnemers zonder dat de publieke partij, die de gegevens verstrekt, zelf deelnemer is van de 'anti-fraud organisation'. Voor publieke partijen bestaat dus een wettelijke basis in het VK op grond waarvan zij zelf deel mogen nemen aan dit samenwerkingsverband ten behoeve van het bestrijden van fraude, dan wel dat zij gegevens mogen verstrekken aan dit samenwerkingsverband zonder dat zij zelf deelnemer zijn.

In Nederland kennen wij een dergelijke algemene juridische basis niet waardoor niet zonder meer gezegd kan worden dat in Nederland ook de mogelijkheid bestaat dat publieke partijen mogen deelnemen aan een eventuele cross-sectorale gegevensdeling. Per publieke partij dient beoordeeld te worden of zij een grondslag hebben, als bedoeld in art. 6 AVG, om deel te kunnen nemen aan het samenwerkingsverband. De grondslag op basis waarvan publieke partijen in dit kader gegevens mogen verwerken, zal vaak gevonden worden in de taak van algemeen belang. Indien cross-sectoraal gegevens gedeeld gaan worden en een publieke partij daar deelnemer van wil zijn, dient voorafgaand per partij beoordeeld te worden of bij wet een taak van algemeen belang of openbaar gezag aan deze partij is toebedeeld op grond waarvan deelgenomen kan worden aan de cross-sectorale gegevensdeling. Ook dient beoordeeld te worden of deze taak zo ver reikt dat aan alle organisaties die deelnemen aan de cross-sectorale gegevensdeling gegevens verstrekt mogen worden en de publieke partij ook gegevens mag ontvangen van al deze organisaties.

Het is dus niet gezegd dat het in Nederland niet mogelijk is dat publieke partijen ook deelnemen aan de gegevensdeling, maar per publieke partij dient beoordeeld te worden of het voor deze partij mogelijk is deel te nemen aan eventuele cross-sectorale gegevensdeling. Voorafgaand kan dus niet gezegd worden dat het voor alle publieke partijen mogelijk is deel te nemen. In het VK is deze algemene juridische basis wel op

[42] Code of practice for public authorities disclosing information to a specified anti-fraud organization under sections 68 to 72 of the Serious Crime Act 2007

dusdanige wijze neergelegd dat publieke partijen in staat worden gesteld tevens deel te nemen aan de gegevensdeling, dan wel gegevens te verstrekken zonder dat zij deelnemer zijn van de gegevensdeling.

Wet gegevensverwerking door samenwerkingsverbanden
Indien de WGS wordt aangenomen en in werking treedt, kan deze wet mogelijk een basis bieden om een privaat- publiekrechtelijk samenwerkingsverband op te richten. In dit samenwerkingsverband kunnen zowel private als publieke partijen deelnemen. Er dient wel te allen tijde een publieke partij onderdeel te zijn van het samenwerkingsverband. Bij AMvB dient te worden uitgewerkt welke partijen deelnemen aan het verband, ten behoeve van welk doel en welke waarborgen worden getroffen. Indien deze wet wordt aangenomen, kan dit de basis voor het oprichten van een privaat- publiek samenwerkingsverband vereenvoudigen. Een publiek-privaatrechtelijk samenwerkingsverband dient wel een algemeen belang te dienen en kan dus niet opgericht worden vanuit het perspectief van de private partijen teneinde het bedrijfsbelang te beschermen en zoals bij Cifas de samenwerking in beginsel is opgericht. De WGS is op het moment nog in voorbereiding. Het is dan ook nog afwachten óf en wanneer de WGS wordt aangenomen en wat de definitieve wettekst gaat worden.

