Ministerie van Justitie en Veiligheid

Handreiking

De aanpak van mensen-handel en het gebruik van persoonsgegevens

De "0.9-versie"

Inhoudsopgave

Leeswijzer

Mensenhandel is vaak lastig te ontdekken. Slachtoffers van mensenhandel verkeren vaak in een kwetsbare positie, er is vaak sprake van bedreigingen en dwang. Dat maakt dat ze zich niet snel zullen melden. Evengoed is mensenhandel een ernstige misstand en een aantasting van onze rechtsstaat die waar mogelijk met kracht bestreden moet worden. Daarom is het van groot belang om alert te zijn op alle signalen, zodat dat deze verder onderzocht kunnen worden. We moeten doen wat mogelijk is om daders op te sporen en aan te pakken. Alleen dan kunnen we slachtoffers de bescherming, zorg en ondersteuning bieden die ze nodig hebben en waar ze in ons land recht op hebben. Om aan die dure plicht invulling te kunnen geven moeten betrokkenen informatie kunnen delen over mogelijke misstanden. Dat is echter in de praktijk ingewikkeld. Veel partijen ervaren belemmeringen bij het delen van die informatie. Soms heeft dit te maken met beperkingen die volgen uit de privacywetgeving. Regelmatig heeft het ook te maken met onduidelijkheid over wat er nou wel en niet gedeeld mag worden. Dit zorgt dan voor handelingsverlegenheid. Te vaak leiden onzekerheid, onbekendheid met regels en de angst om fouten te maken tot een te eenzijdige afweging die resulteert in niet-ingrijpen. Dan worden weliswaar alle risico's op inbreuken op de privacy vermeden, maar blijft de misstand voortbestaan. Slachtoffers van mensenhandel zijn dan de dupe; zij worden niet of onvoldoende geholpen. Dit is onwenselijk. Het streven moet zijn om een optimaal evenwicht te bereiken: effectieve bestrijding van mensenhandel waar nodig bínnen de regels die daarvoor gelden. De enige juiste afweging is een scherpe afweging.

Bij de strijd tegen mensenhandel en de ondersteuning van slachtoffers (verder kortweg: de aanpak van mensenhandel) komen veel verschillende partners in beeld. Uit zowel het opsporingsdomein, het bestuurlijk domein (toezicht, gemeentelijke taken, vreemdelingenketen) en uit het zorg- en hulpverleningsdomein. Zij richten zich daarbij dan weliswaar op dezelfde gevallen van mensenhandel, maar niet primair op dezelfde personen. De nadruk ligt vaak óf bij de daders óf bij de slachtoffers. Desondanks zullen vaak partijen uit alle domeinen betrokken zijn en zowel per domein als tussen de domeinen moeten samenwerken. Ook daarvoor is het nodig om informatie met elkaar uit te wisselen.

De gemakkelijke conclusie is dat mensenhandel alleen effectief bestreden kan worden als op alle niveaus en tussen alle partners intensief wordt samengewerkt. Maar de vraag blijft opkomen in welke gevallen persoonsgegevens verzameld, gebruikt en gedeeld mogen worden. Binnen de eigen organisatie en met anderen. Binnen en buiten de overheid. In deze handreiking wordt hierop zo goed en concreet mogelijk antwoord gegeven.

De "0.9-versie"

Deze handreiking wordt nu in eerste instantie gepubliceerd als ***"0.9-versie"***.
Dat wil zeggen: een versie die inhoudelijk volwaardig en voldragen is, maar die er baat bij heeft als we nog meer voorbeelden en vragen uit de praktijk verzamelen. Daar gaan we actief naar op zoek – wederom met alle betrokken partijen uit de praktijk – zodat we begin 2021 de ***"1.0-versie"*** kunnen publiceren.

Leeswijzer

In **>Deel A** leggen we eerst een aantal van de gebruikte begrippen uit. Omdat de handreiking breed toepasbaar moet zijn, gebruiken we vaak generieke begrippen te gebruiken.

In **>Deel B** schetsen we vervolgens de algemene juridische kaders voor gegevensdeling. Daarbij besteden we in het bijzonder aandacht aan wat ook specifiek van belang is voor de verwerking van persoonsgegevens bij

de aanpak van mensenhandel. Deel B begint met het 'spoorboekje'; de vragen die je moet stellen om te kunnen beoordelen of je in een concreet geval gegevens mag verwerken. Deze worden uiteengezet en toegelicht. Het 'spoorboekje' doet ook dienst als samenvatting van het juridisch kader. Voor degenen die zich daar in willen verdiepen worden de juridische kaders vervolgens ook nog in meer detail besproken.
>Deel C is opgebouwd aan de hand van diezelfde vragen. Stapsgewijs worden ze voor een aantal categorieën partijen beantwoord. Daarbij wordt een gedetailleerder en concreter overzicht gegeven van de mogelijkheden die er zijn om tot verstrekking van persoonsgegevens over te gaan. Dit doen we aan de hand van diverse praktijkvoorbeelden, Q&A's en tips. Dit is gedaan voor de volgende categorieën:

- **>politie, Koninklijke Marechaussee, bijzondere opsporingsdiensten, zoals de Inspectie SZW – Directie Opsporing, en boa's**
- **>(gemeentelijke) toezichthouders, waaronder de Inspectie SZW, en de gemeente voor bepaalde andere taken**
- **>zorgverleners, aanbieders en hulpverleners met een medisch beroepsgeheim (reguliere zorg en sociaal domein) én zonder een medisch beroepsgeheim (sociaal domein)**
- **>publieke en private partijen met een meldpunt- of coördinatiefunctie, waaronder Veilig Thuis, de zorgcoördinator en de aandachtsfunctionaris mensenhande**
- **>niet-strafrechtelijke partners binnen de vreemdelingenketen, waaronder de IND, de Koninklijke Marechaussee en het COA**

Uit het oogpunt van de leesbaarheid is ervoor gekozen in Deel C alleen die artikelverwijzingen op te nemen die een aanvulling of concretisering zijn van het algemene juridische kader dat in deel B uiteengezet en toegelicht wordt. Omdat het ook met de beste bedoelingen weleens verkeerd gaat, staat op de achtervlap een korte **>checklist** voor welke stappen dan genomen moeten worden.

Zit je met een **concrete vraag**? Ga direct door naar het voor jou meest relevante onderdeel van **>Deel C**. Maar, is het de eerste keer, lees dan daarvoor een keer **>Deel A** en het **>spoorboekje**.
Blijf je zitten met verdiepende vragen of kom je uit bij een verwijzing naar Deel B? Dan kan dat een signaal zijn dat het goed is om je privacyfunctionaris / functionaris gegevensbescherming erbij te betrekken. Of misschien een collega die al vaker met hetzelfde vraagstuk te maken heeft gehad?

Wil je graag meer weten over het **algemene kader**, maar heb je niet direct behoefte aan alle juridische details? Ga door naar het **>spoorboekje**. Dat bevat ook diverse verwijzingen naar waar bepaalde onderwerpen in Deel B in meer detail besproken worden. Kom je daar zelf niet uit, dan kan dat een signaal zijn dat het goed is om ook eens door te praten met je privacyfunctionaris / functionaris gegevensbescherming.

Wil je met name meer weten over het algemene kader en in het bijzonder ook de **juridische details**? Ga dan door naar **>Deel B**. Maar, is het de eerste keer, lees dan daarvoor een keer **>Deel A** en het **>spoorboekje**.

DEEL A Algemene begrippen en uitgangspunten

In dit deel leggen we eerst een aantal van de gebruikte begrippen uit. Omdat de handreiking breed toepasbaar moet zijn, hebben we geprobeerd generieke begrippen te gebruiken. In de praktijk zullen er ook andere begrippen gebruikt worden of hebben de begrippen daar een andere invulling. De hier gehanteerde begrippen zijn niet bedoeld als definities die boven alle discussie verheven zijn, maar we gebruiken ze om spraakverwarring te voorkomen.

1. Mensenhandeldossiers

Bij de aanpak van mensenhandel onderscheiden we verschillende soorten dossiers waarin persoonsgegevens worden gebruikt. In deze handreiking gebruiken we hier de volgende generieke termen voor:

Soort dossier	Omschrijving
Signaal	Er is *mogelijk* sprake van mensenhandel. Dit moet echter verder onderzocht worden. Signalen dienen 'opgeplust' te worden: verschillende zwakke signalen moeten gecombineerd worden tot een dossier dat daadwerkelijk opgepakt kan worden.
Melding	Er kan met *redelijke zekerheid* aangenomen worden dat er sprake is van mensenhandel. Bij een melding moet bekeken worden wat er aan de hand is en welke acties nodig en/of mogelijk zijn en wie daarbij betrokken moeten worden.
Routering	Het is voldoende duidelijk en aannemelijk dat er sprake is van mensenhandel. Er kunnen (gerichte) acties ingezet worden. Het dossier moet bij de juiste partijen in het opsporingsdomein en/of bestuurlijke domein en/of het zorg- en hulpverleningsdomein terecht komen. Het dossier kan ook naar een coördinerende partij gaan om (eerst) als coördinatie- of casusdossier opgepakt te worden. Deze kan het dossier vervolgens *verder* routeren naar de aangewezen uitvoerende partijen.
Coördinatie- en casusdossier	Bij de aanpak van daders en de zorg- en hulpverlening aan slachtoffers zijn per domein vaak meerdere partijen betrokken. Bij een *coördinatie*dossier ligt het accent op afstemming van de werkzaamheden van verschillende partijen. Bij een *casus*dossier ligt de nadruk op gezamenlijk overleg om tot een goede inhoudelijke aanpak te komen.
Regulier uitvoering	Het gaat hierbij om de uitvoering van: • het opsporen, vervolgen en sanctioneren van daders; • het inzetten van het bestuurlijk instrumentarium bij de aanpak van overtreders; • het verlenen van zorg en hulp aan slachtoffers en het zorgdragen voor hun fysieke veiligheid met daarbij in het bijzonder: - adviseren en informeren over hun wettelijke rechten en hen daarbij ondersteunen; - ondersteunen bij opvang, maatschappelijke hulp, huisvesting, inkomen, werk en onderwijs en scholing; - medische en geestelijke zorg en bijstand verlenen.

In de praktijk worden ook andere definities gebruikt. In algemene zin wordt bijvoorbeeld een vergelijkbare uitleg gegeven aan zwakke *versus* sterke signalen als hierboven aan signalen *versus* meldingen.

Daarnaast wordt het begrip 'melding' in het opsporingsdomein gebruikt voor een melding die een burger doet bij de meldkamer. Zo'n melding *kan* onvoldoende gefundeerd zijn om tot opsporing over te gaan. Een melding van (mogelijke) mensenhandel komt vaak bij team mensenhandel van de Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel (AVIM) terecht. De melding wordt wanneer mogelijk met informatie uit de organisatie 'opgeplust' tot een 'signaal´. Een signaal wordt dan verder onderzocht met onder andere de inzet van opsporingsmiddelen. Er kan dan sprake zijn van een 'verdenking' en een 'verdachte' als bedoeld in art. 27 Wetboek van Strafvordering).

De 'geringste aanwijzing' is ook een begrip dat gebruikt wordt in de context van mensenhandel. Op grond van internationale regelgeving is de Nederlandse overheid verplicht om in geval van de geringste aanwijzing van mensenhandel bescherming te bieden aan (mogelijke) slachtoffers van mensenhandel. De politie, de Koninklijke Marechaussee of (via de politie) de Directie Opsporing van Inspectie SZW (ISZW-DO) zullen, als ze van oordeel zijn dat er sprake is van de geringste aanwijzing, een (mogelijk) slachtoffer zonder verblijfsstatus de bedenktijd in de zin van de Vreemdelingencirculaire 2000 aanbieden. Dit houdt in dat de vreemdeling een periode van maximaal drie maanden de tijd krijgt om te bedenken of hij aangifte wil doen van mensenhandel. In deze periode heeft de vreemdeling rechtmatig verblijf en krijgt hij opvang en voorzieningen. De drempel om in aanmerking te komen voor de bedenktijd is bewust laag gehouden. Van een 'melding' zoals bedoeld in deze handreiking hoeft dus geen sprake te zijn. Het is echter ook géén synoniem voor 'signaal' (wel zal er vaak sprake zijn van overlap), omdat het bij een signaal ook kan gaan om situaties waarbij helemaal nog geen slachtoffers in beeld zijn.

2. Meldpuntfunctie

Burgers, professionals en organisaties moeten signalen van mensenhandel kunnen doorgeven en meldingen over mensenhandel kunnen doen. Dit gebeurt bij partijen die een meldpuntfunctie hebben. Deze partijen:

- behandelen de binnengekomen signalen en meldingen (hierbij combineren ze de informatie van een signaal of melding – voor zover toegestaan – met informatie van andere meldpuntfuncties, van partijen uit de verschillende domeinen en van andere organisaties die informatie over de gemelde situatie kunnen hebben);
- routeren aan te pakken dossiers naar partijen met een coördinatiefunctie (bij een coördinatie- of casusdossier) en/of naar uitvoerende partijen.

Momenteel treden de volgende partijen op als meldpuntfunctie:

Politie, Koninklijke Marechaussee, Inspectie SZW	Zij maken gebruik van het **>Themaregister Mensenhandel**, op grond waarvan ook (zachte) signalen verwerkt mogen worden.
Stichting Meld Misdaad Anoniem (M.)	M. ontvangt signalen en meldingen die het doorstuurt naar de politie of andere opsporingsdiensten.
Veilig Thuis	Veilig Thuis kan – als overlap is met huiselijk geweld of kindermishandeling – een rol spelen bij meldingen en routering.
Meldpunt loverboys / jeugdprostitutie	Sommige meldpunten loverboys zijn ondergebracht bij Veilig Thuis, andere functioneren zelfstandig. Er is echter géén sprake van eigen **>wettelijke, publieke taak** om als meldpuntfunctie op te treden.
(Gemeentelijke) zorgcoördinator	Zorgcoördinatoren ontvangen signalen en meldingen van burgers en professionals uit het zorg- en hulpverleningsdomein of het onderwijsdomein. Met de komst van Veilig Thuis is er echter géén sprake meer van een eigen **>wettelijke, publieke taak**.
Aandachtsfunctionaris mensenhandel	Aandachtsfunctionarissen ontvangen signalen en meldingen uit de (ambtelijke) organisatie, vaak met oog op samenwerking binnen RIEC's. Er is echter géén sprake van een eigen **>wettelijke, publieke taak**.

>In welke gevallen mogen partijen met een meldpuntfunctie signalen en meldingen van mensenhandel verwerken?

Om het gebruik van gegevens bij partijen met een meldpuntfunctie en bij samenwerking tussen partijen met een meldpuntfunctie zoveel mogelijk te beperken, delen partijen met een meldpuntfunctie bij voorkeur alleen een ingevuld 'scoreformulier' of passend alternatief zoals een indicatielijst met elkaar. De onderliggende gegevens die tot een bepaalde score/indicatie leiden, worden zoveel mogelijk alleen bij de afzonderlijke partijen met een meldpuntfunctie verwerkt.

Praktijkvoorbeeld – Scoremodel en scoreformulier

Voor het verder onderzoeken van signalen en meldingen en om mensenhandel met het Themaregister Mensenhandel in beeld te krijgen, zijn in het kader van de domeinoverstijgende informatiegestuurde werkwijze (DIGW) een scoremodel en scoreformulier ontwikkeld. Met domeinoverstijgend wordt gedoeld op het verbinden van de intelligence- en opsporingsfuncties ten aanzien van de aanwezige informatie binnen in de verschillende deeldomeinen van de dagelijks politietaak, de grotere rechercheonderzoeken en de aanpak van georganiseerde criminaliteit.

Het scoremodel is in de eerste plaats ontwikkeld door de politie, in samenwerking met onder andere de Inspectie SZW, de Koninklijke Marechaussee en het OM. De methode wordt voor het thema mensenhandel landelijk ingevoerd bij de politie, de Koninklijke Marechaussee en de Directie Opsporing van de Inspectie SZW (ISZW-DO). Het model kan ook als basis of blauwdruk worden gebruikt om per domein of organisatie inhoudelijk verschillende 'scoreformulieren' of 'indicatielijsten' vorm te geven die dezelfde grondslag hebben. De afgeleide modellen kunnen vervolgens de basis vormen voor een score-instrument 'op maat', dat naadloos aansluit op de eigen praktijk en terminologie. Op deze manier kan gewerkt worden aan een meer objectieve en efficiënte verwerking van signalen en routering van meldingen.

3. Coördinatiefunctie

Bij de aanpak van mensenhandel spelen zowel partijen uit het opsporingsdomein, het bestuurlijke domen en het zorg- en hulpverleningsdomein tegelijkertijd een rol. De partijen richten zich op dezelfde situatie, maar niet primair op dezelfde personen. Het opsporingsdomein en het bestuurlijke domein richten zich meer op de daders. Het zorg- en hulpverleningsdomein is meer gericht op de slachtoffers. Om de gehele aanpak goed te laten verlopen, spelen partijen met een coördinatiefunctie een belangrijke rol. Zij coördineren de samenwerking binnen en over de grenzen van de domeinen. Deze partijen:

a) coördineren bij dossiers waar meerdere partijen activiteiten verrichten (coördinatiedossiers).
b) stemmen af bij dossiers waar partijen inhoudelijk samen dienen te werken (casusdossiers).

Partijen	Taak coördinatiefunctie
Partijen uit het opsporingsdomein en/of het bestuurlijke domein dienen inhoudelijk samen te werken bij de aanpak van daders.	Afstemmen over de inhoudelijke aanpak, bijvoorbeeld door het organiseren van casusoverleggen, zoals een 'RIEC-overleg'.
Partijen uit het zorg- en hulpverleningsdomein dienen inhoudelijk samen te werken bij de zorg- en hulpverlening aan slachtoffers	Afstemmen over de inhoudelijke aanpak, bijvoorbeeld door het organiseren van casusoverleggen zoals een 'zorgtafel'.
Als mensenhandel tegelijkertijd neerkomt op kindermishandeling of huiselijk geweld dienen partijen uit zowel het sanctie- als het zorg- en hulpverleningsdomein inhoudelijk samen te werken bij de gecombineerde aanpak van daders en de zorg- en hulpverlening aan slachtoffers van huiselijk geweld .	Afstemmen over de inhoudelijke aanpak, bijvoorbeeld door het organiseren van casusoverleggen zoals die plaatsvinden binnen de Veiligheidshuizen.

De volgende partijen vervullen momenteel een coördinatiefunctie:

Domein	Partij
Opsporingsdomein	Politie, Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel (AVIM)
Bestuurlijk domein	*Ketenregisseur* ⊕ en/of *(gemeentelijke) aandachts-functionaris mensenhandel* ⊕
Zorg- en hulpverlenings-domein	*(Gemeentelijke) zorgcoördinator* ⊕ CoMensha Meldpunten loverboys / jeugdprostitutie

>In welke gevallen mogen partijen met een coördinatiefunctie signalen en meldingen van mensenhandel verwerken?

DEEL B Het algemene juridische kader

In dit deel schetsen we de algemene juridische kaders voor gegevensdeling. Daarbij besteden we in het bijzonder aandacht aan wat ook specifiek van belang is voor de verwerking van persoonsgegevens bij de aanpak van mensenhandel. Deel B begint met een 'spoorboekje'; de vragen die je moet stellen om te kunnen beoordelen of je in een concreet geval gegevens mag verwerken worden uiteengezet en toegelicht. Het 'spoorboekje' doet ook dienst als samenvatting van het juridisch kader, dat vervolgens in hoofdstuk 5 tot en met 9 in meer detail wordt besproken.

4. Spoorboekje

Bij de aanpak van mensenhandel speelt samenwerking tussen verschillende partijen en het daarbij delen van persoonsgegevens een centrale rol. Maar met wie mag je eigenlijk persoonsgegevens delen? Wie met jou? En welke persoonsgegevens dan?

STAP 1 Is de AVG of de Wpg van toepassing op de verstrekking?

De **voorvraag** is altijd aan de hand van welk 'regime' je deze vragen moet beantwoorden. Voor het bestuurlijke domein (toezicht, gemeentelijke taken, vreemdelingenketen) en het zorg- en hulpverleningsdomein (inclusief het sociaal domein) is dat in hoofdzaak het regime van de Algemene verordening gegevensbescherming (AVG). Dat omvat ook de Uitvoeringswet AVG (UAVG) en diverse onderdelen van sectorale regelgeving die voor specifieke sectoren, beroepsgroepen of activiteiten gelden.

De gegevensverwerking in het opsporingsdomein is geregeld in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Dat regime biedt de politie, de Koninklijke Marechaussee (voor zover het de politietaak betreft), bijzondere opsporingsdiensten zoals de Inspectie SZW - Directie Opsporing (ISZW-DO) en buitengewoon opsporingsambtenaren (boa's) het kader voor gegevensverwerking bij de opsporing en vervolging van strafbare feiten, de tenuitvoerlegging van strafrechtelijke beslissingen en de bescherming en de voorkoming van gevaren voor de openbare veiligheid. Het is met name de Wpg die binnen het opsporingsdomein het kader biedt voor de fase waarin signalen en meldingen worden verzameld, verwerkt en gedeeld.

De **kernvraag** bij het verwerken van persoonsgegevens is altijd of je daar een 'wettelijke grondslag' voor hebt. Het verwerken van persoonsgegevens heeft privacyrechtelijke gevolgen voor de persoon op wie de persoonsgegevens betrekking hebben ('de betrokkene'). De AVG bepaalt daarom dat je persoonsgegevens alleen mag verwerken als daarvoor een goede reden bestaat (een 'wettelijke grondslag´).

De Wpg heeft een zogenoemde 'gesloten verstrekkingsregime', waarbij de mogelijkheden om politiegegevens te verstrekken uitputtend zijn geregeld. De Wpg regelt zo strikt aan wie en voor welke doeleinden politiegegevens mogen worden verstrekt.

STAP 2 – 4 Zijn er juridische belemmeringen voor de het delen van de persoonsgegevens?

Voordat we aan de kernvraag toekomen moeten eerst een drietal potentiële hordes bezien en mogelijk genomen worden. Het gaat hier om:

(STAP 2) Vallen de persoonsgegevens onder een geheimhoudingsplicht en zo ja, kan deze worden doorbroken?
(STAP 3) Als er bijzondere persoonsgegevens worden verstrekt, is er een wettelijke grondslag die het verbod om bijzondere persoonsgegevens te verwerken doorbreekt?
(STAP 4) Als er strafrechtelijke persoonsgegevens worden verstrekt, is daar een wettelijke grondslag voor?

(STAP 2) Geheimhoudingsplichten en beroepsgeheim
In tegenstelling tot wat vaak gedacht wordt bevat de AVG géén *algemene* bepaling over geheimhouding of verplichting voor lidstaten of organisaties om zelf algemene geheimhoudingsverplichtingen te introduceren. De AVG bevat wél een enkele *specifieke* bepaling over de geheimhouding van bijzondere persoonsgegevens.

Er zijn ook diverse *wettelijke* geheimhoudingsplichten. Deze zijn vaak opgenomen in sectorale regelgeving. Relevante geheimhoudingsplichten zijn onder meer het medisch beroepsgeheim van zorgverleners. Andere voorbeelden zijn de geheimhoudingsplichten van de Wet maatschappelijke ondersteuning 2015 (Wmo 2015) en de Jeugdwet. Daarnaast bevat de Algemene wet bestuursrecht een algemene geheimhoudingsplicht (art. 2:5) die simpel gezegd rust op iedereen werkzaam bij of voor een overheidsinstanties die daarbij in aanraking komt met vertrouwelijke gegevens.

Een geheimhoudingsplicht kan alleen worden doorbroken als daarvoor een expliciete wettelijke grondslag bestaat (een zogenoemde 'doorbrekingsgrond').

>Lees meer over geheimhoudingsplichten, beroepsgeheim en doorbrekingsgronden

Op alle politiegegevens rust een geheimhoudingsverplichting (art. 7 Wpg). Het delen van politiegegevens is alleen mogelijk als:
- dat wettelijk verplicht is;
- de bepalingen van paragraaf 3 Wpg verstrekking toestaan;
- de politietaak het verstrekken in een bijzonder geval noodzakelijk maakt.

Zie **>paragraaf 10.2, stap 2** voor verschillende voorbeelden.

Ook de ontvanger van de politiegegevens is verplicht tot geheimhouding ervan. De ontvanger mag deze geheimhouding alleen doorbreken als hij wettelijk verplicht is de politiegegevens te verstrekken of als dit noodzakelijk is om zijn taak uit te voeren. Dat betekent dat er altijd voldaan moet worden aan de eisen van proportionaliteit en subsidiariteit. Dat houdt in: staat de inbreuk voor betrokkene in verhouding tot het doel van de gegevensverwerking? En is het doel niet op een andere manier te bereiken, die minder nadelig is voor de betrokkene (bijvoorbeeld door geen of minder persoonsgegevens te verwerken)?

>Lees meer over het noodzakelijkheidsbeginsel

(STAP 3) Bijzondere persoonsgegevens
Bijzondere persoonsgegevens zijn vanwege hun aard gevoelig en krijgen extra bescherming in de AVG. Het gaat bijvoorbeeld om persoonsgegevens over iemands ras of etnische afkomst, politieke opvattingen, godsdienst of levensovertuiging, gezondheid, seksuele leven of strafrechtelijk verleden. De verwerking van bijzondere persoonsgegevens is verboden, tenzij er een specifieke wettelijke bepaling bestaat in Nederlands recht of Unierecht die het gebruik van dergelijke gegevens toch mogelijk maakt (art. 9 lid 2 AVG). Ook dit wordt een 'doorbrekingsgrond genoemd. Deze zijn nader uitgewerkt in de artikelen 22 tot en met 30 Uitvoeringswet AVG (UAVG).

>Lees meer over bijzondere persoonsgegevens en de doorbrekingsgronden

Het regime van de Wpg biedt de partijen in het opsporingsdomein de mogelijkheid om bijzondere persoonsgegevens te verwerken én te delen met derden. Zij mogen dat, in aanvulling op de verwerking van 'normale' politiegegevens, als dat voor het doel van de verwerking onvermijdelijk is en de gegevens afdoende zijn beveiligd (art. 5 Wpg). De kwalificatie 'onvermijdelijk' is bedoeld om de opsporingsambtenaar te dwingen zich af te vragen of de verwerking van bepaalde gevoelige gegevens in het concrete geval echt onvermijdelijk is. Gevoelige gegevens mogen nooit bij wijze van automatisme worden verwerkt.

>Lees meer over bijzondere politiegegevens

*(**STAP 4**) Strafrechtelijke persoonsgegevens*
Strafrechtelijke persoonsgegevens vormen onder de AVG een aparte categorie persoonsgegevens. Ook deze gegevens krijgen extra bescherming in de AVG. Het gaat bijvoorbeeld om gegevens over strafrechtelijke veroordelingen, strafbare feiten of een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag. Strafrechtelijke persoonsgegeven mogen alleen worden verwerkt onder toezicht van de overheid of als de verwerking is toegestaan op grond van Nederlands recht of Unierecht dat passende waarborgen voor de rechten en vrijheden van de betrokkene biedt (art. 10 AVG).

>Lees meer over strafrechtelijke persoonsgegevens

Politiegegevens zijn naar hun inhoud vrijwel altijd ook aan te merken als strafrechtelijke gegevens zoals bedoeld in de AVG. Dit houdt in dat als politiegegevens worden verstrekt aan een partij buiten het opsporingsdomein, deze dan na ontvangst door de ontvanger zijn aan te merken als strafrechtelijke persoonsgegevens. Van belang is dat de ontvanger van de politiegegevens zelf beschikt over een verwerkingsgrondslag voor de verwerking van die strafrechtelijke gegevens. Daarvoor moet worden gekeken naar het regime van de AVG, in het bijzonder naar de UAVG.

STAP 5 Kan de verstrekking van de persoonsgegevens worden gebaseerd op een wettelijke grondslag?

Als deze hordes zijn genomen kom je terug bij de **kernvraag**: is er een 'wettelijke grondslag' die het delen van de persoonsgegevens mogelijk maakt? In art. 6 lid 1 AVG staan er zes beschreven:

a) Je hebt toestemming van de betrokkene.
b) Het is noodzakelijk om persoonsgegevens te verwerken om een (behandel) overeenkomst uit te voeren.
c) Het is noodzakelijk om persoonsgegevens te verwerken, omdat je daartoe wettelijk verplicht bent ('wettelijke verplichting').
d) Het is noodzakelijk om persoonsgegevens te verwerken om vitale belangen van de betrokkene of van een ander persoon te beschermen.
e) Het is noodzakelijk om persoonsgegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen ('wettelijke, publieke taak').
f) Het is noodzakelijk om persoonsgegevens te verwerken om gerechtvaardigde belangen van jouzelf of een derde te behartigen die zwaarder wegen dan de belangen van de betrokkene.

De grondslagen (b) tot en met (f) zijn 'noodzakelijkheidsgrondslagen': de verwerking is alleen gerechtvaardigd als dit noodzakelijk is voor de in deze grondslagen genoemde doelen (art. 5 lid 1, aanhef en onder c, AVG). In deze vraag ligt besloten dat de verwerking van de persoonsgegevens proportioneel moet zijn en dat er voldaan moet zijn aan de eis van subsidiariteit.

>Lees meer over het noodzakelijkheidsbeginsel

Grondslag (a) Toestemming
Om beroep op toestemming te kunnen doen moet deze op voldoende informatie berusten en in vrijheid, specifiek en met een ondubbelzinnige, actieve handeling zijn gegeven. Dat betekent dat betrokkenen in vrijheid hun wil moeten kunnen uiten. Ook mag er geen twijfel zijn of betrokkenen hun toestemming hebben gegeven en voor welke specifieke verwerking zij dit

hebben gedaan. Bij de uitvoering van publiekrechtelijke taken, onder andere het sociaal domein, is er vaak een afhankelijkheidsrelatie tussen de betrokkenen en overheidsinstanties. Weigeren mensen toestemming voor het verwerken van hun gegevens, dan kan dat bijvoorbeeld gevolgen hebben voor een gewenste voorziening. Daarom is er in dat soort situaties géén sprake van vrije toestemming in de zin van de AVG. Toestemming kan dan dus niet gelden als de grondslag voor de gegevensverwerking.

Toestemming kan alleen een grondslag vormen voor de *eigen* persoonsgegevens van de betrokkene. Voor het verstrekken van persoonsgegevens over een derde (bijvoorbeeld een dader) kan het dus géén toereikende grondslag vormen. Het verstrekken van persoonsgegevens van een dader zal altijd gebaseerd moeten zijn op een wettelijke verplichting (grondslag (c)) of de uitvoering van een *eigen* wettelijke, publieke taak (grondslag (e)).

>Lees meer over grondslag (a)

Grondslag (b). Uitvoeren van een overeenkomst
In het bijzonder voor de reguliere werkzaamheden van zorgverleners zal het delen van persoonsgegevens regelmatig gebaseerd kunnen worden op de grond dat de verwerking noodzakelijk is om uitvoering te geven aan een overeenkomst, de behandelovereenkomst. Wat mogelijk is zal steeds afhankelijk zijn van de concrete situatie.

Grondslag (c). Wettelijke verplichting
De wettelijke verplichting waar het om gaat moet altijd een duidelijke grondslag hebben in Nederlands recht of Unierecht. Het gaat daarbij altijd om een *eigen* wettelijke verplichting voor de verwerker. Die voor een ontvanger kan géén grondslag vormen voor de verstrekking van persoonsgegevens.

Grondslag (d). Bescherming vitale belangen
In uitzonderlijke gevallen zal er bij de aanpak van mensenhandel sprake kunnen zijn van een beroep op de noodzaak om gegevens te verstrekken voor de bescherming van vitale belangen van de betrokkene of een ander persoon. Daarbij geldt dan dat de betrokkene zelf fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is zijn toestemming te geven. Het moet gaan om een levensbedreigende of crisissituatie, waardoor het niet als algemeen toepasselijke grondslag gebruikt kan worden.

Grondslag (e). Wettelijke, publieke taak
De wettelijke, publieke taak waar het om gaat moet altijd een duidelijke grondslag hebben in Nederlands recht of Unierecht. Het gaat daarbij altijd om een *eigen* wettelijke taak van de verwerker. Die van een ontvanger kan géén grondslag vormen voor het delen van persoonsgegevens.

>Lees meer over grondslag (e)

Grondslag (f). Gerechtvaardigd belang
Voor het delen van signalen of meldingen kan in uitzonderlijke gevallen op het gerechtvaardigde belang van een derde worden teruggevallen. Het kan daarbij gaan om het gerechtvaardigde belang van het slachtoffer, het algemene belang dat mensenhandel zoveel mogelijk moet worden voorkomen (ten aanzien waarvan de ontvanger dan wel een wettelijke, publieke taak moet uitvoeren) of het specifieke belang van de ontvanger (bijvoorbeeld de registratie van dergelijke meldingen). De gegevensverwerking moet daarbij dan noodzakelijk zijn om dat belang te behartigen. De verstrekking kan bovendien alleen plaatsvinden als het gerechtvaardigde belang zwaarder weegt dan de belangen van de betrokkene. Uitganspunt blijft overigens dat, waar mogelijk, de betrokkene wordt gevraagd om toestemming voor het delen van de informatie.

Vanwege het feit dat de wetgever de rechtsgrond bepaalt voor de verwerking van persoonsgegevens door overheidsinstanties, is de rechtsgrond 'gerechtvaardigd belang' niet van toepassing op verwerkingen door overheidsinstanties in het kader van de uitvoering van hun taken.

>Lees meer over grondslag (f)

Het Wpg-regime heeft zoals aangegeven een gesloten verstrekkingsregime, waarmee wettelijk en uitputtend is geregeld aan wie en voor welke doeleinden politiegegevens mogen worden verstrekt. Politiegegevens kunnen onder andere verwerkt worden als dat noodzakelijk is voor de uitvoering van de dagelijkse politietaak (art. 8 Wpg) en de grotere rechercheonderzoeken (art. 9 Wpg). Voor het verwerken van politiegegevens is verder relevant de regeling voor de *Themaregisters Mensenhandel* (art. 10 lid 1, aanhef en onder b, Wpg). Met het Themaregister Mensenhandel is het mogelijk om situaties waarbij er eventueel sprake zou kunnen zijn van mensenhandel (signalen) te onderzoeken.

Verder kunnen politiegegevens alleen worden verstrekt aan partijen buiten het opsporingsdomein als:
- dat wettelijk verplicht is;
- de bepalingen van paragraaf 3 Wpg verstrekking toestaan;
- de politietaak het verstrekken in een bijzonder geval noodzakelijk maakt.

Zie **>paragraaf 10.2, stap 2** voor verschillende voorbeelden.

STAP 6 Staat het doelbindingsbeginsel de verstrekking ('verdere verwerking') van de persoonsgegevens toe?

Als een expliciete wettelijke grondslag voor het delen van de persoonsgegevens ontbreekt, is het verstrekken binnen het AVG-regime daarmee niet op voorhand onmogelijk. Het kan zijn dat het 'doelbeginsel' een met het oorspronkelijke doel van de verzameling 'verenigbare verdere verwerking' toestaat (art. 6 lid 4 AVG). Met een 'verdere verwerking' wordt bedoeld dat persoonsgegevens die oorspronkelijk voor het ene doel zijn verzameld, worden verstrekt voor een ander afwijkend doel. Daarbij geldt dan altijd wel dat de ontvanger zelf ook een beroep moet kunnen doen op één van de wettelijke grondslagen voor de ontvangst en verdere verwerking van de persoonsgegevens (art. 6 lid 1 AVG). Als aan beide kanten een grondslag is voor de verstrekking, dan kan deze plaatsvinden.

>Lees meer over het doelbindingsbeginsel

Een verdere verwerking is ook mogelijk als je daarvoor toestemming hebt van de betrokkene of als Nederlands recht of Unierecht dat het mogelijk maakt. Daarbij kan bijvoorbeeld gedacht worden aan de aangiftebevoegdheid van art. 161 Wetboek van Strafvordering, die iedereen die kennis heeft van het begaan van een strafbaar feit de mogelijkheid biedt om aangifte te doen en zo informatie met de politie of bijzondere opsporingsdiensten te delen.

Het 'intern' hergebruik van gegevens voor andere doelen en het verstrekken van gegevens aan 'derden' dient vanuit de AVG op dezelfde wijze beoordeeld te worden. Als we in deze handreiking kortheidshalve spreken over het verstrekken aan derden voor 'verdere verwerking' van de gegevens door de ontvanger, dan geldt hetzelfde dus ook voor het intern 'hergebruik' voor andere doelen.

STAP 7 en 8 Waar moet verder op gelet worden als verstrekt mag worden?

Als er een wettelijke grondslag aanwezig is, of als expliciet wettelijke grondslag ontbreekt, maar er sprake is van een 'verenigbare verwerking', dan kunnen de persoonsgegevens worden gedeeld. Daarmee komen dan wel twee nieuwe vragen in beeld:

(STAP 7) Wordt er niet meer verstrekt dan de strikt noodzakelijke persoonsgegevens (*need to know*, in plaats van *nice to know*)?
(STAP 8) Moet de betrokkene worden geïnformeerd over de verstrekking of bestaat daarop een uitzondering?

(STAP 7) Noodzakelijkheidsbeginsel
Een concrete verstrekking moet voldoen aan het noodzakelijkheidsbeginsel. Dit betekent dat de verwerking van gegevens 'proportioneel' moet zijn en moet voldoen aan de eis van 'subsidiariteit'. Het noodzakelijkheidsbeginsel heeft ook gevolgen voor de omvang en de aard van de persoonsgegevens die mogen worden gedeeld. De persoonsgegevens moeten toereikend en direct relevant zijn en de verstrekking moet beperkt blijven tot het strikt noodzakelijke. Dit houdt in dat alleen '*need to know*'-informatie gedeeld mag worden (en dus geen '*nice to know*'-informatie).

>Lees meer over het noodzakelijkheidsbeginsel

Bij het verstrekken van gegevens wordt vaak de vraag gesteld of een bepaald document, zoals een proces-verbaal door de politie aan een andere partij verstrekt mag worden. Dit is onvoldoende precies. Het gaat bij het noodzakelijkheidsbeginsel nadrukkelijk om een afweging welke gegevens verstrekt mogen worden. Hetzelfde geldt ook bij de verwerking van politiegegevens en justitiële en strafvorderlijke gegevens.

(STAP 8) Informatieplicht
In veel gevallen geldt er een algemene of specifieke informatieplicht. In **>Deel C** worden deze toegelicht. Dat geldt ook voor de verschillende uitzonderingen hierop.

5. Gegevensverwerking; twee regimes en enkele AVG-begrippen

5.1 Twee regimes

Bij de aanpak van mensenhandel speelt samenwerking tussen verschillende partijen en het daarbij delen van persoonsgegevens een centrale rol. Maar met wie mag je eigenlijk persoonsgegevens delen? Wie met jou? En welke persoonsgegevens dan?

De eerste vraag is altijd aan de hand van welk 'regime' je deze vragen moet beantwoorden. Voor het bestuurlijke domein (toezicht, gemeentelijke taken, vreemdelingenketen) en het zorg- en hulpverleningsdomein (inclusief het 'sociaal domein') is dat in hoofdzaak het regime van de Algemene verordening gegevensbescherming (AVG). Dat omvat ook de Uitvoeringswet AVG (UAVG) en diverse onderdelen van sectorale regelgeving die voor specifieke sectoren, beroepsgroepen of activiteiten gelden. De gegevensverwerking in het opsporingsdomein is daarentegen geregeld in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Dat regime biedt het kader voor de politie, de Koninklijke Marechaussee (voor zover het politietaak betreft), bijzondere opsporingsdiensten zoals de Inspectie SZW - Directie Opsporing (ISZW-DO) en buitengewoon opsporingsambtenaren (boa's), voor gegevensverwerking bij de opsporing en vervolging van strafbare feiten, de tenuitvoerlegging van strafrechtelijke beslissingen en de bescherming en de voorkoming van gevaren voor de openbare veiligheid. Het is met name de Wpg die binnen het opsporingsdomein het kader biedt voor de fase waarin signalen en meldingen worden verzameld, verwerkt en gedeeld.

>Lees meer over het juridisch kader van de Wpg en Wjsg

5.2 Begrippen in de AVG

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Het gaat daarbij om informatie die direct (bijvoorbeeld naam, adres, telefoonnummer) of indirect (bijvoorbeeld BSN) naar een persoon te herleiden is. Van een *´persoonsgegeven'* is dus snel sprake.

Verwerken van gegevens
Vaak hebben we het over het verzamelen, verstrekken of delen van persoonsgegevens. Binnen de AVG wordt dit echter allemaal aangeduid met de verzamelterm 'verwerken'. Het is belangrijk om hierbij op te merken dat er een op punten afwijkend juridisch kader is voor het *verder* verwerken van gegevens met een ander doel dan waarvoor ze oorspronkelijk *verzameld* zijn.

'verzamelen' van persoonsgegevens	Hier gaat het bijvoorbeeld om het vastleggen, ordenen, structureren en opslaan van gegevens of om gegevens die bestemd zijn om in een bestand op te nemen dan wel bestemd zijn om op een later moment alsnog vast te leggen.
'verder verwerken' van persoonsgegevens **>Wat is het specifieke juridisch kader voor 'verder verwerken' met een ander doel?**	Hier gaat het bijvoorbeeld om het: • bijwerken of wijzigen • opvragen • raadplegen • gebruiken • verstrekken door middel van doorzending • verspreiden of op andere wijze ter beschikking stellen • combineren • afschermen • wissen of vernietigen

Verwerkingsverantwoordelijke
De *verwerkingsverantwoordelijke* speelt in het stelsel van de AVG een centrale rol. De verwerkingsverantwoordelijke draagt er de verantwoordelijkheid voor dat de verwerking van de persoonsgegevens rechtmatig is. De verwerkingsverantwoordelijke is degene die, alleen of samen met anderen, het doel (waarvoor) en de middelen (op welke wijze) van de verwerking van persoonsgegevens vaststelt.

Verwerker
De verwerkingsverantwoordelijke kan bij de verwerking van persoonsgegevens ook een zogenoemde *'verwerker'* inschakelen. De verwerker is degene die voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Hierbij kan bijvoorbeeld worden gedacht aan een cloudopslagprovider of beheerder van een portaal. De verwerker ontleent zijn bevoegdheid om persoonsgegevens te verwerken aan de bevoegdheid van de verwerkingsverantwoordelijke die hem inschakelt. Voor de kwalificatie van verwerker is bepalend of de organisatie aanwijzingen van de verwerkingsverantwoordelijke dient op te volgen met betrekking tot de verwerking van persoonsgegevens. Zo ja, dan is de organisatie een verwerker. Dat betekent overigens niet dat de organisatie op detailniveau aanwijzingen van de verwerkingsverantwoordelijke moet ontvangen en volgen, maar in ieder geval wél over het doel van de verwerking en de wezenlijke aspecten van de middelen voor de verwerking.