5.2 Concluderend

Uit het voorgaande blijkt dat het fraudepreventiesysteem in het VK niet één-op-één overgenomen kan worden in Nederland. Hoewel in het VK een wettelijke basis bestaat en de ICO (vooralsnog) geen aanleiding ziet tot handhaving, wil dat niet zeggen dat de wijze waarop Cifas is ingericht binnen de Nederlandse context ook automatisch rechtmatig is en tot een succesvolle vergunningsaanvraag leidt. Zoals uitgewerkt in H1, juridisch kader, is de AVG een Europese verordening die rechtstreeks van toepassing is; dat betekent dat de AVG voor alle lidstaten van de Europese Unie gelijk is. De AVG heeft de lidstaten echter wel op een bepaald aantal punten ruimte gelaten om specifieke bepalingen op te nemen of uitzonderingen te maken. Zo zijn de lidstaten bijvoorbeeld vrij geweest om in hun nationale uitvoeringswetten bepalingen op te nemen waaronder bijzondere en strafrechtelijke persoonsgegevens verwerkt mogen worden. Politieke en maatschappelijke overwegingen die spelen in afzonderlijke lidstaten zullen bij de formulering van deze uitzonderingsgronden van belang zijn geweest.

De AVG bevat daarnaast geen specifieke set aan regels, maar bevat veelal principes waaraan moet worden voldaan wanneer gegevens verwerkt worden. Deze principes zijn geformuleerd als open normen en kunnen daarom verschillend worden ingevuld. Het is aan de toezichthouder van een lidstaat om te bepalen of op juiste wijze invulling is gegeven aan deze principes en dan ook voldoende waarborgen zijn getroffen om de persoonlijke levenssfeer te beschermen. Vanuit de European Data Protection Board (EDPB), waarin alle toezichthouders zijn verenigd, zijn richtlijnen gegeven, dan wel worden richtlijnen gegeven hoe deze principes ingevuld dienen te worden, maar er blijft een bepaalde interpretatieruimte voor lidstaten bestaan. Het kan dan ook zijn dat het VK bepaalde waarborgen als afdoende beschouwd, terwijl de Nederlandse toezichthouder daar anders tegenaan kijkt. Of de wijze waarop Cifas thans is ingericht ook in Nederland rechtmatig is moet zelfstandig worden beoordeeld. Hierbij is de specifieke Nederlandse situatie maatgevend, niet de situatie in het VK. Nu vooralsnog in Nederland maar zeer beperkt wordt gewerkt met sectorale gegevensdeling en vooralsnog geen initiatieven zijn tot omvangrijke cross-sectorale gegevensdelingen, zal het moeilijk te onderbouwen zijn dat een cross-sectorale gegevensdeling op de schaal van Cifas noodzakelijk en proportioneel is en voldoet aan de eis van subsidiariteit. Naast de vraag of er sprake is van een noodzakelijke en proportionele oplossing moet ook gekeken worden naar de waarborgen. Cifas heeft een stelsel van waarborgen dat vastgelegd is in een Handboek. Of deze maatregelen toereikend zijn en ook daadwerkelijk worden nageleefd in de praktijk, is geen onderdeel geweest van ons onderzoek en dan ook niet door ons onderzocht. Hoewel het feit dat ICO niet heeft gehandhaafd tegen Cifas een indicatie is zijn dat de waarborgen afdoende zijn, kan niet gezegd worden dat het uitblijven van handhaving rechtmatigheid impliceert.

Dat Cifas niet één-op-één overgenomen kan worden in Nederland, betekent echter niet dat in Nederland geen juridische mogelijkheden bestaan om tussen private partijen cross-sectoraal gegevens te delen om fraude te

bestrijden. Hieronder wordt ingegaan op de mogelijkheden die in Nederland bestaan op welke wijze cross-sectorale gegevensdeling wel kan plaatsvinden. Hierbij wordt meegegeven dat onderstaande paragrafen opeenvolgend gelezen dienen te worden.