Bijzondere persoonsgegevens

Persoonsgegevens die vanwege hun aard gevoelig zijn krijgen extra bescherming in de AVG. Het gaat om:

gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken	Omdat slachtoffers benaderd dienen te worden in een taal die de slachtoffers kunnen begrijpen en omdat er bijzondere regelingen voor een specifieke verblijfsstatus voor slachtoffers zijn, zullen gegevens over de (spreek)taal en het geboorteland of land van herkomst nodig zijn. Bij deze gegevens kan het gaan om gegevens die (indirect) wijzen op ras of etnische afkomst. Verwerking van gegevens die duiden op ras of etnische afkomst kan ook aan de orde zijn, omdat een bepaalde afkomst of etniciteit juist een rol speelt bij de slachtofferkeuze of de specifieke vorm van uitbuiting. In bepaalde gevallen kan het bij het verlenen van geestelijke bijstand aan slachtoffers gaan om gegevens betreffende religieuze of levensbeschouwelijke overtuigingen van het slachtoffer. Uiteraard is het ook mogelijk dat dergelijke gegevens betrekking hebben op de dader.
***genetische gegevens* + / *biometrische gegevens met het oog op de unieke identificatie van een persoon* +**	Voor een juiste identificatie van daders en slachtoffers zal het in bepaalde gevallen nodig zijn om te beschikken over biometrische gegevens. Het is daarnaast mogelijk dat in het kader van een verblijfsvergunning de beschikking moet worden verkregen over genetische gegevens om bijvoorbeeld verwantschap met eventueel al in Nederland wonende familieleden vast te stellen.
***gegevens over gezondheid* +**	Gezondheidsgegevens omvatten niet alleen de gegevens die in het kader van een medisch onderzoek of een medische behandeling door een arts of zorgverlener worden verwerkt, maar alle gegevens die iets over de (geestelijke of lichamelijke) gezondheid van een persoon zeggen. Elke conclusie over iemands gezondheid is een gezondheidsgegeven, ongeacht de betrouwbaarheid daarvan. Voor de kwalificatie van een gezondheidsgegeven is niet relevant of het gegeven informatie prijsgeeft over de aard van de aandoening. Het enkele gegeven *dat* iemand ziek is, pijn heeft of een afspraak heeft bij een medisch specialist is een gezondheidsgegeven. Het verwerken van gezondheidsgegevens zal zich met name voordoen bij de zorg- en hulpverlening aan slachtoffers van mensenhandel. Zo spreekt art. 11 lid 7 EU Richtlijn over mensenhandel bijvoorbeeld zeer specifiek over het rekening houden met de belangen van slachtoffers met specifieke behoeften die voortkomen uit een eventuele zwangerschap, gezondheidstoestand, een handicap, een geestesstoornis of psychische aandoening die zij hebben en het psychische, fysieke of seksuele geweld dat slachtoffers ondergaan hebben.
gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Het zijn van sekswerker duidt op gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Bij seksuele uitbuiting zal er daardoor ten aanzien van de slachtoffers (al snel) sprake zijn van gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

>Wanneer mogen bijzondere persoonsgegevens verwerkt worden?

Strafrechtelijke persoonsgegevens
Strafrechtelijke persoonsgegevens vormen onder de AVG een aparte categorie persoonsgegevens. Ook deze gegevens krijgen extra bescherming in de AVG.

In het kort kunnen de volgende strafrechtelijke persoonsgegevens worden onderscheiden:
- Gegevens over strafrechtelijke veroordelingen of daarmee verband houdende veiligheidsmaatregelen (bijvoorbeeld het gegeven dat iemand (eerder) is veroordeeld tot gevangenisstraf).
- Gegevens over strafbare feiten of daarmee verband houdende veiligheidsmaatregelen (bijvoorbeeld het proces-verbaal van de politie met betrekken tot strafbare feiten of het gegeven dat iemand is gearresteerd).
- Gegevens over een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag (bijvoorbeeld een gebiedsverbod).

>Wanneer mogen strafrechtelijke persoonsgegevens verwerkt worden?

6. Persoonsgegevens verwerken

6.1 Verwerkingsgrondslagen

Het verwerken van persoonsgegevens heeft privacyrechtelijke gevolgen voor de persoon op wie de persoonsgegevens betrekking hebben ('de betrokkene'). De AVG bepaalt daarom dat persoonsgegevens alleen mogen worden verwerkt als daarvoor een goede reden bestaat. In termen van de AVG worden deze 'wettelijke grondslagen´ genoemd. In art. 6 lid 1 AVG staan er zes beschreven:
a) Je hebt toestemming van de betrokkene.
b) Het is noodzakelijk om persoonsgegevens te verwerken om een (behandel) overeenkomst uit te voeren.
c) Het is noodzakelijk om persoonsgegevens te verwerken, omdat je daartoe wettelijk verplicht bent ('wettelijke verplichting').
d) Het is noodzakelijk om persoonsgegevens te verwerken om vitale belangen van de betrokkene of van een ander persoon te beschermen.
e) Het is noodzakelijk om persoonsgegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen ('wettelijke, publieke taak').
f) Het is noodzakelijk om persoonsgegevens te verwerken om gerechtvaardigde belangen van jouzelf of een derde te behartigen die zwaarder wegen dan de belangen van de betrokkene.

De mogelijkheden om van de verschillende wettelijke grondslagen gebruik te kunnen maken worden in **>Deel C** telkens in stap 5 besproken. Grondslag (d) (bescherming van vitale belangen) komt daarnaast ook vaak terug bij stap 3 en stap 4, als het gaat over het delen van bijzondere en strafrechtelijke persoonsgegevens.

Een wettelijke verplichting (grondslag (c)) en een taak van algemeen belang of openbaar gezag ('wettelijke, publieke taak') (grondslag (e)) moet altijd een duidelijke grondslag hebben in Nederlands recht of Unierecht. Het gaat daarbij altijd om een *eigen* wettelijke verplichting of publieke taak van de verwerker. Die van de ontvanger kan géén grondslag vormen voor de verstrekking van persoonsgegevens.

Private partijen, die géén wettelijke publieke taak hebben, zullen bij het verzamelen van informatie voor signalen en meldingen en bij het indienen daarvan vaak gebruik moeten maken van grondslag (f) (gerechtvaardigd belang). Bij medische zorg aan slachtoffers zal ook grondslag (a) (toestemming) of (b) (uitvoeren (geneeskundige behandel)overeenkomst) van toepassing kunnen zijn. Hetzelfde geldt voor bijvoorbeeld advocaten die slachtoffers bijstaan. Wat mogelijk is zal steeds afhankelijk zijn van de concrete situatie.

In uitzonderlijke gevallen zal er bij de aanpak van mensenhandel sprake kunnen zijn van een beroep op de noodzaak om gegevens te verstrekken voor de bescherming van vitale belangen van de betrokkene of een ander persoon (grondslag (d)). Daarbij geldt dan dat de betrokkene zelf fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is zijn toestemming te geven. Het moet gaan om een levensbedreigende of crisissituatie, waardoor het niet als algemeen toepasselijke grondslag gebuikt kan worden.

6.2 Toestemming (grondslag (a))

Toestemming vragen van de betrokkene is niet snel de voorkeursoptie om gegevensverwerking te legitimeren. Als je hard kunt maken dat de verwerking van persoonsgegevens noodzakelijk is voor één van de onder (b) tot en met (f) genoemde doelen, is toestemming ook niet nodig. Daar komt bij dat toestemming voor met name overheidsinstanties vaak géén wettelijke grondslag kan vormen.

Om beroep op *toestemming* te kunnen doen moet deze op voldoende informatie berusten en in vrijheid, specifiek en met een ondubbelzinnige, actieve handeling zijn gegeven. Dat betekent dat betrokkenen in vrijheid hun wil moeten kunnen uiten. Ook mag er geen twijfel zijn of betrokkenen hun toestemming hebben gegeven en voor welke specifieke verwerking zij dit hebben gedaan. Bij de uitvoering van publiekrechtelijke taken, onder andere in het sociaal domein, is er vaak een afhankelijkheidsrelatie tussen de betrokkenen en overheidsinstanties. Weigeren mensen toestemming voor het verwerken van hun gegevens, dan kan dat bijvoorbeeld gevolgen hebben voor een gewenste voorziening. Daarom is er in dat soort situaties géén sprake van vrije toestemming in de zin van de AVG. Toestemming kan dan dus niet gelden als de grondslag voor de gegevensverwerking.

Belangrijk is verder dat toestemming alleen een grondslag vormt voor de eigen persoonsgegevens van de betrokkene. Voor het verstrekken van persoonsgegevens over een derde (bijvoorbeeld een dader) kan het géén toereikende grondslag vormen. Het verstrekken van persoonsgegevens van de dader zal altijd gebaseerd moeten zijn op een wettelijke verplichting (grondslag (c)) of, in het geval van een overheidsinstantie, grondslag (e) (publieke taak) dan wel, in het geval van een private partij, grondslag (f) (gerechtvaardigd belang).

6.3 Wettelijke, publieke taak (grondslag (e))

Grondslag (e) kan voor overheidsinstanties *die een daartoe strekkende wettelijke, publieke taak hebben* een basis bieden voor:

- het als meldpuntfunctie behandelen van signalen en meldingen;
- het als meldpunt- of coördinatiefunctie routeren van aan te pakken dossiers;
- het als coördinatiefunctie coördineren en afstemmen bij organisatie- en/of domeinoverstijgende dossiers;
- het verwerken van persoonsgegevens bij de uitvoering van reguliere taken en werkzaamheden zoals:
  - het bestuurlijk toezicht en de inzet van het bestuurlijk instrumentarium bij de aanpak van daders van mensenhandel;
  - het verlenen van zorg en hulp aan slachtoffers van mensenhandel en het zorgdragen voor hun fysieke veiligheid.
- het door ambtenaren en overheidsinstanties verzamelen van informatie over signalen en meldingen en het indienen van signalen en meldingen bij partijen met een meldpuntfunctie (het indienen van signalen en meldingen kan ook als er sprake is van een **>'verenigbare verdere verwerking'**).

6.4 Gerechtvaardigd belang (grondslag (f))

Voor het verstrekken van de signalen kan door private partijen, doch alleen in uitzonderlijke gevallen, op het gerechtvaardigde belang van een derde (grondslag (f)) worden teruggevallen. De gegevensverwerking moet daarbij dan *noodzakelijk* zijn om dat belang te behartigen. Het kan daarbij gaan om het gerechtvaardigde belang van het slachtoffer, het algemene belang dat mensenhandel zoveel mogelijk moet worden voorkomen (ten aanzien waarvan de beoogde ontvanger dan wel een **>wettelijke, publieke taak** moet uitvoeren) of het specifieke belang van de ontvanger (bijvoorbeeld de registratie van dergelijke meldingen). De *Autoriteit Persoonsgegevens* zegt hierover:

> "Het belang zelf moet wel steeds echt, concreet en rechtstreeks zijn. En dus niet speculatief, toekomstig of afgeleid. Maar dat kan in beginsel ieder materieel of immaterieel belang zijn.
>
> Wat *niet* als een gerechtvaardigd belang kwalificeert, is een algemeen belang van 'de samenleving' of iets dergelijks. Hierbij gaat het namelijk niet om een echt, concreet en rechtstreeks gerechtvaardigd belang van de verwerkingsverantwoordelijke of derde. Het is dan aan de wetgever om daarin te voorzien met concrete wetgeving."

De verstrekking kan bovendien alleen plaatsvinden als het gerechtvaardigde belang zwaarder weegt dan de belangen van de betrokkene. Dit houdt in dat deze grondslag niet gebruikt kan worden als de belangen, rechten en fundamentele vrijheden van de betrokkene (hier: het slachtoffer of de daders waarover gegevens verstrekt worden) zwaarder wegen dan het belang om (mogelijke) slachtoffers te beschermen en de belangen die de ontvangende partij heeft. Bij de belangenafweging kijk je naar:

- de gevolgen voor de betrokkenen;
- hoe ernstig de inbreuk is op de privacy van de betrokkenen;
- welke (aanvullende) maatregelen je hebt genomen om ongewenste gevolgen voor de betrokkenen te voorkomen of beperken;
- of de betrokkenen de verwerking min of meer kunnen verwachten, bijvoorbeeld als vervolg op een eerdere verwerking waarvoor zij toestemming hebben gegeven of als vervolg op verwerkingen die noodzakelijk zijn om een contract uit te voeren.

> Wil je persoonsgegevens verwerken van kinderen (jonger dan 16 jaar)? Dan weegt het gerechtvaardigde belang minder snel op tegen hun rechten en fundamentele vrijheden.

Uitganspunt blijft overigens dat, waar mogelijk, de betrokkene om **>toestemming** voor het delen van de informatie wordt gevraagd.

> Vanwege het feit dat de wetgever de rechtsgrond bepaalt voor de verwerking van persoonsgegevens door overheidsinstanties, is de rechtsgrond 'gerechtvaardigd belang' niet van toepassing op verwerkingen door overheidsinstanties in het kader van de uitvoering van hun taken.

6.5 Recht om bezwaar te maken tegen de verwerking op grond van grondslag (e) en (f)

Bij een verwerking op basis van grondslag (e) (wettelijke, publieke taak) of (f) (gerechtvaardigd belang) heeft de betrokkene het recht om bezwaar te maken tegen de verwerking van zijn persoonsgegevens. De verwerking moet dan worden gestaakt, tenzij er dwingende gerechtvaardigde gronden voor de verwerking zijn die zwaarder wegen dan de belangen, rechten en fundamentele vrijheden van de betrokkene. Bijvoorbeeld wanneer de verwerking noodzakelijk is voor de opsporing van strafbare feiten (zie art. 23 AVG).

6.6 Persoonsgegevens voor andere doelen verstrekken ('verder verwerken') dan waarvoor ze oorspronkelijk verzameld zijn

Een organisatie mag op grond van het 'doelbindingsbeginsel' niet zomaar persoonsgegevens verstrekken aan personen of partijen binnen of buiten de eigen organisatie. In termen van de AVG heet dat 'verder verwerken'. Persoonsgegevens moeten namelijk worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen vervolgens niet zomaar voor *andere* doeleinden worden gebruikt (art. 5 lid 1, aanhef en onder b, AVG).

⚠ Het intern hergebruik van gegevens voor andere doelen en het verstrekken van gegevens aan 'derden' dient vanuit de AVG op dezelfde wijze beoordeeld te worden. Als we in deze handreiking kortheidshalve spreken over het verstrekken aan derden voor 'verdere verwerking' van de gegevens door de ontvanger, dan geldt hetzelfde dus ook voor het intern hergebruik voor andere doelen.

Bij de aanpak van mensenhandel zal juist vaak sprake zijn van het verder verwerken van gegevens voor andere doelen dan waarvoor ze eerder verzameld zijn. Er zijn namelijk weinig specifieke wettelijke bepalingen die partijen opdragen tot:

- het (intern) opstellen van een signaal of melding over (mogelijke) mensenhandel;
- het zenden van een signaal of melding over (mogelijke) mensenhandel aan een aangewezen meldpuntfunctie;
- het (op verzoek) verstrekken van gegevens aan partijen met een meldpunt- of coördinatiefuncties voor de aanpak van mensenhandel.

De AVG onderscheidt de volgende situaties waarin het verder verwerken van persoonsgegevens voor andere doeleinden tóch is toegestaan (art. 6 lid 4 AVG):

- Er is toestemming van de betrokkene.
- Er is een Nederlands recht of Unierecht dat het verder verwerken zonder toestemming mogelijk maakt en die "in een democratische samenleving een noodzakelijke en evenredige maatregel vormt" voor de waarborging van *de in art. 23 lid 1 AVG vermelde doelen*. ⊕ Gedacht kan worden aan *de aangiftebevoegdheid* ⊕ van art. 161 Wetboek van Strafvordering.
- De verdere verwerking past binnen de vijf 'verenigbaarheidscriteria´ en is daardoor in termen van de AVG 'verenigbaar' met het oorspronkelijke doel.

Deze vijf verenigbaarheidscriteria zijn:

1. *Ieder verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking.* Hierbij speelt mee of de verschillende doeleinden voldoende bij elkaar passen. Hoe groter de verwantschap, hoe sneller gezegd zal kunnen worden dat sprake is van een verenigbaar doel. Als bijvoorbeeld in het kader van gemeentelijk toezicht op de prostitutiebranche wordt gestuit op een signaal van mensenhandel en dit signaal wordt verstrekt aan de politie, omdat het signaal ook strafrechtelijk relevant is, zal sneller sprake zijn van verwantschap dan wanneer een zorgverlener bij de behandeling van een patiënt op de hoogte raakt van mensenhandel en dit signaal verstrekt aan de politie, temeer omdat hierbij ook het medisch beroepsgeheim van de zorgverlener in beeld komt.
2. *Het kader waarin de persoonsgegevens zijn verzameld, met name wat de verhouding tussen de betrokkenen en de verwerkingsverantwoordelijke betreft.* Als het bijvoorbeeld gaat om een verdere verwerking van gegevens die verplicht verstrekt moesten worden aan de partij die die gegevens nu verder wil verwerken, zijn daar minder mogelijkheden toe.
3. *De aard van de persoonsgegevens, met name of bijzondere persoonsgegevens of persoonsgegevens over strafrechtelijke veroordelingen en strafbare feiten worden verwerkt.* Hoe gevoeliger de persoonsgegevens zijn, hoe minder snel sprake zal zijn van verwantschap. Bijzondere persoonsgegevens (waaronder medische gegevens) en strafrechtelijke gegevens zijn naar hun aard gevoelig. Gegevens kunnen ook gevoelig zijn door de context waarin ze worden gebruikt.

4. *De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen.* Als gegevens voor bijvoorbeeld sanctionering worden verstrekt, heeft dat grotere gevolgen dan als de gegevens worden verstrekt voor hulpverlening aan een slachtoffer.
5. *Het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.* Welke waarborgen passend zijn zal per concreet geval moeten worden beoordeeld. Het kan zijn dat de betrokkene over het voorgenomen gebruik wordt geïnformeerd, dan wel – een stap verder – in de gelegenheid wordt gesteld om bezwaar te maken. In de AVG worden ook het versleutelen of pseudonimisering van persoonsgegevens als passende waarborgen genoemd. Het versleutelen of pseudonimisering van de te verstrekken gegevens is bij de aanpak van mensenhandel veelal géén optie: dan weet de ontvanger van de gegevens niet op welke persoon deze betrekking hebben.

Bij de beoordeling of sprake is van verenigbaar gebruik speelt ook de redelijke verwachting van de betrokkene een rol: kan deze de verdere verwerking redelijkerwijs verwachten? Daarnaast moet steeds worden gekeken of de sectorale regelgeving op grond waarvan de persoonsgegevens zijn verkregen aan de verdere verwerking in de weg staat, bijvoorbeeld als die wet een bijzondere geheimhoudingsplicht bevat of anderszins is bepaald dat de gegevens niet voor andere doelen mogen worden gebruikt dan voor de uitvoering van de wettelijke, publieke taak die de verstrekker of ontvanger op grond van die bijzondere wet heeft. Het is namelijk mogelijk dat de wettelijke regeling een 'strikte doelbinding' bevat. Dit houdt in dat de regeling specifiek benoemt voor welke doeleinden of welke taken en werkzaamheden de gegevens verder verwerkt en verstrekt mogen worden. Bij bijzondere persoonsgegevens is hier zelfs vrijwel altijd sprake van.

Het argument dat het verstrekken van signalen voor het kunnen bieden van bescherming of zorg- en hulpverlening *altijd* als verenigbare verwerking valt aan te merken omdat dit *ten gunste* van het slachtoffer kan zijn, gaat niet op.

De mogelijkheden om persoonsgegevens verder te verwerken worden in **>Deel C** telkens in stap 6 besproken.

Onder de Wet bescherming persoonsgegevens (Wbp), de voorloper van de AVG, was het mogelijk het doelbindingsbeginsel buiten toepassing te laten als de verstrekking noodzakelijk was voor bijvoorbeeld de voorkoming, opsporing en vervolging van strafbare feiten (art. 43 Wbp). De Uitvoeringswet AVG (UAVG) bevat geen vergelijkbare bepaling. Direct gevolg daarvan is dat in veel gevallen de verstrekking alleen kan plaatsvinden als aan de hand van de verenigbaarheidscriteria wordt vastgesteld dat de beoogde verstrekking verenigbaar is.

6.7 Het beginsel van noodzakelijkheid

De grondslagen (b) tot en met (f) zijn 'noodzakelijkheidsgrondslagen': de verwerking is alleen gerechtvaardigd als dit noodzakelijk is voor de in deze grondslagen genoemde doelen (art. 5 lid 1, aanhef en onder c, AVG). In deze vraag ligt besloten dat de verwerking van gegevens proportioneel moet zijn en dat er voldaan moet zijn aan de eis van subsidiariteit.

Proportio-naliteit	De afweging tussen middel (het verwerken van persoonsgegevens) en doel (de werkzaamheden waarvoor de gegevens gebruikt worden). Dit betreft de vraag naar effectiviteit en evenredigheid. Als je met de verwerking van de gegevens niet het gestelde doel kunt bereiken of wanneer dat zeer onwaarschijnlijk is, is de verwerking niet snel proportioneel. Het tweede element van de proportionaliteitstoets betreft de evenredigheid. Het doel dat wordt nagestreefd moet in verhouding staan tot het feit waarvoor persoonsgegevens moeten worden verwerkt. Ook de omvang en de aard van de persoonsgegevens moeten zijn beperkt tot het strikt noodzakelijke. Dit houdt onder meer in dat de verstrekking moet worden beperkt tot '*need to know*'-informatie, in plaats van '*nice to know*'-informatie.
Subsidiariteit	Subsidiariteit betreft de vraag of het genoemde doel niet op een andere, minder ingrijpende wijze kan worden bereikt (bijvoorbeeld door geen of minder persoonsgegevens te verwerken). Zo ja, dan dient voor dit minder ingrijpende alternatief te worden gekozen. Voor een dergelijke afweging zijn de volgende factoren van belang: • De aard van de gegevens en de ernst van de situatie waarop deze betrekking hebben. Bij aanwijzingen dat er ernstige feiten spelen, zal informatie eerder mogen worden gedeeld. • De ernst van de inbreuk die op de persoonlijke levenssfeer van de betrokkene wordt gemaakt. Daarbij is onder meer relevant: - de vraag in hoeverre een compleet beeld van de betrokkene ontstaat; - in hoeverre een betrokkene negatieve gevolgen zal ondervinden van de verstrekking - de aard van de gegevens (hoe gevoeliger, hoe terughoudender ermee moet worden omgegaan), en - of een betrokkene zich effectief kan verweren tegen de verstrekking (bijvoorbeeld mogelijkheden tot rechtsbescherming). Bij alternatieven kan bijvoorbeeld gedacht worden aan alleen het verstrekken van zogenaamde '*dat-informatie*' ⊕ of '*uitwendige- of buitenkant-informatie*'. ⊕ Hierbij is overigens van belang dat 'dat-informatie' en 'uitwendige- of buitenkant-informatie' nog steeds kunnen kwalificeren als **>bijzondere persoonsgegevens**.

⚠ Bij het verstrekken van gegevens wordt vaak de vraag gesteld of een bepaald document, zoals een proces-verbaal door de politie aan een andere partij verstrekt mag worden. Dit is onvoldoende precies. Het gaat bij het noodzakelijkheidsbeginsel nadrukkelijk om een afweging *welke gegevens* verstrekt mogen worden. Hetzelfde geldt ook bij de verwerking van politiegegevens en justitiële en strafvorderlijke gegevens.

7. Geheimhoudingsverplichting en andere beperkingen

7.1 Wanneer geldt een geheimhoudingsverplichting?

De AVG bevat geen *algemene* bepaling over geheimhouding. En ook geen verplichting voor lidstaten of organisaties om zelf algemene geheimhoudingsverplichtingen te introduceren.

De AVG bevat wél een *specifieke* bepaling over geheimhouding. Bijzondere persoonsgegevens mogen alleen worden verwerkt voor medische diagnoses en gezondheidszorg als dit plaatsvindt onder de verantwoordelijkheid van een beroepsbeoefenaar die aan het beroepsgeheim is gebonden of tot geheimhouding is verplicht (art. 9 lid 3 AVG). Alle personen die op grond van *art. 30 Uitvoeringswet AVG (UAVG)* ⊕ gezondheidsgegevens mogen verwerken, zijn bovendien gebonden aan hun medisch beroepsgeheim of wettelijke geheimhoudingsplichten. Voor de personen die op grond van art. 30 UAVG gezondheidsgegevens mogen verwerken, maar niet gebonden zijn aan een beroepsgeheim of geheimhoudingsplicht, geldt een vergelijkbare geheimhouding (art. 30 lid 4 UAVG). Deze geheimhoudingsplicht is niet alleen beperkt tot zorgverleners, maar ook bijvoorbeeld een reclasseringsinstelling.

Er zijn ook diverse *wettelijke* geheimhoudingsplichten. Deze zijn vaak opgenomen in de sectorale regelgeving van specifieke sectoren of beroepsgroepen. Een relevante geheimhoudingsplicht is onder meer het medisch beroepsgeheim van zorgverleners (art. 88 Wet BIG en art. 7:457 Burgerlijk Wetboek (BW)). Het beroepsgeheim van de zorgverlener is niet beperkt tot medische informatie, maar ziet op alle informatie die de patiënt aan de zorgverlener heeft toevertrouwd. Het beroepsgeheim strekt zich eveneens uit tot de medewerkers van de zorgverlener (zoals assistenten en secretaresses). Voor hen geldt een zogenaamd **>afgeleid beroepsgeheim**. Ander voorbeelden zijn de geheimhoudingsplichten van de Wet maatschappelijke ondersteuning 2015 (Wmo 2015) en de Jeugdwet (art. 5.3.3 lid 1 Wmo 2015 en art. 7.3.11 lid 1 Jeugdwet).

Daarnaast bevat de Algemene wet bestuursrecht een algemene geheimhoudingsplicht (art. 2:5). Deze rust op iedereen die als (onderdeel van een) bestuursorgaan of als daarvoor werkzame persoon (in welke rechtsverhouding ook) in aanraking komt met vertrouwelijke gegevens. Daarnaast rust de geheimhoudingsplicht ook op adviesorganen die door een bestuursorgaan worden betrokken bij de uitvoering van zijn taak, evenals daartoe behorende of daarvoor werkzame personen. Deze geheimhoudingsplicht houdt in dat zij ten aanzien van die vertrouwelijke informatie verplicht zijn tot geheimhouding, tenzij de verstrekking:

- - wettelijk verplicht is, of
- - de verstrekking noodzakelijk is voor de uitvoering van de wettelijke, publieke taak van het bestuursorgaan.

Uitgangspunt daarbij is dat als er sprake is van een **>'verenigbare verdere verwerking'**, de geheimhoudingsplicht geen beletsel vormt voor de verdere verstrekking van de persoonsgegevens, mits de ontvanger zelf ook beschikt over een *eigen* wettelijke grondslag om de persoonsgegevens te verwerken.

Een geheimhoudingsplicht kan alleen worden doorbroken als daarvoor een expliciete wettelijke grondslag bestaat (een zogenoemde 'doorbrekingsgrond'). Pas als de wettelijke geheimhoudingsplicht is doorbroken, wordt toegekomen aan de vraag of er zo nodig ook een doorbrekingsgrond is voor de verstrekking van **>bijzondere persoonsgegevens** in algemene zin (art. 9 AVG) en een **>wettelijke grondslag** voor de verwerking van de persoonsgegevens (art. 6 AVG).

De mogelijkheden om geheimhoudingsplichten te doorbreken worden in **>Deel C** telkens in stap 2 besproken.

7.2 Geheimhoudingsverplichtingen en strikte doelbindingen op basis van eigen beleid voor verwerkingsverantwoordelijke

Er is in de praktijk ook regelmatig sprake van eigen beleid en vrijwillig zelf geformuleerde geheimhoudingsverplichtingen en strikte doelbindingen. Bijvoorbeeld:

- De verwerkingsverantwoordelijke neemt zelf in een protocol, reglement, privacystatement, interne instructie of arbeidsovereenkomst een 'bovenwettelijke' geheimhoudingsverplichting of strikte doelbinding op.
- In een gedrags- of beroepscode van een bepaalde beroepsgroep staat een 'bovenwettelijke' geheimhoudingsverplichting of strikte doelbinding.
- In een samenwerkingsovereenkomst of convenant staat een door meerdere partijen vastgestelde 'bovenwettelijke' geheimhoudingsverplichting of strikte doelbinding.

De beperkingen die worden aangebracht gaan vaak verder dan nodig (en soms zelfs beoogd). Ook is er soms sprake van onduidelijke formuleringen. Dit leidt tot een situatie waarbij men gegevens niet mag of durft te verstrekken. Het is dan zinvol om deze beperkingen tegen het licht te houden. De beperkingen kunnen wellicht weggenomen worden.

7.3 Aanvullende voorwaarden

Het is mogelijk dat bij het verstrekken van gegevens aanvullende voorwaarden worden gesteld die op de persoonsgegevens blijven rusten. Voorbeelden van dergelijke voorwaarden zijn:

- Je dient contact op te nemen met de eerdere verstrekker of je dient je in de positie van die eerdere verstrekker te verplaatsen.
- Verstrekking is alleen mogelijk als dat wettelijk verplicht is.
- Je hebt toestemming nodig van de eerdere verstrekker.

8. Bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens

8.1 Verwerken van bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn vanwege hun aard gevoelig en krijgen daarom extra bescherming in de AVG. De verwerking van bijzondere persoonsgegevens is verboden, tenzij er een specifieke wettelijke bepaling bestaat in Nederlands recht of Unierecht die het gebruik van dergelijke gegevens toch mogelijk maakt (art. 9 lid 2 AVG). Ook dit wordt een 'doorbrekingsgrond' genoemd. Deze zijn nader uitgewerkt in de artikelen 22 tot en met 30 Uitvoeringswet AVG (UAVG).

>Wat zijn bijzondere persoonsgegevens?

Er zijn doorbrekingsgronden waar bij de aanpak van mensenhandel – sommige alleen bij hoge uitzondering – een beroep op gedaan kan worden:

- De betrokkene geeft *uitdrukkelijke* toestemming (art. 9 lid 2, aanhef en onder a, AVG jo art. 22 lid 2, aanhef en onder a, UAVG).
- De verwerking is nodig voor de bescherming van de vitale belangen van de betrokkene of van een ander persoon, terwijl de betrokkene fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is om toestemming te geven (art. 9 lid 2, aanhef en onder c, AVG jo art. 22 lid 2, aanhef en onder b, UAVG).
- Het gaat om gegevens die door de betrokkene kennelijk openbaar gemaakt zijn (art. 9 lid 2, aanhef en onder e, AVG jo art. 22 lid 2, aanhef en onder d, UAVG).

Bij het verzamelen, verwerken en delen van signalen van mensenhandel zal hier eerder bij uitzondering sprake van zijn.

> *Uitdrukkelijke* toestemming is een verzwaarde vorm van de 'normale', ondubbelzinnige toestemming van art. 6 AVG. De term 'uitdrukkelijk' verwijst naar de manier waarop de betrokkene zijn toestemming tot uitdrukking brengt: met een uitdrukkelijke verklaring van toestemming. Verder gelden voor *uitdrukkelijke* toestemming **>dezelfde eisen** als voor 'normale', ondubbelzinnige toestemming.

Verwerken van bijzondere persoonsgegevens is ook mogelijk als Nederlands recht of Unierecht dit mogelijk maakt in verband met:

- Het sociale zekerheids- en sociale beschermingsrecht. Hier gaat het bijvoorbeeld om het gebruik van gegevens over de gezondheid en andere bijzondere gegevens, als dit nodig is voor de uitvoering van sociale zekerheidsvoorzieningen (art. 9 lid 2, aanhef en onder b, AVG).
- Redenen van zwaarwegend algemeen belang (zoals de aanpak van mensenhandel), waarbij passende en evenredige maatregelen zijn getroffen voor de bescherming van de belangen van de betrokkene (art. 9 lid 2, aanhef en onder g, AVG). Hier gaat het bijvoorbeeld om:
  - de verwerking van bijzondere persoonsgegevens, als dit nodig is voor het uitvoeren van internationaalrechtelijke verplichtingen (art. 23, aanhef en onder a, UAVG);
  - de mogelijkheid om gegevens over de gezondheid te verwerken voor onder andere de reclassering, de Raad voor de Kinderbescherming en gecertificeerde instellingen (art. 30 lid 2 UAVG);
  - de verwerking van bijzondere persoonsgegevens, als dit *noodzakelijk* is in aanvulling op de verwerking van strafrechtelijke persoonsgegevens (art. 23, aanhef en onder c, UAVG).
- Gezondheidszorg of sociale dienstverlening. Hier gaat het bijvoorbeeld om het gebruik van gegevens over de gezondheid (zie bijvoorbeeld art. 30 lid 3 UAVG). Het gaat in deze situatie om strafrechtelijke gegevens die gelijktijdig ook een bijzonder persoonsgegeven vormen over de betrokkene of daarmee

strikt verband houden. De wetgever noemt als voorbeeld het verwerken van incidenten van seksuele intimidatie op de werkvloer (zowel een bijzonder gegeven over iemands seksuele leven als een strafrechtelijk gegeven). Voor wat betreft mensenhandel zou kunnen worden gedacht aan de situatie dat een burgemeester informatie ontvangt over een slachtoffer van mensenhandel dat tevens iets zegt over het strafrechtelijke delict dat tegen het slachtoffer is gepleegd.

De mogelijkheden voor het verwerken van bijzondere persoonsgegevens worden in **>Deel C** telkens in stap 3 besproken.

8.2 Verwerken van strafrechtelijke persoonsgegevens

Strafrechtelijke persoonsgegeven mogen alleen worden verwerkt onder toezicht van de overheid of als dat is toegestaan op grond van Nederlands recht of Unierecht dat passende waarborgen voor de rechten en vrijheden van de betrokkene biedt (art. 10 AVG).

>Wat zijn strafrechtelijke persoonsgegevens?

Voor zorgverleners en private partijen zal er nooit sprake van zijn dat zij strafrechtelijke persoonsgegevens verwerken 'onder toezicht van de overheid'. Alleen de overheid mag namelijk een omvattende registratie van strafrechtelijke veroordelingen en strafbare feiten bijhouden. Dit maakt dat zij zich op één van de nationale uitzonderingsbepalingen moeten kunnen beroepen. Deze zijn nader uitgewerkt in de artikelen 31 tot en met 33 UAVG.

De UAVG bevat een aantal algemene grondslagen waar bij de aanpak van mensenhandel – sommige alleen bij hoge uitzondering – een beroep op gedaan zou kunnen worden:

- De betrokkene geeft *uitdrukkelijke* toestemming (art. 32, aanhef en onder a, UAVG.
- De verwerking is nodig voor de bescherming van de vitale belangen van de betrokkene of van een ander persoon, terwijl de betrokkene fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is om toestemming te geven (art. 32, aanhef en onder b, UAVG).
- Het gaat om gegevens die door de betrokkene kennelijk openbaar gemaakt zijn (art. 32, aanhef en onder c, UAVG).

Bij het verzamelen, verwerken en delen van signalen van mensenhandel zal hier eerder bij uitzondering sprake van zijn.

Daarnaast bevat de UAVG ook nog enkele specifieke wettelijke grondslagen voor de verwerking van strafrechtelijke gegevens. Voor de aanpak van mensenhandel zijn met name de volgende grondslagen van belang:

- De verwerking van strafrechtelijke gegevens vindt plaats door een orgaan dat wettelijk belast is met de toepassing van het strafrecht (bijvoorbeeld de Raad voor de Kinderbescherming in strafzaken en de reclassering; art. 33 lid 1, aanhef en onder a, UAVG).
- De strafrechtelijke gegevens zijn verkregen op grond de Wet politiegegevens (Wpg) of de Wet justitiële en strafvorderlijke gegevens (Wjsg) (bijvoorbeeld doordat de politie of het Openbaar Ministerie (OM) deze gegevens heeft verstrekt aan de burgemeester, voor de uitvoering van diens taken; art. 33 lid 1, aanhef en onder a, UAVG).
- De strafrechtelijke gegevens worden door of voor een samenwerkingsverband (bijvoorbeeld het RIEC, het Veiligheidshuis of het Expertisecentrum Mensenhandel en Mensensmokkel (EMM)) verwerkt (art. 33 lid 1, aanhef en onder b, UAVG). Daarbij gelden de volgende twee voorwaarden:
  1. De verwerking is noodzakelijk voor het uitvoeren van de taak van het samenwerkingsverband.
  2. Bij de uitvoering van de samenwerking wordt voorzien in zodanige waarborgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.

Voor hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening is relevant dat strafrechtelijke gegevens ook mogen worden verwerkt in aanvulling op gezondheidsgegevens, als dat

noodzakelijk is met het oog op een goede behandeling of verzorging van de betrokkene (art. 33 lid 1, aanhef en onder c, UAVG).

Tot slot mogen strafrechtelijke persoonsgegevens ten behoeve van derden worden verwerkt als de Autoriteit Persoonsgegevens daarvoor een vergunning heeft verleend (art. 33 lid 4, aanhef en onder c, jo. lid 5 UAVG). Hierbij kan bijvoorbeeld worden gedacht aan vergunningen voor het verwerken van zwarte lijsten door brancheorganisaties. Voor zover bekend heeft de Autoriteit Persoonsgegevens nog nooit een vergunning verleend voor het verwerken van strafrechtelijke persoonsgegevens gerelateerd aan mensenhandel.

De mogelijkheden voor het verwerken van strafrechtelijke persoonsgegevens worden in **>Deel C** telkens in stap 4 besproken.

9. Gegevensverwerking voor de opsporing en vervolging van strafbare feiten en het tenuitvoerleggen van (strafrechtelijke) straffen

De gegevensverwerking in het opsporingsdomein is geregeld in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Dat regime biedt de politie, de Koninklijke Marechaussee (*voor zover het politietaak betreft*), bijzondere opsporingsdiensten zoals de Inspectie SZW - Directie Opsporing (*ISZW-DO*) en buitengewoon opsporingsambtenaren (boa's) het kader voor gegevensverwerking bij de opsporing en vervolging van strafbare feiten, de tenuitvoerlegging van strafrechtelijke beslissingen en de bescherming en de voorkoming van gevaren voor de openbare veiligheid. Het is met name de Wpg die binnen het opsporingsdomein het kader biedt voor de fase waarin signalen en meldingen worden verzameld, verwerkt en gedeeld.

Hetgeen eerder is opgemerkt over het vereiste van noodzaak en de rol en betekenis van geheimhoudingsverplichtingen is hier ook van toepassing.

>Lees meer over het noodzakelijkheidsbeginsel

>Lees meer over geheimhoudingsplichten en beroepsgeheim

9.1 Wet politiegegevens

Voor de partijen in het opsporingsdomein is de gegevensverwerking voor de voorkoming en opsporing van mensenhandel geregeld in de Wpg. De Wpg heeft een zogenoemd 'gesloten verstrekkingsregime', waarbij de mogelijkheden om politiegegevens te verstrekken uitputtend zijn geregeld. De Wpg regelt zo strikt aan wie en voor welke doeleinden politiegegevens mogen worden verstrekt.
De Wpg maakt hierbij een onderscheid tussen de verstrekking van politiegegevens tussen opsporingsinstanties *onderling* en aan derden. De Wpg gaat uit van een systeem van 'free flow of information' tussen de partijen in het opsporingsdomein.

Verwerken van politiegegevens
Politiegegevens kunnen onder andere verwerkt worden als dat noodzakelijk is voor de uitvoering van de dagelijkse politietaak (art. 8 Wpg). Ook kunnen ze gericht worden verwerkt voor concrete onderzoeken met het oog op de handhaving van de rechtsorde, de 'grotere rechercheonderzoeken' (art. 9 Wpg).

Voor het verwerken van politiegegevens is verder relevant de regeling voor het **>Themaregister Mensenhandel** (art. 10 lid 1, aanhef en onder b, Wpg). Met het Themaregister Mensenhandel is het mogelijk om situaties waarbij er eventueel sprake zou kunnen zijn van mensenhandel te onderzoeken. Het hoeft hierbij nog niet te gaan om verdachten in de zin van art. 27 Wetboek van Strafvordering of om personen ten aanzien van wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het beramen of plegen van zware misdrijven of georganiseerde criminaliteit zoals bedoeld in art. 10 lid 2 Wpg. Het gaat om gegevens die op zichzelf staand onvoldoende feitelijk zijn om daarop het vermoeden te baseren dat bepaalde personen betrokken zijn bij handelingen die kunnen wijzen op het beramen of plegen van mensenhandel. Het verkrijgen van zicht hierop noodzaakt ertoe om over langere perioden 'laagwaardige' gegevens te verwerken. Pas na analyse en het samenvoegen van verschillende van deze zachte signalen, kan worden bezien of er inderdaad sprake is van mensenhandel en kan verder onderzoek ertoe leiden dat bepaalde personen in beeld komen als betrokkene bij het beramen of plegen van het misdrijf.

De Wpg biedt de partijen in het opsporingsdomein ook de mogelijkheid om bijzondere politiegegevens te verwerken. Het gaat daarbij om politiegegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijkt. En om genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, of gegevens over gezondheid, seksuele leven en seksuele gerichtheid. Ze mogen deze bijzondere politiegegevens verwerken én verstrekken aan derden, in aanvulling op de verwerking van 'normale' politiegegevens, als dat voor het doel van de verwerking *onvermijdelijk* is en de gegevens afdoende zijn beveiligd (art. 5 Wpg).

Verstrekken van politiegegevens

Art. 7 lid 1 Wpg bepaalt dat er een geheimhoudingsplicht rust op politiegegevens, maar dat:

- gegevens verstrekt kunnen worden als dat verplicht is;
- de bepalingen van paragraaf 3 Wpg verstrekking toestaan;
- de politietaak het verstrekken in een bijzonder geval noodzakelijk maakt.

Zie **>paragraaf 10.2, stap 2** voor verschillende voorbeelden.

Ook de ontvanger van de politiegegevens is verplicht tot geheimhouding van de politiegegevens. De ontvanger mag deze geheimhouding alleen doorbreken als hij wettelijk verplicht is de politiegegevens te verstrekken of als dit noodzakelijk is om zijn taak uit te voeren (art. 7 lid 2 Wpg).