5.3 Mogelijkheden inrichting cross-sectorale gegevensdeling in Nederland

5.3.1 Vergunningaanvraag onder AVG en UAVG

In hoofdstuk 2, juridisch kader, en hoofdstuk 3, cross-sectorale gegevensdeling ten behoeve van fraudebestrijding in het Nederlandse rechtsbestel, is uitgewerkt wat de juridische mogelijkheden zijn voor private partijen om cross-sectoraal gegevens te delen in Nederland om fraude te bestrijden. Daaruit is gebleken dat er mogelijkheden bestaan onder de AVG, in samenhang met de UAVG om cross-sectorale gegevensdeling in te richten. De UAVG vereist wel dat voordat gestart kan worden met de cross-sectorale gegevensdeling door de organisaties die gegevens met elkaar willen gaan delen een vergunning aangevraagd dient te worden bij de Autoriteit Persoonsgegevens. De organisaties, mogelijk met een beherende partij, dienen gezamenlijk een vergunningstraject in te gaan. Onderdeel van deze vergunningsaanvraag is dat de organisaties eerst gezamenlijk een DPIA uitvoeren waarin de risico's van de cross-sectorale gegevensdeling voor de betrokkenen in kaart worden gebracht, alsmede de maatregelen die genomen worden om deze risico's te verkleinen. Daarnaast dienen de organisaties ook gezamenlijk een privacy protocol op te stellen over de cross-sectorale gegevensdeling. Afhankelijk van de uitkomsten van de DPIA, kan vastgesteld worden hoe het vergunningstraject verder moet worden vervolgd. Zie voor meer informatie over de wijze waarop de gegevensdeling ingericht kan worden hoofdstuk 3 en de wijze waarop een vergunningsaanvraag dient plaats te vinden bijlage I - Aanvraag vergunning UAVG.

Onder de huidige wetgeving is het dus mogelijk om cross-sectorale gegevensdeling tussen private partijen in te richten, maar daartoe dient wel eerst door de organisaties, die gezamenlijk gegevens willen gaan delen, een vergunningstraject in te worden gegaan. Voorafgaand kan dan ook niet gezegd worden dat de cross-sectorale gegevensdeling daadwerkelijk kan gaan plaatsvinden. Dit is afhankelijk van de uitkomsten van het vergunningstraject.

5.3.2 Oprichting privaat- publiekrechtelijk samenwerkingsverband op basis van de WGS

Op het moment wordt nog gewerkt aan het conceptwetsvoorstel WGS. Indien deze wet wordt aangenomen en in werking treedt, kan op basis van deze wet ook gekozen worden om een privaat- publiekrechtelijk samenwerkingsverband in te richten ten behoeve van het algemeen belang om fraude te bestrijden. Bij AMvB dienen nadere regels gesteld te worden welke organisaties, privaat en publiek, deelnemen aan de samenwerking, ten behoeve van welk doel deze samenwerking plaatsvindt en onder welke voorwaarden en welke waarborgen getroffen worden bij deze samenwerking. Indien de gegevensdeling wordt ingericht op basis van de WGS krijgt de samenwerking mogelijk een andere insteek dan bedoeld onder 5.3.1 en zoals bij Cifas in het VK het geval is. Een vereiste bij de inrichting van een samenwerkingsverband onder de WGS is dat het verband een algemeen belang moet dienen en ziet dan ook minder op het bedrijfsbelang van de private partijen. Dit betekent echter niet dat de samenwerking t.b.v. het algemeen belang ook met zich mee kan brengen dat de bedrijfsbelangen van de organisaties beschermd worden, maar de initiële inrichting van een samwerkingsverband onder de WGS is anders van aard dan geschetst bij de inrichting in 5.3.1. Bij de inrichting genoemd onder 5.3.1 zal de doelstelling van de organisaties om gegevens te delen er in beginsel op zien om hun bedrijfsbelangen te beschermen. Ook hierbij kan het zo zijn dat het de bescherming van de bedrijfsbelangen van de organisaties tevens met zich meebrengt dat een algemeen belang wordt gediend.
De initiële inrichtingen van een samenwerkingsverband onder de WGS en zoals bedoeld onder 5.3.1 zijn echter verschillend van aard. Nu de WGS nog in voorbereiding is en de definitieve wettekst nog niet gereed is, is het nog afwachten hoe dit scenario in de praktijk exact kan worden ingericht.

5.3.3 Wetswijziging UAVG

Indien op termijn zou blijken dat bovenstaande juridische mogelijkheden verbetering behoeven en er een politieke en maatschappelijke wens bestaat deze verbeteringen door te voeren, zou gedacht kunnen worden een wijziging te creëren in de UAVG die een zelfstandige wettelijke basis biedt voor cross-sectorale gegevensdeling. Hierbij zijn twee verschillende wetswijzigingen mogelijk.