Voor de politie gelden op grond van de Wpg de volgende vuistregels bij het verstrekken van gegevens:

a) Er is een specifieke bepaling over verstrekken in de Wpg (waaronder bijvoorbeeld het verstrekken van politiegegevens voor een **>samenwerkingsverband op grond van een convenant**).
b) Er is een specifieke verplichting tot verstrekken in de materiewetgeving van de ontvangende partij.
c) De politietaak maakt het noodzakelijk om in bijzondere gevallen te verstrekken (zoals voor de bescherming van vitale belangen van de betrokkene).

9.2 Wet justitiële en strafvorderlijke gegevens

De Wjsg regelt onder meer de gegevensverwerking door het OM bij opsporing en vervolging en de tenuitvoerlegging van straffen. De Wjsg maakt onderscheid tussen verschillende categorieën gegevens en bevat voor die verschillende categorieën regels voor de verwerking daarvan.

Justitiële gegevens zijn bij algemene maatregel van bestuur omschreven persoonsgegevens (of gegevens over een rechtspersoon) inzake de toepassing van het strafrecht of de strafvordering die in een gegevensbestand zijn of worden verwerkt (art. 1, aanhef en onder a, Wjsg). Justitiële gegevens mogen onder andere worden verwerkt voor een goede rechtspleging. Daarmee wordt bedoeld dat de gegevens mogen worden verwerkt voor de werkzaamheden van de rechter en het OM, onder meer om de hoogte van de straf te bepalen. Daarnaast mogen justitiële gegevens worden verwerkt om vast te stellen of er nog openstaande zaken zijn waarmee de rechter of het OM bij het bepalen van

een straf(eis) rekening moeten houden, kortom het vaststellen van het strafrechtelijke verleden van de verdachte.

Strafvorderlijke gegevens zijn persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het OM in een strafdossier of langs geautomatiseerde weg in een gegevensbestand verwerkt (art. 1, aanhef en onder b, Wjsg). Hoofdregel is dat strafvorderlijke gegevens worden verwerkt als dat noodzakelijk is voor en goede vervulling van de taak van het OM of het nakomen van een andere wettelijke verplichting.

Tenuitvoerleggingsgegevens zijn alle persoonsgegevens of gegevens over een rechtspersoon inzake de tenuitvoerlegging van strafrechtelijke beslissingen die worden verwerkt in een dossier of een ander gegevensbestand (art. 1, aanhef en onder d, Wjsg). Een voorbeeld van tenuitvoerleggingsgegevens zijn de persoonsgegevens die door het Centraal Justitieel Incassobureau (CJIB) namens de minister wordt verwerkt, als het gaat om het innen van strafbeschikkingen. Geen tenuitvoerleggingsgegevens zijn persoonsgegevens die worden verwerkt voor de tenuitvoerlegging van een andere dan een strafrechtelijke beslissing, zoals voor de inning van een opgelegde bestuurlijke boete.

Gerechtelijke strafgegevens zijn alle persoonsgegeven of gegevens van rechtspersonen die zijn verkregen in het kader van het behandelen en beslissen van zaken waarop het Nederlandse strafrecht van toepassing is en die in een gegevensbestand zijn of worden verwerkt (art. 1, aanhef en onder e, Wjsg).

Voor strafvorderlijke gegevens, justitiële gegevens, tenuitvoerleggingsgegevens en gerechtelijke strafgegevens gelden afzonderlijke verwerkingsgrondslagen binnen de Wjsg. Gemakshalve ligt de focus in het verdere deel op de verstrekking van justitiële gegevens door de minister Justitie en Veiligheid en strafvorderlijke gegevens door het OM.

Verwerken (waaronder verstrekken) van justitiële gegevens
De minister van Justitie en Veiligheid is de verwerkingsverantwoordelijke voor justitiële gegevens (art. 1, aanhef en onder k, Wjsg). Het verstrekken van justitiële gegevens is geregeld in de artikelen 8 tot en met 15 Wjsg. Het verstrekken van justitiële gegevens is onder meer toegestaan als:

a) Er een specifiek bepaling is over het verstrekken in de Wjsg (zie met name art. 8 Wjsg jo. art. 11 tot en met art. 31 Besluit justitiële en strafvorderlijke gegevens).
b) Iedereen die op grond van de Wjsg de beschikking krijgt over gegevens met betrekking tot een derde, is gebonden aan geheimhouding, behoudens als een wettelijk voorschrift mededelingen toelaat, dan wel de uitvoering van de taak met het oog waarop de gegevens zijn verstrekt tot het ter kennis brengen daarvan noodzaakt (art. 52 lid 1 Wjsg).

Verwerken van strafvorderlijke gegevens
Het College van procureurs-generaal van het OM is de verwerkingsverantwoordelijke voor strafvorderlijke gegevens (art. 39a Wjsg). Het OM mag strafvorderlijke persoonsgegevens verwerken als dit noodzakelijk is voor de goede vervulling van de taak van het OM (waaronder de opsporing en vervolging van daders van mensenhandel of het nakomen van een andere wettelijke verplichting (art. 39b lid 1 Wjsg)). Het verwerken van bijzondere persoonsgegevens is geregeld in art. 39c lid 3 Wjsg.

Verstrekken van justitiële en strafvorderlijke gegevens
Voor het OM gelden op basis van de Wjsg de volgende algemene vuistregels voor het verstrekken van gegevens:

a) Er is een specifieke bepaling over het verstrekken in de bij of krachtens de Wjsg gestelde regels.
b) Iedereen die op grond van de Wjsg de beschikking krijgt over gegevens met betrekking tot een derde, is gebonden aan geheimhouding, behoudens als een wettelijk voorschrift mededelingen toelaat, dan wel als de uitvoering van de taak met het oog waarop de gegevens zijn verstrekt tot het ter kennis brengen daarvan noodzaakt (art. 52 lid 1 Wjsg).

Het OM kan bij de opsporing en vervolging van daders van mensenhandel persoonsgegevens met opsporingsambtenaren en -instanties uitwisselen op basis van art. 39e lid 1, aanhef en onder d, e en h, Wjsg. Of als het bijzondere persoonsgegevens betreft, op basis van art. 39c lid 3 Wjsg.

Voor het verstrekken van persoonsgegevens aan niet-politiële partijen met een daartoe strekkende **>wettelijke, publieke taak** (die zelf onder de AVG vallen) kan het OM gebruik maken van de mogelijkheden die art. 39f Wjsg biedt. Daarin is onder andere opgenomen dat als er sprake is van een zwaarwegend algemeen belang en als dit past bij de goede uitvoering van de taken en werkzaamheden, het OM gegevens kan verstrekken voor:

- het voorkomen en opsporen van strafbare feiten (art. 39f lid 1, aanhef en onder a);
- het handhaven van de orde en veiligheid (art. 39f lid 1, aanhef en onder b)
- het uitoefenen van toezicht op het naleven van regelgeving art. (39f lid 1, aanhef en onder c);
- het nemen van een bestuursrechtelijke beslissing (art. 39f lid 1, aanhef en onder d);
- het verlenen van hulp aan slachtoffers en anderen die bij een strafbaar feit betrokken zijn (art. 39f lid 1, aanhef en onder f).

DEEL C Gegevensverwerking in de praktijk

10. Stappenplan beoordelen gegevensverwerking

10.1 Inleiding

In **>Deel B** hebben we de algemene juridische kaders voor gegevensdeling uiteengezet en toegelicht. In de eerste plaats aan de hand van een 'spoorboekje'; de vragen die je moet stellen om te kunnen beoordelen of je in een concreet geval gegevens mag verwerken. Ook dit deel is opgebouwd aan de hand van die vragen. Aan de hand van het stappenplan hiernaast is voor een aantal categorieën en partijen een gedetailleerder en concreter overzicht gegeven van de mogelijkheden die er zijn om tot verstrekking van persoonsgegevens gegevens over te gaan. Het gaat daarbij om de volgende categorieën:

- **>politie, Koninklijke Marechaussee, bijzondere opsporingsdiensten, zoals de Inspectie SZW – Directie Opsporing, en boa's**
- **>(gemeentelijke) toezichthouders, waaronder de Inspectie SZW, en de gemeente voor bepaalde andere taken**
- **>zorgverleners, aanbieders en hulpverleners met een medisch beroepsgeheim (reguliere zorg en sociaal domein) én zonder een medisch beroepsgeheim (sociaal domein)**
- **>publieke en private partijen met een meldpunt- of coördinatiefunctie, waaronder Veilig Thuis, de zorgcoördinator en de aandachtsfunctionaris mensenhandel**
- **>niet-strafrechtelijke partners binnen de vreemdelingenketen, waaronder de IND, de Koninklijke Marechaussee en het COA**

1	Is de AVG of de Wet politiegegevens (Wpg) van toepassing op de verstrekking?
2	Vallen de persoonsgegevens onder een geheimhoudingsplicht en zo ja, kan deze worden doorbroken?
3	Als er bijzondere persoonsgegevens worden verstrekt, is er een wettelijke grondslag die het verbod om bijzondere persoonsgegevens te verwerken doorbreekt?
4	Als er strafrechtelijke persoonsgegevens verstrekt worden, is daar een wettelijke grondslag voor?
5	Kan de verstrekking van de persoonsgegevens worden gebaseerd op een wettelijke grondslag?
6	Staat het doelbindingsbeginsel de verstrekking ('verdere verwerking') van de persoonsgegevens toe?
7	Wordt er niet meer verstrekt dan de strikt noodzakelijke persoonsgegevens (need to know, in plaats van nice to know)?
8	Moet de betrokkene worden geïnformeerd over de verstrekking of bestaat daarop een uitzondering?

Uit het oogpunt van de leesbaarheid is ervoor gekozen in dit deel alleen die artikelverwijzingen op te nemen die een aanvulling of concretisering zijn van het algemene juridische kader dat in **>Deel B** uiteengezet en toegelicht is.

10.2 Politie, Koninklijke Marechaussee, bijzondere opsporingsdiensten en boa's

In deze paragraaf gaan we in op de verstrekking van *politiegegevens* door de politie, de Koninklijke Marechaussee, bijzondere opsporingsdiensten zoals de Inspectie SZW - Directie Opsporing (ISZW-DO) en buitengewoon opsporingsambtenaren (boa's). Zowel aan het verstrekken aan andere strafrechtelijke partners (waaronder het Openbaar Ministerie (OM)) als op het verstrekken aan andere partijen (zoals zorgverleners, toezichthouders en burgemeesters). De Wet politiegegevens (Wpg) maakt hierbij een onderscheid tussen de verstrekking van politiegegevens tussen opsporingsinstanties *onderling* en aan derden. De Wpg gaat uit van een systeem van 'free flow of information' binnen het opsporingsdomein.

1 Is de AVG of de Wet politiegegevens (Wpg) van toepassing op de verstrekking?

Politie

Het verwerken van *politiegegevens* door de politie voor de uitvoering van de politietaak valt onder het regime van de Wpg. Datzelfde geldt voor het verwerken van politiegegevens door bijzondere opsporingsdiensten zoals de *ISZW-DO*, boa's en de Koninklijke Marechaussee (als het gaat om de politietaak).

>Lees meer over het Wpg-regime

De politietaak valt uiteen in:

- De bevoegdheden die gericht zijn op de handhaving van de openbare orde. Hierbij treedt de politie op onder het gezag van de burgemeester (art. 11 Politiewet 2012). De doelen voor het aanwenden van deze bevoegdheden zijn:
  - het voorkomen of beëindigen van zich concreet voordoende of dreigende verstoringen van de openbare orde, en
  - het algemene, bestuurlijke voorkomen van strafbare feiten die invloed hebben op de orde en de rust in de gemeente.
- De hulpverleningstaak. Deze taak hangt samen met de opdracht van de politie om de rechtsorde te handhaven. Ook deze wordt uitgevoerd onder het gezag van de burgemeester (art. 11 Politiewet 2012). Het doel van de hulpverleningstaak is dat iedereen die daadwerkelijk hulp nodig heeft een beroep kan doen op de politie.
- De bevoegdheden die gericht zijn op strafrechtelijke handhaving. Hierbij gaat het om het voorkomen, opsporen, beëindigen, vervolgen en berechten van strafbare feiten, waaronder de uitvoering van beslissingen van de rechter of het OM in strafzaken. De uitoefening van deze bevoegdheden vindt plaats onder het gezag van de officier van justitie (art. 12 Politiewet 2012).
- Het verzorgen van de eerste opvang, als dit dringend nodig is, totdat een hulpverlenende instantie het kan overnemen.

Het verwerken van gegevens door de politie en Koninklijke Marechaussee **>in het kader van bestuurlijk toezicht** en **>het uitvoeren van de vreemdelingwetgeving** valt onder de Algemene verordening gegevensbescherming (AVG). Vanaf het moment dat bij het uitvoeren van de bestuurlijke taken (zoals toezicht) blijkt dat er aanleiding bestaat voor een strafrechtelijk onderzoek, valt de verwerking van gegevens van dat onderzoek wél onder de reikwijdte van de Wpg. De eerdergenoemde 'free flow of information' is alleen van toepassing binnen het opsporingsdomein.
Dit houdt in dat in de informatiehuishouding een knip ('Chinese wall') bestaat tussen de gegevens die in het kader van de opsporing worden verwerkt (en waarvoor de 'free flow of information' geldt) en de gegevens die in het kader van de bestuursrechtelijke taken worden verwerkt.

Als de politiegegevens aan een andere partij die zich bezighoudt met de opsporing en vervolging van strafbare feiten *ter beschikking* worden gesteld, toetst de ontvanger diens verdere verwerking van de politiegegevens aan de Wpg of de Wet justitiële en strafvorderlijke gegevens (Wjsg)). Als de politiegegevens echter aan (andere) bestuursorganen of private partijen buiten het strafrecht worden *verstrekt*, dan is op de verdere verwerking in beginsel het regime van de AVG van toepassing (**>zie verder stap 5**).

Praktijkvoorbeeld – Verdere verwerking door burgemeester

Aan de burgemeester mogen politiegegevens verstrekt worden als deze direct relevant en noodzakelijk zijn voor de beoordeling die de burgemeester moet maken om tot onmiddellijke handhaving van de openbare orde over te gaan (art. 16 lid 1, aanhef en onderdeel b, onder 2, Wpg). Beoordeeld naar de huidige stand van de rechtspraak blijft op de verdere verwerking van de gegevens door de burgemeester dan wél de Wpg van toepassing. Dit betekent bijvoorbeeld dat de burgemeester deze gegevens alleen kan verstrekken aan een derde of het college van B&W als daarvoor een grondslag bestaat in de Wpg en de geheimhoudingsplicht van de Wpg dat toestaat.

2 Vallen de persoonsgegevens onder een geheimhoudingsplicht en zo ja, kan deze worden doorbroken?

De partijen in het opsporingsdomein zijn in principe gebonden aan een geheimhoudingsplicht ten aanzien van de politiegegevens die door hen worden verwerkt. Deze mag worden doorbroken als:
- de opsporingsambtenaar wettelijk verplicht is om de politiegegevens te verstrekken;
- de verstrekking op grond van paragraaf 3 van de Wpg is toegestaan, of
- de politietaak dit in een bijzonder geval noodzakelijk maakt.

Ook de ontvanger van de politiegegevens is verplicht tot geheimhouding van de politiegegevens. De ontvanger mag deze geheimhouding alleen doorbreken als hij wettelijk verplicht is de politiegegevens te verstrekken of als dit noodzakelijk is om zijn taak uit te voeren.

Bij incidentele verstrekking van politiegegevens aan derden en bij structurele verstrekking aan samenwerkingsverbanden is de verstrekkende opsporingsambtenaar verplicht de ontvangers te wijzen op de geheimhoudingsplicht die op de politiegegevens blijft rusten (art. 4:8 Besluit politiegegevens).

Praktijkvoorbeelden – Doorbrekingsgronden geheimhoudingsplicht opsporingsambtenaren

Wettelijke verplichtingen

De partijen in het opsporingsdomein moeten aan de officier van justitie politiegegevens over mensenhandel verstrekken, als het OM deze politiegegevens nodig heeft voor de uitvoering van zijn wettelijke taak (art. 16 lid 1, aanhef en onder a, Wpg). Het gaat daarbij bijvoorbeeld om de situatie dat de officier van justitie besluit een dader te vervolgen en de politie het dossier samenstelt en aan de officier van justitie verstrekt voor het strafproces.

Op de politie rust daarnaast een wettelijke verplichting tot verstrekking van politiegegevens als de burgemeester deze nodig heeft om de openbare orde te handhaven (art. 16 lid 1, aanhef en onder b, onder 2˚, Wpg). Dit geldt niet voor bijzondere opsporingsdiensten zoals de ISZW-DO, omdat de burgemeester géén gezag of zeggenschap heeft over de taakuitoefening van bijzondere opsporingsdiensten.

Grondslagen paragraaf 3 van de Wpg

De partijen in het opsporingsdomein kunnen politiegegevens verstrekken aan het Schadefonds geweldsmisdrijven als dat noodzakelijk is voor het uitbrengen van een deskundigenbericht of als aannemelijk is dat de aanvrager slachtoffer is van mensenhandel (art. 18 lid 1 Wpg jo. 4:2 lid 1, aanhef en onder a, Besluit politiegegevens).

De partijen in het opsporingsdomein kunnen structureel de politiegegevens aan CoMensha verstrekken, die CoMensha nodig heeft voor het uitvoeren van hun taken met betrekking tot de coördinatie van de opvang en verzorging van slachtoffers van mensenhandel en de *registratie van gegevens over mensenhandel* (art. 18 lid 1 Wpg jo. art. 4:2 lid 1, aanhef en onder b, onder 3˚, Besluit politiegegevens).

De partijen in het opsporingsdomein mogen structureel politiegegevens over mensenhandel verstrekken aan gecertificeerde instellingen voor de uitvoering van kinderbeschermingsmaatregelen of jeugdreclassering en, als dat noodzakelijk is voor de uitvoering van hun taken, aan Veilig Thuis (art. 18 lid 1 Wpg jo art. 4:2 lid 1 aanhef en onder i, Besluit politiegegevens). Veilig Thuis treedt overigens in de eerste plaats op als meldpunt voor gevallen of vermoedens van huiselijk geweld of kindermishandeling. Deze misdrijven kunnen een overlap hebben met mensenhandel, maar het aantal situaties waarbij politiegegevens over mensenhandel met Veilig Thuis gedeeld mogen worden blijft daarom beperkt tot die gevallen waarin er sprake is van overlap (**>zie ook paragraaf 10.5**).

De partijen in het opsporingsdomein kunnen bij een zwaarwegend algemeen belang in incidentele gevallen overgaan tot het verstrekken van politiegegevens aan personen of instanties (art. 19 Wpg). Het moet dan gaan om één van de volgende doeleinden:
(a) het voorkomen en opsporen van strafbare feiten;
(b) het handhaven van de openbare orde;
(c) het verlenen van hulp aan hen die deze behoeven (hierbij kan bijvoorbeeld gedacht worden aan zorgverleners die zorg bieden aan slachtoffers van mensenhandel), en
(d) het uitoefenen van toezicht op het naleven van regelgeving.

De partijen in het opsporingsdomein kunnen structureel politiegegevens verstrekken aan samenwerkingsverbanden (zoals het RIEC, het Veiligheidshuis en het Expertisecentrum Mensenhandel en Mensensmokkel (EMM) als dat met het oog op een zwaarwegend algemeen belang (zoals de aanpak van mensenhandel) *noodzakelijk* is voor het doel van het samenwerkingsverband (art. 20 lid 1 Wpg).
De verstrekking moet plaatsvinden:

- In overeenstemming met het bevoegde gezag (dus de burgemeester of de officier van justitie).
- Voor één van de volgende doeleinden:
  a) het voorkomen of opsporen van strafbare feiten;
  b) het handhaven van de openbare orde;
  c) het verlenen van hulp aan hen die deze behoeven, of
  d) het uitoefenen van toezicht op de naleven van regelgeving.

In een zogenoemde ‘artikel 20-beslissing’ moet zorgvuldig onderbouwd en vastgelegd worden welke gegevens in zijn algemeenheid met het samenwerkingsverband mogen worden uitgewisseld (zie art. 20 lid 2 Wpg).

Een voorbeeld van een samenwerkingsverband is *het Veiligheidshuis*. Binnen het Veiligheidshuis werken partners uit het zorg- en veiligheidsdomein integraal samen. De samenwerking is gericht op het voorkomen en verminderen van recidive, (ernstige) overlast, criminaliteit en maatschappelijke uitval bij complexe problemen, door een combinatie van repressie, bestuurlijke interventie én zorg. Dit wordt gezien als een zwaarwegend algemeen belang. Het komt in de praktijk regelmatig voor dat signalen en meldingen van mensenhandel binnen het Veiligheidshuis worden aangekaart en besproken.

Bijzondere gevallen waarin de politietaak het noodzakelijk maakt

De partijen uit het opsporingsdomein mogen bij afwezigheid van een wettelijke verplichting of grondslag in de Wpg bijvoorbeeld overgaan tot het verstrekken van politiegegevens bij het tonen van compositietekeningen of foto's van verdachten aan een aangever of aan buurtbewoners.

3 Als er bijzondere persoonsgegevens worden verstrekt, is er een wettelijke grondslag die het verbod om bijzondere persoonsgegevens te verwerken doorbreekt?