- Een mogelijkheid is om in aanvulling op artikel 33 lid 4 sub c en lid 5 UAVG een specifiek kader te creëren dat van toepassing is wanneer een vergunning aangevraagd wordt teneinde (cross-sectoraal) gegevens te gaan delen ten behoeve van fraudebestrijding. In dit specifieke kader dient nader uitgewerkt te worden aan welke randvoorwaarden en waarborgen een vergunningaanvraag dient te voldaan wanneer organisaties (cross-sectoraal) gegevens willen gaan delen ten behoeve van fraudebestrijding. Deze randvoorwaarden en waarborgen geven organisaties de ruimte en geeft hen meer concrete handvatten om de gegevensdeling in te richten. De waarborgen die in dit specifieke kader zijn opgenomen zorgen ervoor dat, net als bij publiekrechtelijke samenwerkingsverbanden waarbij veelal een wet aan ten grondslag ligt, bij de gegevensdeling meer waarborgen worden getroffen om te spreken van een zorgvuldige verwerking. Het kader dwingt organisaties ertoe om deze waarborgen ook daadwerkelijk in de praktijk te verankeren. De Autoriteit Persoonsgegevens behoudt uiteraard de mogelijkheid van voorafgaande toetsing en dient te oordelen over de vergunningaanvraag. Doordat in dit specifieke kader democratisch geborgd is wat de randvoorwaarden zijn voor de inrichting van de gegevensdeling en de waarborgen waaronder deze gegevensdeling dient te worden ingericht, is het voor organisaties duidelijker waaraan zij moeten voldoen om een dergelijke vergunning te kunnen verkrijgen.
- Daarnaast kan overwogen worden om de UAVG te wijzigen en de uitzonderingsgrond, zoals die nu is opgenomen in de Data Protection Act 2018, over te nemen in de UAVG. Op basis van deze uitzonderingsgrond is het mogelijk voor organisaties en een eventuele beherende partij om strafrechtelijke gegevens te verwerken om fraude te bestrijden zonder dat daarvoor een vergunning wordt aangevraagd. Net als in het VK wordt het aanbevolen om bij besluit of in een nadere regeling uit te werken welke organisaties deze gegevens mogen verwerken, zodat duidelijk is begrensd welke organisaties ten behoeve van welk doel strafrechtelijke gegevens mogen verwerken.
  De overname van deze bepaling in de Nederlandse UAVG, betekent dat een nieuwe uitzonderingsgrond wordt gecreëerd om strafrechtelijke gegevens te verwerken zonder dat een vergunning nodig is. De toevoeging van deze uitzonderingsgrond laat uiteraard onverlet dat de Autoriteit Persoonsgegevens te allen tijde de bevoegdheid behoudt om, zelfstandig of op verzoek van betrokkenen, toezicht te houden. De Autoriteit Persoonsgegevens kan dan ook onderzoek doen naar de cross-sectorale gegevensdeling tussen private partijen en oordelen dat de gegevensdeling niet in overeenstemming is met de AVG en op basis van de AVG bevoegdheden inzetten om deze gegevensdeling stop te zetten.

Bijlage I – Aanvraag vergunning UAVG

Vergunningsaanvraag

Voordat door de organisaties op basis van artikel 33 lid 4 sub c en lid 5 UAVG een aanvraag tot een vergunning kan worden gedaan bij de Autoriteit Persoonsgegevens, moet op grond van art. 35 AVG eerst een gegevensbeschermingseffectbeoordeling (ook wel *Data Protection Impact Assessment 'DPIA'* genaamd) te worden uitgevoerd.

Naast de DPIA, moeten de indieners bij de vergunningaanvraag ook een privacy protocol overleggen. In dit protocol is omschreven hoe de persoonsgegevens verwerkt worden en hoe de voorgenomen gegevensdeling voldoet aan de eisen uit de AVG.