De partijen uit het opsporingsdomein zijn bevoegd om bijzondere categorieën politiegegevens ('bijzondere politiegegevens') te verwerken. Het gaat daarbij om politiegegevens waaruit ras, etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijkt. En om genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, of gegevens over gezondheid, seksuele leven en seksuele gerichtheid. De partijen uit het opsporingsdomein mogen deze bijzondere categorieën politiegegevens verwerken én verstrekken aan derden, in aanvulling op de verwerking van 'normale' politiegegevens, als dat voor het doel van de verwerking *onvermijdelijk* is.

Tips & Tricks

Kijk ook of de wetgever heeft toegelicht welke gegevens op grond van een expliciete wettelijke grondslag mogen worden verstrekt (en maak hier aantekening van voor een volgende keer of collega's). Soms heeft de wetgever in de wettekst of de toelichting bij de regeling uitdrukkelijk aangegeven of, en zo ja, in hoeverre er ook bijzondere politiegegevens mogen worden verstrekt aan een specifieke partij.

Een voorbeeld daarvan is art. 4:2 Besluit politiegegevens (>Stcrt. 2015, nr. 186). Daarin is bepaald dat de partijen uit het opsporingsdomein politiegegevens mogen verstrekken aan Slachtofferhulp Nederland en CoMensha. Het doel van de verstrekking aan Slachtofferhulp Nederland is het behartigen van de belangen van de slachtoffers van strafbare feiten, zoals mensenhandel. De wetgever heeft aangegeven dat het hier ook kan gaan om de ernst van het letsel, wat in veel gevallen een medisch gegeven betreft over het slachtoffer en dus eveneens een bijzonder politiegegeven kan zijn. Het verstrekken van gegevens over slachtoffers van mensenhandel aan CoMensha heeft tot doel de coördinatie van de opvang en verzorging van slachtoffers van mensenhandel en de *registratie van gegevens over mensenhandel*.

Uiteraard geldt dat de tekst van de regeling zelf bepalend is. Als die tekst duidelijk bepaalde mogelijkheden uitsluit of omvat, kan hier 'via' de toelichting niet van afgeweken worden. Maar daarentegen is wat in de toelichting staat ook niet noodzakelijk een *uitputtende* opsomming van wat mogelijk is.

Vanaf het moment dat een overheidsinstantie of een private partij politiegegevens heeft ontvangen en buiten de strafrechtelijke context verwerkt, is het regime van de AVG van toepassing. De gegevens worden namelijk niet langer voor de politietaak verwerkt.

Als de ontvanger op grond van de Wpg bijzondere politiegegevens ontvangt, dan bevat de AVG een doorbrekingsgrond om deze te verwerken als dat *noodzakelijk* is *in aanvulling op* de verwerking van strafrechtelijke persoonsgegevens voor de doeleinden waarvoor deze gegevens worden verwerkt. Politiegegevens zijn naar hun inhoud namelijk vrijwel altijd ook aan te merken als strafrechtelijke gegevens zoals bedoeld in de AVG. Dit houdt in dat als politiegegevens worden verstrekt aan een partij buiten het opsporingsdomein, deze dan na ontvangst door de ontvanger zijn aan te merken als strafrechtelijke persoonsgegevens. De wetgever noemt als voorbeeld het verwerken van incidenten van seksuele intimidatie op de werkvloer; een dergelijk gegeven betreft zowel een bijzonder gegeven over iemands seksuele leven als een strafrechtelijk gegeven. Voor wat betreft mensenhandel zou kunnen worden gedacht aan de situatie dat een burgemeester informatie ontvangt over een slachtoffer van mensenhandel die tevens iets zegt over het strafrechtelijke delict dat tegen het slachtoffer is gepleegd.

Praktijkvoorbeeld – Verstrekking aan burgemeester en gemeentelijke toezichthouders

De politie beschikt in het kader van een strafrechtelijk onderzoek over informatie dat binnen een bepaald pand illegale prostitutie wordt bedreven. Daarbij is ook sprake van mensenhandel. Omdat er mogelijk ook sprake is van een verstoring van de openbare orde in en rondom het pand, besluit de politie aan de burgemeester en de gemeentelijke toezichthouders informatie te verstrekken over het pand en de slachtoffers.

In deze situatie verstrekt de politie strafrechtelijke persoonsgegevens aan de burgemeester en de toezichthouders. Deze strafrechtelijke persoonsgegevens kunnen echter ook iets zeggen over het seksuele (professionele) leven van de betrokken prostituees. De gegevens zijn daardoor zowel strafrechtelijke als bijzondere persoonsgegevens. De burgemeester en de toezichthouders mogen deze (eveneens als) bijzondere persoonsgegevens (aan te merken persoonsgegevens) verwerken.

4 Als er strafrechtelijke persoonsgegevens verstrekt worden, is daar een wettelijke grondslag voor?

De rechtmatigheid van het verstrekken van de politiegegevens door de partijen in het opsporingsdomein wordt zoals aangegeven getoetst aan de hand van de Wpg. Omdat politiegegevens vrijwel altijd ook strafrechtelijke gegevens zoals bedoeld in de AVG zijn, is het uitgangspunt dat de verstrekkingsgrondslagen van de Wpg ook als grondslag gelden voor de verstrekking van die gegevens.

>Wat zijn strafrechtelijke persoonsgegevens?

De ontvanger van de politiegegevens moet in dit geval zelf ook over een verwerkingsgrondslag voor de verwerking van de strafrechtelijke gegevens beschikken. Daarvoor moet worden gekeken naar het regime van de AVG, in het bijzonder naar de **>grondslagen in de UAVG**. De in deze situatie meest gangbare grondslagen voor de ontvangst en verdere verwerking van strafrechtelijke gegevens zijn:

- De ontvangst en verdere verwerking is toegestaan omdat de verwerking gedaan wordt door een verwerkingsverantwoordelijke (zoals de burgemeester) die de persoonsgegevens op grond van de Wpg (of de Wjsg) heeft verkregen.
- De verwerking gedaan wordt door of voor publiekrechtelijke samenwerkingsverbanden (zoals het RIEC, het Veiligheidshuis of het Expertisecentrum Mensenhandel en Mensensmokkel (EMM)). Daarbij gelden overigens de volgende twee voorwaarden:
  1. De verwerking is noodzakelijk voor het uitvoeren van de taak van het samenwerkingsverband.
  2. Bij de uitvoering van de samenwerking wordt voorzien in zodanige waarborgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.

Voor hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening is verder relevant dat strafrechtelijke gegevens ook mogen worden verwerkt in aanvulling op gezondheidsgegevens,

als dat *noodzakelijk* is met het oog op een goede behandeling of verzorging van de betrokkene. Hierbij kan gedacht worden aan verschillende situaties. Enerzijds kan worden gedacht aan wetenschap over het delict om als zorgverlener (psychische) zorg te kunnen verlenen aan het slachtoffer. Anderzijds kan ook gedacht worden aan het delen van de strafrechtelijke gegevens van de dader om eventuele nadere veiligheidsmaatregelen voor de zorgverlener te treffen.

Praktijkvoorbeeld – Het Expertisecentrum Mensenhandel en Mensensmokkel

Een voorbeeld van een samenwerkingsverband betreft het EMM. Daaraan nemen de politie, de Koninklijke Marechaussee, de Immigratie- en Naturalisatiedienst (IND) en de ISZW-DO deel om informatie, kennis en ervaring over mensenhandel en mensensmokkel met elkaar te delen. Hieronder vallen ook signalen over mensenhandel. Een aantal van deze signalen wordt na analyse en aanvulling met de nodige informatie periodiek met aangesloten partners en de landelijk officier mensenhandel besproken.

5 Kan de verstrekking van de persoonsgegevens worden gebaseerd op een wettelijke grondslag?

Een opsporingsambtenaar kan overgaan tot het verstrekken van politiegegevens als:

- hij daartoe wettelijk verplicht is;
- dit op grond van paragraaf 3 van de Wpg is toegestaan, of
- de politietaak dit in een bijzonder geval noodzakelijk maakt.

Zie **>stap 2** voor verschillende voorbeelden.

Praktijkvoorbeeld – Ter beschikking stellen van gegevens uit het Themaregister Mensenhandel

Mensenhandel betreft een misdrijf dat een ernstig gevaar oplevert voor de rechtsorde. Omdat slachtoffers en (andere) betrokkenen worden geïntimideerd en bedreigd is het mogelijk dat mensenhandel niet snel aan het licht komt. Voor een effectieve opsporing is het belangrijk dat gegevens over personen die betrokken zijn bij handelingen die kunnen wijzen op het beramen of plegen van deze misdrijven verwerkt kunnen worden. Hierbij kan het bijvoorbeeld gaan om personen die betrokken zijn bij het vervoer of bij het bieden van onderdak.
Om mensenhandel te kunnen ontdekken is het noodzakelijk dat ook gegevens van niet-verdachte personen worden verwerkt. Het gaat dan om gegevens die op zichzelf staand onvoldoende feitelijk zijn om daarop het vermoeden te baseren dat bepaalde personen betrokken zijn bij handelingen die kunnen wijzen op het beramen of plegen van dit misdrijf.

Om zicht te krijgen op mensenhandel is het belangrijk om over langere perioden 'laagwaardige' gegevens te verwerken. Pas na het analyseren en samenvoegen van verschillende van dit soort signalen, kan bepaald worden of er inderdaad sprake is van mensenhandel. Verder onderzoek kan ertoe leiden dat bepaalde personen in beeld komen als betrokkene bij het beramen of plegen van mensenhandel. Er zijn meestal meerdere signalen nodig om tot een verdenking van mensenhandel te komen op basis waarvan een opsporingsonderzoek kan worden gestart en opsporingsbevoegdheden kunnen worden ingezet.
Om mensenhandel op te kunnen sporen, heeft de wetgever bepaald dat laagwaardige gegevens verwerkt mogen worden in het Themaregister Mensenhandel (art. 10 lid 1, onder 3, aanhef en onder b, Wpg jo. art. 3:2, aanhef en onder b, Besluit politiegegevens). De verwerking beperkt zich tot twee categorieën personen, namelijk:

1. personen die betrokken zijn bij handelingen die kunnen wijzen op het beramen of plegen van de aangewezen categorieën van misdrijven, en
2. personen die in een bepaalde relatie staan tot de eerdergenoemde personen.

Vanwege de mogelijke inbreuk op de privacy van de betrokkenen en het belang van afscherming in verband met afbreukrisico komen de zachte gegevens in het themaregister niet in aanmerking voor *verstrekking* aan andere derden (zoals gemeenten en zorginstellingen). Deze beperking geldt zowel voor incidentele gevallen als voor samenwerkingsverbanden waaraan de politie deelneemt. Het is uiteraard wél mogelijk om binnen het opsporingsdomein gegevens *ter beschikking te stellen* aan degenen die geautoriseerd zijn voor de verwerking van politiegegevens, voor zover zij deze behoeven voor de uitvoering van hun taak (art. 15 Wpg).

6 Staat het doelbindingsbeginsel de verstrekking ('verdere verwerking') van de persoonsgegevens toe?

De Wpg heeft een gesloten verstrekkingsregime. Dit houdt in dat de Wpg wettelijk en uitputtend is geregeld aan wie en voor welke doeleinden politiegegevens mogen worden verstrekt. Hierdoor bestaat er géén ruimte om buiten deze wettelijke geregelde mogelijkheden toch over te gaan tot het verstrekken, omdat de verwerking 'verenigbaar' zou kunnen worden geacht. Dit volgt ook uit art. 3 lid 3 Wpg dat bepaalt dat politiegegevens (alleen) voor een ander doel verwerkt kunnen worden als de Wpg of Unierecht daar uitdrukkelijk in voorziet.

7 Wordt er niet meer verstrekt dan de strikt noodzakelijke persoonsgegevens (need to know, in plaats van nice to know)?

Als uit voorgaande stappen volgt dat de verstrekking plaats kan vinden geldt verder nog dat de concrete verstrekking moet voldoen aan het **>noodzakelijkheidsbeginsel**.

Hieruit volgt dat de privacyinbreuk die gepaard gaat met de verstrekking van de persoonsgegevens evenredig moet zijn met het doel waarvoor de persoonsgegevens worden verstrekt (de zorg voor het slachtoffer van mensenhandel of de bestrijding van mensenhandel). Daarnaast mag een partij alleen gegevens verstrekken als het doel niet met minder vergaande maatregelen kan worden bereikt ('subsidiariteit').

Het noodzakelijkheidsbeginsel heeft ook gevolgen voor de omvang en de aard van de persoonsgegevens die door de betreffende partij mogen worden verstrekt. De persoonsgegevens dienen toereikend en direct relevant te zijn en moeten beperkt blijven tot het strikt noodzakelijke. Dit houdt in dat alleen '*need to know*'-informatie verstrekt mag worden (en dus geen '*nice to know*'-informatie).

Kort en goed gelden de volgende uitgangspunten:

- Ga alleen over tot verstrekking van die politiegegevens welke de ontvanger echt nodig heeft om zijn taak uit te voeren.
- Controleer of de gegevens toereikend, direct relevant en niet bovenmatig zijn.
- Stel vast of er geen minder ingrijpende middelen voorhanden zijn.
- Houd bij iedere verstrekking rekening met de verwachting van de betrokkene, de eigen belangen en die van de ontvanger.
- Controleer altijd of de gegevens betrekking hebben op de juiste persoon.
- Controleer of de gegevens betrouwbaar, juist en nauwkeurig zijn aan de hand van al beschikbare bronnen (zachte informatie die niet te verifiëren is moet sowieso niet worden verstrekt aan derden).
- Vermeld bij de gegevens eventuele contextinformatie als die noodzakelijk is voor de ontvanger om de gegevens goed te begrijpen.
- Wijs de ontvanger van de gegevens op de geheimhoudingsplicht die op de gegevens blijft rusten.

8 Moet de betrokkene worden geïnformeerd over de verstrekking of bestaat daarop een uitzondering?

De politie is verplicht om proactief algemene informatie toegankelijk te maken voor betrokkenen, bijvoorbeeld via haar website (art. 24b Wpg). Het gaat daarbij om:

- de identiteit en contactgegevens van de verwerkingsverantwoordelijke en de functionaris voor gegevensbescherming;
- de doelen van de verwerking waarvoor de politiegegevens zijn bestemd;
- het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens;
- de rechten van de betrokkene (waaronder het recht op inzage, correctie, verwijdering en afscherming van politiegegevens).

De informatie aan de betrokkene moet worden verstrekt in een beknopte en toegankelijke vorm en in duidelijke en eenvoudige taal.

De Wpg bevat naast de algemene informatieplicht ook een specifieke informatieplicht. In bepaalde gevallen dient de betrokkene proactief te worden ingelicht over:

- de grondslag van de verwerking;
- de bewaartermijn van de politiegegevens;
- in voorkomend geval, de categorieën van de ontvangers van de politiegegevens;
- indien noodzakelijk, extra informatie, in het bijzonder wanneer politiegegevens zonder medeweten van de betrokkene worden verzameld;
- het gebruik van besluitvorming op basis van automatisch verwerkte gegevens ('geautomatiseerde besluitvorming' zonder tussenkomst van een persoon), met inbegrip van besluitvorming op basis van profielen van personen ('profilering'), en nuttige informatie over de onderliggende logica en het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

⚠ Wanneer sprake is van een 'specifiek geval' waarin moet worden overgegaan tot het informeren van de betrokkene wordt niet specifiek benoemd in de Wpg. De verplichting geldt in elk geval niet als het gaat om een verstrekking van persoonsgegevens die betrekking heeft op personen waarbij een gegrond vermoeden bestaat dat zij een strafbaar feit hebben gepleegd of zullen gaan plegen (art. 24b lid 4 jo. art. 6b, aanhef en onder a, Wpg).

Het specifiek informeren van de betrokkene mag worden uitgesteld, beperkt of achterwege worden gelaten als dit noodzakelijk en evenredig is (art. 27 lid 1 jo. art. 24b lid 3 Wpg):

a) ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures;
b) ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen;
c) ter bescherming van de openbare veiligheid;
d) ter bescherming van de rechten en vrijheden van derden;
e) ter bescherming van de nationale veiligheid.

10.3 (Gemeentelijke) toezichthouders en gemeente

Het komt vaak voor dat toezichthouders bij het uitvoeren van bestuursrechtelijk toezicht op signalen van strafrechtelijk handelen stuiten, waaronder signalen van mensenhandel. De Inspectie SZW stuit bij het toezicht op de naleving van de *publiekrechtelijke arbeidswetgeving* ⊕ bijvoorbeeld regelmatig op signalen van arbeidsuitbuiting. Ook andere toezichthouders kunnen in het kader van het toezicht op sectorale regelgeving, de Gemeentewet of de APV stuiten op signalen van mensenhandel. Hierbij kan onder meer worden gedacht aan de toezichthouders die toezicht houden op de prostitutiebranche en het gemeentelijke bouw- en woningtoezicht. In deze paragraaf lichten we juridische mogelijkheden toe die zij hebben om dergelijke signalen en meldingen van mensenhandel met andere partijen te delen. Daarnaast lichten we ook diverse mogelijkheden toe die het college van B&W en de burgemeester hebben bij de uitvoering van bepaalde gemeentelijke taken.

Het spreekt waarschijnlijk voor zich, maar waar wordt verwezen naar het college van B&W en de burgemeester gaat het in de meeste gevallen om de ambtenaren die namens hen optreden.

1 Is de AVG of de Wet politiegegevens (Wpg) van toepassing op de verstrekking?

Het verwerken van persoonsgegevens door toezichthouders, het college van B&W en de burgemeester voor het toezicht, de handhaving en het uitvoeren van sectorale regelgeving, de Gemeentewet of de APV valt onder het regime van de AVG. Het vindt namelijk plaats in het kader van de uitvoering van hun bestuursrechtelijke bevoegdheden.

Praktijkvoorbeeld – Gemeente wijst politie aan als toezichthouder

Verschillende gemeenten hebben ook de politie of boa's aangewezen als toezichthouder voor het toezicht op de gemeentelijke prostitutieregelgeving. Op de uitvoering van die taken door de betreffende opsporingsambtenaren is dan de AVG van toepassing in plaats van de Wet politiegegevens (Wpg). Echter, vanaf het moment dat bij het uitvoeren van deze bestuurlijke taken blijkt dat er aanleiding bestaat voor een strafrechtelijk onderzoek, valt de verwerking van gegevens in het kader van dat onderzoek wél onder de reikwijdte van de Wpg. Van belang hierbij is dat in de informatiehuishouding een knip ('Chinese wall') bestaat tussen de gegevens die **>in het kader van de opsporing** worden verwerkt en de gegevens die in het kader van de bestuursrechtelijke taken worden verwerkt**.**

Toezichthouders en het college van B&W en de burgemeester zijn *niet* belast met de opsporing van mensenhandel. De strafrechtelijke handhaving, waaronder de opsporing van mensenhandel, valt binnen de taak van het Openbaar Ministerie (OM) en de opsporingsdiensten. De burgemeester mag persoonsgegevens die mede betrekking hebben op signalen en meldingen van mensenhandel alleen verwerken als dat noodzakelijk is voor de uitvoering van zijn eigen taken, bijvoorbeeld de handhaving van de openbare orde. De toezichts- en handhavingsbevoegdheden van de toezichthouder en de gemeente zijn gericht op het bestuursrechtelijk afdwingen van de naleving van wettelijke voorschriften. Het gericht zoeken naar signalen en het verwerken van signalen van mensenhandel kan dus nooit een doel op zich zijn.

2 Vallen de persoonsgegevens onder een geheimhoudingsplicht en zo ja, kan deze worden doorbroken?

Op toezichthouders, het college van B&W en de burgemeester rust de algemene geheimhoudingsplicht van de Algemene wet bestuursrecht. Deze geheimhoudingsplicht houdt in dat een ambtenaar bij vertrouwelijke informatie verplicht is tot geheimhouding, tenzij de verstrekking:

- wettelijk verplicht is, of
- noodzakelijk is voor de uitvoering van de wettelijke, publieke taak van het betreffende bestuursorgaan.

Uitgangspunt hierbij is dat als er sprake is van een **>verenigbare verdere verwerking**, deze geheimhoudingsplicht geen beletsel vormt voor de verstrekking van de persoonsgegevens aan een ander persoon of orgaan, mits de ontvanger zelf ook beschikt over een *eigen* wettelijke grondslag om de persoonsgegevens te verwerken.

>Lees meer over geheimhoudingsplichten en beroepsgeheim

Gemeentelijke toezichthouders en het college van B&W zijn in sommige gevallen daarnaast ook gebonden aan een bijzondere geheimhoudingsplicht. Deze situatie doet zich met name voor binnen het sociaal domein. Bij de gemeentelijke uitvoering van de Participatiewet, de Jeugdwet en de Wmo 2015 zijn de gemeentelijke toezichthouders en het college van B&W gebonden aan een wettelijke geheimhoudingsplicht. Tenzij deze wetten zelf een uitzondering bevatten zal deze geheimhoudingsplicht vaak een belemmering zijn voor zowel het intern delen van signalen en meldingen aan een andere afdeling (bijvoorbeeld Openbare Orde en Veiligheid) als voor het aan externe partijen verstrekken van signalen en meldingen.

De burgemeester zal in ieder geval, waar het de handhaving van de openbare orde betreft, wél kunnen beschikken over informatie die hij van de politie heeft verkregen overeenkomstig de Wpg. Beoordeeld naar de huidige stand van de rechtspraak blijft op de verdere verwerking van de gegevens door de burgemeester dan wél de Wpg van toepassing. Dit betekent bijvoorbeeld dat de burgemeester deze gegevens alleen kan verstrekken aan een derde of het college van B&W als daarvoor een grondslag bestaat in de Wpg en de geheimhoudingsplicht van de Wpg dat toestaat.

Praktijkvoorbeelden – Geheimhoudingsplicht toezichthouder Wmo 2015

Specifiek voor toezichthouders die in het kader van de Wmo 2015 toezicht houden op aanbieders van Wmo-voorziening geldt dat zij gebonden zijn aan een afgeleide geheimhoudingsplicht als het gaat om informatie die is verkregen van een aanbieder die is gebonden aan (medisch) beroepsgeheim. Doordat de toezichthouder gebonden is aan een afgeleid beroepsgeheim, kan hij alleen overgaan tot het verstrekken van deze informatie aan derden als hij zich kan beroepen op een wettelijke uitzondering. Een uitzondering is bijvoorbeeld de wettelijke verplichting van de toezichthouder om het college van B&W informatie te verstrekken die relevant is om de Wmo-voorziening te heroverwegen (art. 5.2.4 lid 3 Wmo 2015 jo. art. 2.3.9 Wmo 2015).

Hoewel per concreet geval kritisch moet worden getoetst op een specifieke geheimhoudingsplicht rust op de verzamelde persoonsgegevens, geldt in zijn algemeenheid dat de Inspectie SZW bij het uitoefenen van toezicht niet gebonden is aan een geheimhoudingsplicht uit sectorale regelgeving.

3 Als er bijzondere persoonsgegevens worden verstrekt, is er een wettelijke grondslag die het verbod om bijzondere persoonsgegevens te verwerken doorbreekt?

Toezichthouders verwerken bij de uitoefening van hun toezicht soms bijzondere persoonsgegevens. Datzelfde geldt voor het college van B&W en de burgemeester bij de uitvoering van hun gemeentelijke taken. Dit is alleen toegestaan als er een wettelijke grondslag aanwezig is die het verbod op de verwerking van bijzondere persoonsgegevens doorbreekt. Daar is voor toezichthouders, het college van B&W en de burgemeester maar in enkele gevallen sprake van.

>Lees meer over bijzondere persoonsgegevens

Praktijkvoorbeeld – Toezicht op de (il)legale prostitutiebranche

Bij het toezicht op de prostitutiebranche lijkt vrijwel altijd sprake te zijn van de verwerking van bijzondere persoonsgegevens. In veel gevallen gaat het bij de uitoefening van dit toezicht over gegevens met betrekking tot het seksuele gedrag en seksuele gerichtheid van de sekswerker. Daarnaast worden in sommige gevallen ook gegevens over ras of etnische afkomst of de gezondheid van de sekswerker verwerkt. Dat het hier (mede) gaat om het *professionele* seksuele leven van een sekswerker doet aan de kwalificatie van bijzonder persoonsgegeven niet af. *Ook de verwerking van gegevens over het professionele leven van een sekswerker valt namelijk onder het verwerkingsverbod.* ➕ Op dit moment is er *géén wettelijke grondslag* ➕ voorhanden voor de doorbreking van het verwerkingsverbod van deze bijzondere persoonsgegevens.

***Praktijkvraag** – Mogen bijzondere persoonsgegevens van slachtoffers van mensenhandel of daders worden verwerkt als deze openbaar zijn gemaakt op internet?*

***Antwoord** – In de praktijk speelt de vraag of de 'kennelijke openbaarmaking' van bijzondere persoonsgegevens door de betrokkene een doorbrekingsgrond kan vormen voor het verwerken van bijzondere persoonsgegevens. Bijvoorbeeld wanneer gemeentelijke toezichthouders met behulp van openbare internetbronnen (bijvoorbeeld een advertentiesite) onderzoek doen naar illegale prostitutie en daarbij op signalen van mensenhandel stuiten.

Een verwerkingsverantwoordelijke mag bijzondere persoonsgegevens verwerken als deze door de betrokkene kennelijk openbaar zijn gemaakt. Toezichthouders kunnen deze doorbrekingsgrond alleen gebruiken bij de verwerking van bijzondere gegevens op internet, als kan worden aangenomen dat deze gegevens uit vrije wil door de betrokkene op internet zijn gezet. Dan moet kunnen worden aangenomen dat een advertentie zelfstandig online is gezet door de sekswerker. Vaak kan betwijfeld worden of een sekswerker daadwerkelijk vrij is om de plaatsing van de advertentie te voorkomen. Het zal in ieder geval vaak niet met zekerheid vastgesteld kunnen worden. De doorbrekingsgrond (zeker bij een strikte lezing van deze doorbrekingsgrond) zal daarom beperkt bruikbaar zijn.

Hierbij dient wel nog te worden benadrukt dat rechtspraak over de vraag wanneer sprake is van 'kennelijke openbaarmaking' van bijzondere persoonsgegevens schaars is. Of het plaatsen van een advertentie als kennelijke openbaarmaking kan gelden, is op dit moment nog niet in de rechtspraak vastgesteld. Het is mogelijk dat de Autoriteit Persoonsgegevens of de rechter zal oordelen dat sprake is van kennelijke openbaarmaking van persoonsgegevens. Gelet op de rechtspraak over de ontoelaatbaarheid van de verwerking van bijzondere gegevens over het seksuele leven van sekswerkers ligt dat alleen niet voor de hand.

Praktijkvraag *– Kan de verwerking van bijzondere persoonsgegevens door toezichthouders worden gebaseerd op de internationaalrechtelijke verplichtingen die voortvloeien uit mensenrechtenverdragen?*

Antwoord – Bijzondere persoonsgegevens mogen worden verwerkt als dit noodzakelijk is voor het uitvoeren van een internationaalrechtelijke verplichting. De vraag hierbij is dan of de verwerking van bijzondere persoonsgegevens mogelijk toelaatbaar is, omdat de verstrekking van signalen en meldingen van mensenhandel noodzakelijk is om de doeleinden van de verschillende mensenhandelverdragen te behalen (in het bijzonder kan hierbij gedacht worden aan *art. 4 EVRM en art. 5 Handvest van de grondrechten van de Europese Unie*). +

In de eerste plaats is van belang dat deze grondslag voor toezichthouders, het college van B&W of de burgemeester sowieso **géén** uitkomst kan bieden om bijzondere persoonsgegevens voor de bestrijding van mensenhandel te verwerken. Deze verdragen brengen namelijk alleen verplichtingen met zich mee voor de Staat. Daar komt bovendien bij dat uit deze verdragen zelf niet duidelijk genoeg volgt dat het voor de aanpak van mensenhandel noodzakelijk is om bijzondere persoonsgegevens te verwerken.

Tips & Tricks

De partijen in het opsporingsdomein zijn overeenkomstig de Wpg in specifieke gevallen bevoegd of zelfs verplicht om politiegegevens aan de toezichthouders of de burgemeester te verstrekken. Als zij de verwerkingsgrondslagen van de Wpg optimaal benutten, kunnen toezichthouders en de burgemeester worden voorzien van de bijzondere persoonsgegevens die zij nodig hebben voor de uitoefening van hun taken.

De volgende situaties zijn daarbij denkbaar:

1. De politie voert een eigen strafrechtelijk onderzoek uit naar mensenhandel onder het gezag van de officier van justitie en verstrekt relevante informatie aan de burgemeester voor de handhaving van de openbare orde
2. De politie voert een eigen strafrechtelijk onderzoek uit naar mensenhandel onder het gezag van de officier van justitie en verstrekt relevante informatie aan de toezichthouder.
3. De politie verricht onder het gezag van de burgemeester een onderzoek naar daders of slachtoffers van mensenhandel voor de handhaving van de openbare orde en verstrekt deze aan de burgemeester.

De politie voert een eigen strafrechtelijk onderzoek uit naar mensenhandel onder het gezag van de officier van justitie en verstrekt relevante informatie aan de burgmeester voor de handhaving van de openbare orde

De politie is bevoegd om voor het uitvoeren van strafrechtelijk onderzoek politiegegevens te verwerken (art. 2 lid 1 Wpg en art. 8 Wpg jo. art. 12 Politiewet 2012 jo. art. 3 Politiewet 2012). Ook boa's komt deze bevoegdheid toe (art. 142 Wetboek van Strafvordering jo. art. 2 lid 1 Besluit politiegegevens buitengewoon opsporingsambtenaar jo. de artikelen 2 en 8 Wpg). Bij het verrichten van het onderzoek mogen naast 'normale' politiegegevens ook bijzondere politiegegevens verwerkt worden als dit *onvermijdelijk* + is. Voorwaarde voor de verwerking is dat de gegevens voldoende beveiligd zijn.

Zij moeten de verzamelde politiegegevens vervolgens ook aan de burgemeester verstrekken als deze direct relevant en noodzakelijk zijn voor de beoordeling die de burgemeester moet maken om tot onmiddellijke handhaving van de openbare orde over te gaan (art. 16 lid 1, aanhef en onderdeel b, onder 2, Wpg). Beoordeeld naar de huidige stand van de rechtspraak blijft op de verdere verwerking van de gegevens door de burgemeester dan wél de Wpg van toepassing. Dit betekent bijvoorbeeld dat de burgemeester deze gegevens alleen kan verstrekken aan een derde of het college van B&W als daarvoor een grondslag bestaat in de Wpg en de geheimhoudingsplicht van de Wpg dat toestaat. De burgemeester mag daarbij bijzondere politiegegevens verwerken als dit *onvermijdelijk* + is.

>Lees meer over het Wpg-regime

De politie voert een eigen strafrechtelijk onderzoek naar mensenhandel uit onder het gezag van de officier van justitie en verstrekt relevante informatie aan de toezichthouder

Voor deze situatie geldt hetzelfde, met als enig verschil dat de verstrekking hier plaatsvindt op grond van art. 19, aanhef en onder d, Wpg (het uitoefenen van toezicht op het naleven van de regelgeving). Op de verdere verwerking van de gegevens door de toezichthouder is de AVG van toepassing.

De toezichthouder beschikt in specifieke gevallen over een doorbrekingsgrond voor de verwerking van eventuele bijzondere persoonsgegevens die hij van de politie heeft verkregen. Het verbod om bijzondere persoonsgegevens te verwerken is niet van toepassing als de verwerking *noodzakelijk* is in aanvulling op de verwerking van strafrechtelijke persoonsgegevens voor de doeleinden waarvoor deze gegevens worden verwerkt. Het gaat daarbij om politiegegevens die zowel een strafrechtelijk persoonsgegeven zijn (bijvoorbeeld omdat ze iets zeggen over een strafrechtelijk delict) als een bijzonder persoonsgegeven (bijvoorbeeld omdat ze ook iets zeggen over de gezondheid of het seksuele leven van het slachtoffer) en dat de verstrekking bijvoorbeeld noodzakelijk is in het kader van de zorg voor het slachtoffer.

De politie verricht onder het gezag van de burgemeester een onderzoek naar daders of slachtoffers van mensenhandel voor de handhaving van de openbare orde en verstrekt deze aan de burgemeester

De burgemeester kan een beroep doen op de politie als het onderzoek gericht is op de handhaving van de openbare orde. De politie mag vervolgens – onder gezag van de burgemeester en voor de (onmiddellijke) handhaving van de openbare orde – gebruikmaken van de algemene bevoegdheden die voortvloeien uit art. 3 Politiewet 2012. Van belang daarbij is dat het onderzoek géén stelselmatig karakter mag hebben.

De burgemeester mag de politie in een concreet geval verzoeken om een internetonderzoek te verrichten naar mensenhandel of misstanden in de prostitutiebranche, als de handhaving van de openbare orde dit vereist (art. 172 Gemeentewet jo. art. 11 Politiewet 2012 jo. art. 3 Politiewet 2012);

De politie is bevoegd om de verzamelde politiegegevens te verwerken (art. 2 lid 1, Wpg en art. 8 Wpg jo. art. 172 Gemeentewet jo. art. 11 Politiewet 2012 jo. art. 3 Politiewet 2012). Ook boa's komt deze bevoegdheid toe (art. 142 Wetboek van Strafvordering jo. art. 2 lid 1 Besluit politiegegevens buitengewoon opsporingsambtenaar jo. art. 2 en 8 Wpg).

De politie mag de verzamelde politiegegevens aan de burgemeester verstrekken als deze direct relevant en noodzakelijk zijn voor de beoordeling die de burgemeester moet maken om tot onmiddellijke handhaving over te gaan (art. 16 lid 1, aanhef en onderdeel b, onder 2, Wpg). Ook in deze situatie blijft de Wpg van toepassing op de verdere verwerking van de gegevens door de burgemeester.

4 Als er strafrechtelijke persoonsgegevens verstrekt worden, is daar een wettelijke grondslag voor?

Toezichthouders, het college van B&W en de burgemeester kunnen strafrechtelijke persoonsgegevens verwerken als dat gebeurt door of voor publiekrechtelijke samenwerkingsverbanden (zoals het RIEC, het Veiligheidshuis en het Expertisecentrum Mensenhandel en Mensensmokkel (EMM)). Daarbij gelden de volgende twee voorwaarden:

1. De verwerking is *noodzakelijk* voor het uitvoeren van de taak van het samenwerkingsverband.
2. Bij de uitvoering van de samenwerking wordt voorzien in zodanige waarborgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.

>Wat zijn strafrechtelijke persoonsgegevens?

Deze grondslag biedt in de eerste plaats een uitkomst voor de *ontvangst* van strafrechtelijke gegevens van de partijen in het opsporingsdomein. Deze bepaling biedt toezichthouders, het college van B&W en de burgemeester daarnaast ook de mogelijkheid om stafrechtelijke gegevens aan samenwerkingsverbanden te *verstrekken*. Hier doet zich wel nog de vraag voor op basis van welke wettelijke grondslag en van welke organisatie de toezichthouder of het college van B&W deze strafrechtelijke gegevens heeft verkregen. Het is mogelijk dat zij daarbij gebonden zijn aan een geheimhoudingplicht (bijvoorbeeld als zij deze hebben gekregen op grond van de Wpg).

Voor alle overige situaties geldt dat de toezichthouders, het college van B&W en de burgemeester niet over een wettelijke grondslag beschikken om strafrechtelijke persoonsgegevens te verstrekken aan derden.

5 Kan de verstrekking van de persoonsgegevens worden gebaseerd op een wettelijke grondslag?

Toezichthouders, het college van B&W en de burgemeester beschikken niet over een wettelijke, publieke taak ten aanzien van de bestrijding van mensenhandel. Er kan daarom géén beroep worden gedaan op **>grondslag (e)**.
Ook toestemming **>(grondslag (a))** kan voor overheidsinstanties vaak géén grondslag vormen, omdat in veel gevallen niet gesproken kan worden van 'vrijelijk' gegeven toestemming.

>Waaraan moet de toestemming voldoen?

>Welke andere wettelijke grondslagen zijn er?

Praktijkvoorbeeld – Wettelijke verplichting vordering opsporingsambtenaren of officier van justitie

Er is een wettelijke verplichting (grondslag (c)) tot het verstrekken van persoonsgegevens aanwezig als een opsporingsambtenaar of de Koninklijke Marechaussee in het kader van een strafrechtelijk onderzoek naar mensenhandel gegevens vordert (art. 126nd Wetboek van Strafvordering). Voor ambtenaren geldt daarnaast dat op verzoek van de officier van justitie alle inlichtingen verstrekt moeten worden met betrekking tot strafbare feiten ten aanzien waarvan zij zelf geen opsporingstaak hebben (art. 162 lid 2 Wetboek van Strafvordering).

Praktijkvraag *– Mag een toezichthouder strafrechtelijke signalen van mensenhandel delen met de politie?*

Antwoord – Als een toezichthouder bij het uitvoeren van zijn taak op informatie stuit die mogelijk relevant is voor opsporingsambtenaren, zoals die van de politie, gaat het zijn toezichthoudende taak niet te buiten als hij deze informatie vervolgens aan een opsporingsambtenaar verstrekt. Deze verstrekking moet dan wel gebaseerd kunnen worden op de aangiftebevoegdheid van art. 161 Wetboek van Strafvordering of verenigbaar zijn met het oorspronkelijke doel (**>zie verder stap 6**).
De gemeente mag overigens alleen een signaal doorsturen, niet (ook) zelfstandig een register van signalen bijhouden. Aannemelijk is evenwel dat het signaal wél eerst kortstondig intern kan worden besproken, voordat het wordt verstrekt. Het lijkt ook gerechtvaardigd dat een bijvoorbeeld baliemedewerker een mogelijk signaal intern doorgeeft aan een toezichthouder, dit signaal vervolgens intern wordt besproken en daarna wordt gedeeld met de politie in het kader van een aangifte.

6 Staat het doelbindingsbeginsel de verstrekking ('verdere verwerking') van de persoonsgegevens toe?

Het delen van signalen en meldingen van mensenhandel is een 'verdere verwerking', waarbij de persoonsgegevens voor een ander doel worden verstrekt (bijvoorbeeld voor de opsporing van strafbare feiten), dan waarvoor zij oorspronkelijk zijn verzameld (het houden van toezicht, de handhaving of uitvoering van andere wettelijke, publieke taken).

Als je op basis van stap 5 hebt vastgesteld dat er een wettelijke grondslag aanwezig is voor de verstrekking van de persoonsgegevens, dan is de verdere verwerking in ieder geval toegestaan. Als een dergelijke wettelijke grondslag ontbreekt, dien je te toetsen of de verdere verwerking in overeenstemming met het doelbindingsbeginsel kan plaatsvinden. De verdere verwerking is op een enkele uitzondering na alleen toegestaan als dit op grond van de **>verenigbaarheidscriteria** als 'verenigbare verwerking' kan worden beschouwd.

>Wat is het doelbindingsbeginsel?

Een relevante wettelijke grondslag die de verdere verwerking van persoonsgegevens ook toestaat is de aangiftebevoegdheid (art. 161 Wetboek van Strafvordering). Deze biedt de mogelijkheid om aangifte te doen van strafbare feiten en zo informatie met de politie of bijzondere opsporingsdiensten te delen.

De verdere verwerking van signalen die in het kader van het sociaal domein zijn verkregen zullen door de strikte doelbinding en de geheimhoudingsplichten vaak niet voor verstrekking voor een ander doel in aanmerking komen. Een voorbeeld daarvan is art. 74 lid 2 Wet SUWI dat bepaalt dat gegevens die in het kader van de uitvoering van deze wet worden verwerkt niet mogen worden verstrekt aan derden, tenzij een wettelijke verplichting tot bekendmaking verplicht of de betrokkene schriftelijk toestemming heeft verleend.

7 Wordt er niet meer verstrekt dan de strikt noodzakelijke persoonsgegevens (need to know, in plaats van nice to know)?

Als uit voorgaande stappen volgt dat de verstrekking plaats kan vinden geldt verder nog dat de concrete verstrekking moet voldoen aan het **>noodzakelijkheidsbeginsel**.

Hieruit volgt dat de privacyinbreuk die gepaard gaat met de verstrekking van de persoonsgegevens evenredig moet zijn met het doel waarvoor de persoonsgegevens worden verstrekt (de zorg voor het slachtoffer van mensenhandel of de bestrijding van mensenhandel). Daarnaast mag een partij alleen gegevens verstrekken als het doel niet met minder vergaande maatregelen kan worden bereikt ('subsidiariteit').

Het noodzakelijkheidsbeginsel heeft ook gevolgen voor de omvang en de aard van de persoonsgegevens die door de betreffende partij mogen worden verstrekt. De persoonsgegevens dienen toereikend en direct relevant te zijn en moeten beperkt blijven tot het strikt noodzakelijke. Dit houdt in dat alleen '*need to know*'-informatie verstrekt mag worden (en dus geen '*nice to know*'-informatie).

Kort en goed gelden de volgende uitgangspunten:
- Ga alleen over tot verstrekking van die persoonsgegevens zonder welke de ontvanger zijn taak niet kan uitvoeren.
- Controleer of de gegevens toereikend, echt relevant en niet bovenmatig zijn.
- Stel vast of er geen minder ingrijpende middelen voorhanden zijn.
- Houd bij iedere verstrekking rekening met de verwachting van de betrokkene, de eigen belangen en die van de ontvanger.
- Controleer altijd of de gegevens betrekking hebben op de juiste persoon.
- Controleer of de gegevens betrouwbaar, juist en nauwkeurig zijn aan de hand van al beschikbare bronnen (zachte informatie die niet te verifiëren is moet in beginsel niet worden verstrekt aan derden).
- Vermeld bij de gegevens eventuele contextinformatie als die noodzakelijk is voor de ontvanger om de gegevens goed te begrijpen.

8 Moet de betrokkene worden geïnformeerd over de verstrekking of bestaat daarop een uitzondering?

De verstrekkende partij is verplicht om de betrokkene te informeren over het verstrekken van zijn persoonsgegevens (art. 13 AVG). Als de persoonsgegevens niet van de betrokkene zelf zijn ontvangen moet de verwerkingsverantwoordelijke de betrokkene ook informeren over (art. 14 AVG):

- Het soort persoonsgegevens.
- De bron waar de persoonsgegevens vandaan komen en of de gegevens afkomstig zijn van openbare bronnen.