DPIA

De AVG stelt het vereiste om een DPIA uit te voeren bij verwerkingen die waarschijnlijk een groot risico inhouden voor de rechten en vrijheden van de betrokkene(n). Hiervan is onder meer sprake wanneer het voornemen bestaat om op grote schaal strafrechtelijke gegevens te verwerken. Ook wanneer het voornemen bestaat om een zwarte lijst bij te houden en te delen, dient een DPIA te worden uitgevoerd. Gelet hierop, kan gezegd worden dat bij het cross-sectoraal delen van gegevens tussen private partijen ten behoeve van het bestrijden van fraude, sprake is van een hoog risico verwerking en een DPIA uitgevoerd dient te worden.
Een DPIA dient een systematische beschrijving te bevatten van de voorgenomen gegevensverwerking, waarbij ook ingegaan moet worden op de noodzaak en de evenredigheid van de gegevensverwerking. Ook dienen eventuele privacyrisico's voor de betrokkenen in kaart te worden gebracht en de maatregelen die worden genomen om die risico's te beperken.

Indien uit de DPIA blijkt dat geen hoog risico resteert voor de persoonlijke levenssfeer van de betrokkenen of dat met maatregelen het risico voor de betrokkenen beperkt kan worden, dan kan een vergunning, de ontheffing voor het verwerken van strafrechtelijke gegevens, worden aangevraagd middels het aanvraagformulier op de website van de Autoriteit Persoonsgegevens 'vergunning zonder voorafgaande raadpleging'.

Indien uit een DPIA blijkt dat de voorgenomen gegevensverwerking een hoog risico oplevert voor de persoonlijke levenssfeer van de betrokkenen en het niet mogelijk is (voldoende) maatregelen te treffen om dit risico te verkleinen, dient op basis van artikel 36 AVG de Autoriteit Persoonsgegevens geraadpleegd te worden over de voorgenomen gegevensverwerking. Dit proces dient dan eerst doorlopen te worden voordat de vergunningsaanvraag voor het verwerken van strafrechtelijke gegevens gedaan kan worden.

Voorafgaande raadpleging Autoriteit Persoonsgegevens

Bij een voorafgaande raadpleging geeft de Autoriteit Persoonsgegevens advies hoe de risico's van een voorgenomen verwerking beperkt kunnen worden. Op grond van artikel 36 AVG dient bij een voorafgaande raadpleging de volgende informatie te worden verstrekt aan de Autoriteit Persoonsgegevens:

- De doelen en middelen van de voorgenomen gegevensverwerking;
- De maatregelen en waarborgen die worden getroffen voor de naleving van de AVG;
- De uitkomsten van de DPIA;
- De respectievelijke verantwoordelijkheden, van de verschillende organisaties; of sprake is van gezamenlijke verwerkingsverantwoordelijken en verwerkers.

Daarnaast moet, indien van toepassing, de volgende informatie worden verstrekt:

- De contactgegevens van de functionaris van de gegevensbescherming;
- Alle andere informatie waar de Autoriteit Persoonsgegevens om verzoekt.

Nadat de voorafgaande raadpleging is doorlopen, kan – met inachtneming met de uitkomsten van de voorafgaande raadpleging – verder worden gegaan met het vergunningstraject. Indien een voorafgaande raadpleging heeft plaatsgevonden, dient via het aanvraagformulier 'vergunning na voorafgaande raadpleging' een vergunning te worden aangevraagd.

Ook wanneer een voorafgaande raadpleging heeft plaatsgevonden en voorts een vergunning wordt aangevraagd, dient bij de vergunningaanvraag een privacy protocol te worden aangeleverd waarin is omschreven hoe de persoonsgegevens verwerkt worden en hoe deze voorgenomen gegevensdeling voldoet aan de eisen uit de AVG.

Toetsing vergunningaanvraag
Bij de aanvraag voor een vergunning toetst de Autoriteit Persoonsgegevens of de verwerking voldoet aan de eisen uit de AVG en UAVG. Er mag pas gestart worden met het verwerken van de strafrechtelijke persoonsgegevens als de vergunning daadwerkelijk is verleend. Uit de informatie op de website van de Autoriteit Persoonsgegevens en uit nader contact met de Autoriteit Persoonsgegevens is gebleken dat bij de beoordeling van de vergunningsaanvraag de proportionaliteits- en noodzakelijkheidstoets een belangrijke rol speelt. Er wordt onder meer rekening gehouden met de volgende vereisten:

- Noodzakelijkheid: is de verwerking van de strafrechtelijke persoonsgegevens noodzakelijk om het doel van de verwerking te bereiken? Het doel van de verwerking mag niet op een andere manier bereikt kunnen worden die minder ingrijpend is voor de persoonlijke levenssfeer van de betrokkenen. Indien cross-sectoraal gegevens gedeeld gaan worden, dient goed onderbouwd te worden waarom deze cross-sectorale gegevensdeling noodzakelijk is om het doel te bereiken of dat in dit geval ook alternatieven mogelijk zijn reeds al voldoende alternatieven bestaan? Wat is de effectiviteit van de cross-sectorale gegevensdeling?
- Zwaarwegend algemeen belang: Organisaties die een vergunning verleend willen hebben, moeten goed aan kunnen tonen waarom hun (bedrijfs)belang zwaarder weegt dan het privacybelang van de mensen over wie het gaat. Er moet dan ook goed aangetoond worden waarom het bestrijden van fraude voor de organisaties die cross-sectoraal gegevens willen delen van dusdanige betekenis is, dat het gerechtvaardigd is deze gegevens te delen over de betrokkenen. Organisaties dienen dit zwaarwegend belang zelf aantoonbaar te maken. Nu de wens bestaat cross-sectoraal gegevens te delen tussen private partijen en daarmee de impact op de persoonlijke levenssfeer van de betrokkenen groter kan zijn dan wanneer uitsluitend binnen een bepaald bedrijf of bepaalde bedrijfstak gegevens gedeeld gaan worden, moet goed aangetoond worden door de organisaties wat het belang is van deze deling. Zie voor meer informatie over de invulling van het belang in 3.1.3.1.
- Waarborgen: er moeten voldoende waarborgen worden getroffen om de persoonlijke levenssfeer van de betrokkenen niet onevenredig te schaden. Hoe meer impact de gegevensverwerking heeft, hoe meer waarborgen getroffen dienen te worden om de persoonlijke levenssfeer van de betrokkenen te beschermen. Zodra een betrokkene onderdeel wordt van cross-sectorale gegevensdeling, kan dit stigmatiserend werken en mogelijk leiden tot uitsluiting. Indien cross-sectoraal gegevens gedeeld gaan worden, dient bij de inrichting daarvan zeer goed nagedacht te worden hoe de inbreuk op de persoonlijke levenssfeer zo beperkt mogelijk blijft en welke waarborgen daartoe getroffen worden. Zie voor waarborgen 3.1.3.1 gerechtvaardigd belang en 3.1.6 zorgvuldige gegevensverwerking.

Verloop procedure
Zoals uiteengezet in 3.1.5, dient door de partijen gezamenlijk voorafgaand aan de vergunningaanvraag een DPIA te worden uitgevoerd en een privacy protocol te worden opgesteld. Indien uit de DPIA blijkt dat sprake is van een hoog risico, dient - voordat de vergunning kan worden aangevraagd - eerst de Autoriteit Persoonsgegevens geraadpleegd te worden over de voorgenomen verwerking. In beginsel is de Autoriteit

Persoonsgegevens gehouden om binnen acht weken antwoord te geven op een voorafgaande raadpleging. Deze termijn kan onder omstandigheden worden verlengd wanneer bijvoorbeeld de voorgenomen verwerking zeer complex is. De aanvraag van de vergunning zelf wordt voorts behandeld in overeenstemming met de Algemene wet bestuursrecht en de daarin opgenomen termijnen.

Zoals uit het voorgaande blijkt, dienen meerdere stappen doorlopen te worden voordat een vergunning aangevraagd kan worden. Indien organisaties cross-sectoraal gegevens gaan delen, dienen zij te starten met het uitvoeren van een DPIA en het opstellen van een privacy protocol. Om het traject zo efficiënt en effectief mogelijk te laten verlopen, wordt het raadzaam geacht als de organisaties voorafgaand aan de start van het traject overeenstemming hebben bereikt over de inrichting van de gegevensdeling, de input die zij willen leveren ten behoeve van de gegevensdeling en voornamelijk de input die zij als organisatie willen leveren om een dergelijk traject in te gaan. Het wordt aanbevolen de belangen goed af te stemmen en zoveel mogelijk overeen te laten komen, zodat het traject zo efficiënt en effectief mogelijk kan worden doorlopen.