De verstrekkende partij hoeft de betrokkene daarentegen niet te informeren als:

- De betrokkene al op de hoogte is van de informatie die anders verstrekt wordt (art. 13 lid 4 AVG en art. 14 lid 5, aanhef en onder a, AVG).
- Het voldoen aan de informatieverplichting de doelen van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (deze uitzondering geldt overigens alleen als de gegevens *niet* bij de betrokkene zelf zijn verkregen). Deze situatie kan zich bijvoorbeeld voordoen als informeren ertoe leidt dat een slachtoffer van mensenhandel in gevaar komt.
- Zich een situatie voordoet waarbij het niet informeren van de betrokkene noodzakelijk en evenredig is voor bijvoorbeeld:
  - de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten (art. 23 AVG jo. art. 41 lid 1, aanhef en onder d, UAVG);
  - een taak op het gebied van toezicht (art. 23 AVG jo. art. 41 lid. 1 aanhef en onder h, UAVG), of
  - de bescherming van de betrokkene of van de rechten en vrijheden van anderen (art. 23 AVG jo. art. 41 lid 1, aanhef en onder j, UAVG).

10.4 Zorgverleners, aanbieders en hulpverleners met een medisch beroepsgeheim (reguliere zorg en sociaal domein) én zonder een medisch beroepsgeheim (sociaal domein)

In deze paragraaf gaan we in op de verstrekking van signalen van en informatie over mensenhandel aan derden door zorgverleners, aanbieders en hulpverleners:

- met een medisch beroepsgeheim, werkzaam binnen de reguliere zorg of het sociaal domein;
- zonder medisch beroepsgeheim, werkzaam binnen het sociaal domein.

1 Is de AVG of de Wet politiegegevens (Wpg) van toepassing op de verstrekking?

Het verwerken van medische informatie en persoonsgegevens van *patiënten en cliënten* door zorgverleners, aanbieders en hulpverleners valt onder het regime van de AVG. Bijzondere vereisten die in aanvulling op de algemene regels van de AVG gelden staan nader beschreven in de sectorale regelgeving. Daarbij zijn de artikelen 7:446 tot en met 7:468 Burgerlijk Wetboek (BW) over de rechten van de patiënt en het medisch beroepsgeheim in het bijzonder van belang. Voor het sociaal domein zijn daarnaast met name de Wmo 2015 en de Jeugdwet relevant.

2 Vallen de persoonsgegevens onder een geheimhoudingsplicht en zo ja, kan deze worden doorbroken?

Op de persoonsgegevens die zorgverleners, aanbieders en hulpverleners voor hun zorgtaak verwerken rust vrijwel altijd een wettelijke geheimhoudingsplicht of medisch beroepsgeheim.

Medisch beroepsgeheim
Hier zal worden volstaan met een nadere uitwerking van het medisch beroepsgeheim dat voortvloeit uit art. 88 Wet BIG en art. 7:457 BW. Dit beroepsgeheim rust op 'hulpverleners', in deze handreiking ook wel aangeduid als 'zorgverleners' of 'aanbieders'. Op (hulp)personen die de zorgverlener inschakelt rust een 'afgeleid medisch beroepsgeheim'. Uit het oogpunt van de leesbaarheid wordt verder steeds alleen het begrip 'zorgverlener' gebruikt, tenzij de bespreking van specifieke wetgeving aanleiding geeft om een ander begrip te gebruiken.

⚠ Onder de geheimhoudingplicht van art. 88 Wet BIG vallen alle BIG-geregistreerde zorgverleners (waaronder artsen, verpleegkundigen, GGZ-psychologen). Het medische beroepsgeheim van art. 7:457 BW is ruimer dan het beroepsgeheim in de Wet BIG, aangezien ook niet-geregistreerde zorgverleners onder de reikwijdte van deze bepaling vallen. De strekking van beide geheimhoudingsbepalingen is hetzelfde. Hieronder zal daarom verder alleen worden stilgestaan bij de geheimhoudingplicht van artikel 7:457 BW.

Praktijkvoorbeeld – Afgeleid medisch beroepsgeheim administratief medewerker of doktersassistente

Een administratief medewerker of doktersassistente heeft een afgeleid medisch beroepsgeheim ten aanzien van de medische dossiers die administratief verwerkt worden of ten aanzien van de werkzaamheden als assistente. Een beslissing over het verstrekken van die gegevens dient in beginsel genomen te worden door de huisarts zelf. In de praktijk wordt de bevoegdheid om over verstrekken te beslissen met een aantal instructies toebedeeld aan een assistente, zodat de assistent niet iedere keer de huisarts zelf moet vragen om een beslissing. Een administratief medewerker heeft geen (enkele) inhoudelijke betrokkenheid of rol. Daarom dient de geheimhouder altijd zelf te beslissen.

Het medisch beroepsgeheim kan op de volgende vijf manieren worden doorbroken:

1. Uitdrukkelijke *toestemming (art. 7:457 lid 1 BW)*

Een zorgverlener met medisch beroepsgeheim mag alleen inlichtingen over een patiënt aan derden verstrekken als de patiënt daarvoor zijn uitdrukkelijke toestemming heeft verleend. De patiënt moet voorafgaand aan het verlenen van toestemming ingelicht worden over het doel, de inhoud en de mogelijke consequenties van de verstrekking. De uitdrukkelijke toestemming van de patiënt kan zowel mondeling als schriftelijk worden gegeven.

Als het specifiek gaat om het verstrekken van medische informatie van een slachtoffer of het verstrekken van informatie over een (mogelijke) dader die afkomstig is van de patiënt, geldt – tenzij het verstrekken kan worden gebaseerd op een **>'conflict van plichten'**– dat zijn toestemming moet worden verkregen als de medische gegevens:

- aan een andere zorgverlener worden verstrekt voor een nieuwe behandelingsovereenkomst;
- aan een partij buiten de gezondheidszorg worden verstrekt (bijvoorbeeld aan politie, justitie, werkgever of een advocaat) zonder dat een wettelijke bepaling daartoe verplicht.

Praktijkvoorbeeld – Overdracht van dossier bij vertrek patiënt naar andere regio

Als een slachtoffer van mensenhandel verhuist naar een andere regio, dan geldt als uitgangspunt dat de arts toestemming moet hebben van zijn patiënt om het medisch dossier te verstrekken aan zijn opvolger. In principe kan de zorgverlener dus niet 'uit bezorgdheid' zonder overleg met de desbetreffende patiënt informatie met zorgverleners in die regio delen. Het zonder toestemming van de betrokken patiënt verstrekken van dergelijke informatie is dan alleen denkbaar als kan worden gesproken

van een situatie waarin een **>'conflict van plichten'** kan worden aangenomen. De arts moet dan kunnen aangeven dat er ernstig gevaar op fysieke of psychische schade bestaat voor (de gezondheid van) zijn patiënt of anderen.

2. *Wettelijke plicht (art. 7:457 lid 1 BW)*

Voorafgaande toestemming van de patiënt is niet vereist als de arts bij of krachtens de wet verplicht is gegevens te verstrekken. Voor specifieke signalen van mensenhandel lijkt een dergelijke wettelijke plicht niet te bestaan.

3. *Veronderstelde toestemming (art. 7:457 lid 2 BW)*

In bepaalde gevallen mag worden uitgegaan van 'veronderstelde toestemming' van de patiënt: de patiënt is op de hoogte van de gegevensverstrekking en heeft daartegen geen bezwaren geuit. Hierbij dient gedacht te worden aan de situatie dat een patiënt instemt met een verwijzing naar een andere zorgverlener. De verstrekking van een signaal van mensenhandel aan een derde zal in veel gevallen niet gebaseerd kunnen worden op de toestemming van de patiënt, omdat de toestemming specifiek voor een dergelijke 'verdere verwerking' vaak ontbreekt.

4. *Rechtstreeks betrokken zorgverleners, vervangers en vertegenwoordigers (art. 7:457 lid 2 BW)*

Een arts mag zonder toestemming van de patiënt gegevens verstrekken aan personen die
1. rechtstreeks betrokken zijn bij de uitvoering van de behandelingsovereenkomst;
2. als vervanger van de (behandelend) arts optreden, of
3. optreden als vertegenwoordiger van de patiënt (bijvoorbeeld een ouder, curator of mentor).

Welke personen rechtstreeks bij de uitvoering van de behandelingsovereenkomst zijn betrokken is niet altijd goed vast te stellen. Uit de toelichting op art. 7:457 BW volgt dat het om personen die de zorgverlener assisteren kan gaan. De toelichting noemt onder andere doktersassistenten. Alle leden van het behandelteam zijn aan te merken als personen die rechtstreeks bij de behandeling betrokken zijn. Ook collega's die door de zorgverlener worden geconsulteerd (bijvoorbeeld in het kader van een intercollegiaal consult) zijn aan te merken als personen die rechtstreeks bij de behandeling betrokken zijn.

Of er daadwerkelijk sprake is van rechtstreekse betrokkenheid bij de behandelingsovereenkomst moet per geval beoordeeld worden. De Autoriteit Persoonsgegevens heeft in het verleden de volgende factoren geformuleerd om te bepalen of bij het uitwisselen van gegevens van een patiënt sprake is van een behandelrelatie:
1. de mate waarin inschakeling van de betreffende persoon of instelling binnen de kring van beroepsgenoten wordt aanvaard;
2. de vraag of redelijke alternatieven voorhanden zijn;
3. de zeggenschap van de arts over de werkzaamheden van de betrokkene (met name wanneer het niet-medici betreft);
4. de maatregelen die zijn getroffen voor de bescherming van de persoonlijke levenssfeer van de patiënt;
5. de kenbaarheid voor de patiënt;
6. de vraag of het belang van de patiënt erdoor wordt gediend.

Als de inschakeling van de betreffende persoon of instantie buiten het verwachtingspatroon van de patiënt ligt of tegen diens belang indruist, heeft de arts toch in beginsel *uitdrukkelijke toestemming* van de patiënt nodig.

Ook waar er sprake is van rechtstreekse betrokkenheid gelden er aanvullende voorwaarden voor het verstrekken van persoonsgegevens:

- De verstrekking moet noodzakelijk zijn voor de door de ontvangende behandelaar te verrichten werkzaamheden.
- De patiënt dient op de hoogte te worden gesteld van de voorgenomen verstrekking van de gegevens, zodat de patiënt hiertegen eventueel bezwaar kan maken.

5. *Conflict van plichten*

Als sprake is van een 'conflict van plichten' mag de zorgverlener zijn beroepsgeheim doorbreken. Het gaat hierbij om een noodtoestand of overmachtssituatie, waarbij de zorgverlener zich verplicht voelt om zijn geheimhoudingsplicht te doorbreken om ernstige schade voor de patiënt of een ander te voorkomen. Deze doorbrekingsgrond kan alleen in hoogst uitzonderlijke situaties worden ingeroepen, als er ernstig gevaar voor de patiënt of anderen dreigt. Hiermee wordt gedoeld op fysieke of psychische schade (zoals bij moord, mishandeling, seksueel misbruik). De dreiging voor de patiënt of voor een ander moet reëel zijn en niet op een andere, minder ingrijpende wijze afgewend kunnen worden.

Praktijkvraag – Een medewerker van een zorginstelling neemt contact op met politie en vertelt over een cliënt bij wie mogelijk sprake is van mensenhandel. Als de politie aangeeft dat het inderdaad om een signaal van mensenhandel gaat, twijfelt de zorginstelling om de naam en andere persoonsgegevens van het slachtoffer te delen. *Welke afwegingen kunnen zorginstellingen maken om persoonsinformatie wél te delen? Welke ruimte hebben zij daarvoor?*

Antwoord – De zorgverlener kan zich beroepen op een 'conflict van plichten' en op basis daarvan tot het delen van informatie overgaan. De voorwaarden hiervoor zijn:

- Alles is in het werk gesteld om eerst toestemming van de patiënt te verkrijgen.
- De arts verkeert in gewetensnood door het handhaven van de geheimhoudingsplicht.
- Het niet doorbreken van de geheimhoudingsplicht zal de patiënt of een ander (onder wie mogelijk de zorgverlener zelf) ernstige fysieke of psychische schade opleveren.
- Er is geen andere weg dan doorbreking van de geheimhoudingsplicht om het probleem op te lossen.
- Het is vrijwel zeker dat het probleem door de geheimhoudingsplicht te doorbreken kan worden voorkomen of beperkt.
- Het 'voordeel' van de schending van het beroepsgeheim weegt op tegen de schade die wordt voorkomen.
- De geheimhoudingsplicht wordt zo min mogelijk geschonden. Alleen direct relevante gegevens worden verstrekt.

Er zijn ook gevallen denkbaar waarin een arts concrete aanwijzingen heeft dat sprake is van een gevaarlijke situatie, maar toch bewust besluit om na de belangenafweging de geheimhoudingsplicht (nog) niet te doorbreken. In een dergelijk geval *adviseert de KNMG* om de redenen hiervoor altijd te noteren in het medisch dossier.

Praktijkvraag – Een zorginstelling vermoedt dat een cliënt slachtoffer is van mensenhandel. Er is steeds een bepaalde jongen die het meisje oppikt. De zorginstelling besluit foto's van het kenteken van de jongen te maken en deze te delen met de wijkagent. *Mag dit? Eenmalig? En wanneer de zorginstelling vaker foto's maakt en deelt, ook van deze jongen zelf?*

Antwoord – Hier kan getwijfeld worden of er sprake is van een conflict van plichten die de verstrekking noodzakelijk maakt. Uiteindelijk is het een persoonlijke afweging van de zorgverlener. Hier speelt met name de vraag of de dreiging van de cliënt in deze fase voldoende reëel is en niet op een andere, minder ingrijpende wijze afgewend kan worden. Ook is het belangrijk om eerst te proberen toestemming van de cliënt of diens ouder (als de cliënt minderjarig is) te krijgen. Als al sprake is van een doorbrekingsgrond van het medisch beroepsgeheim, dient de inbreuk op de geheimhoudingsplicht én de privacyinbreuk sowieso zoveel mogelijk beperkt te blijven. Dit betekent dat er zo min mogelijk foto's gedeeld worden of bijvoorbeeld echt alleen foto's van het kenteken.

Praktijkvoorbeelden – Doorbreken beroepsgeheim

Gevaar voor anderen
Een patiënt vertelt dat hij betrokken is bij mensenhandel en momenteel diverse vrouwen voor hem heeft werken als prostituee. De arts mag zijn beroepsgeheim doorbreken als hij de dreiging als reëel inschat en door de melding aan de politie (mogelijk) kan voorkomen dat deze misdrijven voortduren.

Gevaar voor het kind
Bij een patiëntbespreking met een jeugdige vangt de arts signalen op dat de begeleider van de jeugdige niet zijn voogd is. De verwondingen van het kind duiden op mishandeling. In een veilige omgeving vertelt het kind dat hij ongewild voor deze volwassene moet werken. De arts mag de politie inlichten als hij van oordeel is dat er een direct gevaar bestaat voor het kind.

Tips & Tricks – Het komt regelmatig voor dat een zorgverlener afziet van het melden van een signaal uit angst voor de verslechtering van de behandelrelatie of voor mogelijke represailles tegen de cliënt of zichzelf. De zorgverlener zou in een dergelijk geval in overleg kunnen treden met zijn werkgever en kunnen verzoeken of de werkgever de daadwerkelijke aangifte kan doen, zodat in ieder geval zijn eigen identiteit zoveel mogelijk anoniem blijft. Belangrijk is evenwel dat het niet is uitgesloten dat de politie de betreffende zorgverlener alsnog benadert of de zorgverlener later in het strafproces toch wordt gevraagd om als getuige op te treden.

Het *Centraal Tuchtcollege heeft overwogen* dat er bij de doorbreking van het medisch beroepsgeheim altijd een kritische toets moet worden verricht naar de noodzaak en de omvang van de verstrekking. Bij het doen van aangifte geldt daarbij het volgende:

> "Het doen van aangifte is vrijwel onmogelijk zonder het beroepsgeheim in enige mate te doorbreken. Daarbij zijn twee uitgangspunten aan de orde. Het eerste is dat bij het doen van een aangifte het beroepsgeheim zo min mogelijk moet worden geschonden, bijvoorbeeld door het accent te leggen op de feitelijke gedragingen van de persoon op wie de aangifte betrekking heeft en niet, of zo min mogelijk, op diens medische situatie. Het andere uitgangspunt is dat een aangifte voldoende informatie moet bevatten om de opsporingsautoriteiten in staat te stellen op basis daarvan zo nodig vervolgstappen te zetten. In een dergelijke context moet aan hulpverleners een zekere afwegingsruimte worden gegund, om te voorkomen dat het doen van aangifte zinloos is of dat de negatieve effecten van door hen ervaren geweld of bedreiging worden versterkt. Het is doorgaans voor de betreffende hulpverlener niet makkelijk te beoordelen welke gegevens over een patiënt in het kader van de aangifte wel en niet relevant zijn."

De KNMG adviseert om bij een verzoek te vragen om gerichte vragen op schrift te stellen en het verstrekken van informatie zoveel mogelijk te beperken tot feitelijke gegevens, dus géén vermoedens of interpretaties. De KNMG adviseert de arts om in het medisch dossier aantekening van zijn afwegingen te maken.

Verschoningsrecht
In aanvulling op het medisch beroepsgeheim komt zorgverleners met betrekking tot de onder hen berustende informatie een verschoningsrecht toe tegenover de rechter, de rechter-commissaris, de officier van justitie en de politie. Dit verschoningsrecht houdt in dat de zorgverlener mag weigeren om een getuigenis af te leggen of vertrouwelijke informatie over de patiënt te verstrekken. Het verschoningsrecht geldt in het strafrecht, het civiele recht, bestuursrecht en tuchtrechtelijke procedures. Aan de medewerkers van de zorgverlener (zoals doktersassistenten, administratief medewerkers en medewerkers van de IT-afdeling) komt een afgeleid verschoningsrecht toe.

Als er een verzoek wordt gedaan om verstrekking van patiëntinformatie staat het degene met een afgeleid verschoningsrecht niet vrij om daar zelfstandig over te beslissen. De zorgverlener blijft als oorspronkelijke verschoningsgerechtigde de zeggenschap behouden over of en zo ja, in hoeverre een beroep wordt gedaan op het verschoningsrecht.

Praktijkvoorbeeld – Afgeleid verschoningsrecht

De situatie kan zich voordoen dat gegevens gevorderd worden bij een persoon of instantie die zelf geen verschoningsrecht heeft en die aangeeft de gegevens niet te willen verstrekken omdat er een geheimhouder is die ten aanzien van de gevorderde gegevens wel een verschoningsrecht kan uitoefenen. De *Hoge Raad* kwam in 2017 tot de conclusie dat de gevorderde gegevens dan toch verstrekt moeten worden aan de rechter-commissaris (onderzoeksrechter) en dat deze vervolgens contact op dient te nemen met de verschoningsgerechtigde. Het oordeel van die verschoningsgerechtigde is dan doorslaggevend, tenzij er redelijkerwijs geen twijfel erover kan bestaan dat het beroep op het verschoningsrecht onjuist is.

Sociaal domein

Geheimhoudingsplicht Jeugdwet
De Jeugdwet bevat een specifieke geheimhoudingsbepaling die zich richt op jeugdhulpverleners (art. 7.3.11 lid 1 Jeugdwet). De jeugdhulpverlener mag alleen inlichtingen over een jeugdige geven en inzage in of een afschrift van het betreffende dossier verstrekken als de jeugdige daarvoor toestemming verleent. Deze regeling lijkt op art.7:457 BW, maar is specifiek toegespitst op de relatie tussen jeugdhulpverlener en de jeugdige. In de praktijk gelden voor de jeugdhulpverlener dezelfde doorbrekingsgronden als voor een reguliere zorgverlener.

In bepaalde gevallen is de toestemming van de met het gezag belaste ouders vereist (art. 7.3.15 Jeugdwet en art. 7:465 BW).

Geheimhoudingsplicht Wmo 2015
Ook de Wmo 2015 kent een geheimhoudingsplicht (art. 5.3.3 Wmo 2015). Uitgangspunt is dat anderen dan de betrokkene alleen inzage in of afschriften van bescheiden mogen ontvangen als de betrokkene daarvoor toestemming heeft gegeven. Onder 'anderen dan de betrokkene' vallen *niet* degenen van wie beroepshalve de medewerking vereist is bij de uitvoering van de wettelijke taken van het college van B&W of een (andere) aanbieder (art. 5.3.3 lid 3 Wmo 2015). De geheimhoudingsplicht van de Wmo 2015 staat het verstrekken van bescheiden aan een andere aanbieder dus niet in de weg, als dit noodzakelijk is voor de continuïteit van de behandeling van de cliënt. Als de betrokkene geen toestemming geeft voor de verstrekking van zijn persoonsgegevens, kan het verder verstrekken alleen plaatsvinden als in de Wmo 2015 voor deze verstrekking een specifieke grondslag staat.

Praktijkvraag *– In hoeverre moeten signalen van mensenhandel op grond van de Wmo 2015 worden gemeld aan Veilig Thuis?*

Antwoord – De Wmo 2015 bevat een meldrecht zodat zorgverleners *zonder* toestemming signalen van kindermishandeling en huiselijk geweld kunnen melden aan Veilig Thuis, als dat noodzakelijk is om kindermishandeling of huiselijk geweld te stoppen of te laten onderzoeken. Deze misdrijven kunnen een overlap hebben met mensenhandel, maar het aantal situaties waarbij politiegegevens over mensenhandel met Veilig Thuis gedeeld mogen worden blijft beperkt tot die gevallen waarin er van die overlap sprake is.

De KNMG heeft een *meldcode* opgesteld voor dergelijke meldingen.
De meldcode bevat de volgende stappen:
1. Het verrichten van onderzoek waarbij de zorgverlener signalen en aanwijzingen in kaart brengt

2. Het vragen van anoniem advies aan Veilig Thuis. Bij sociaal-medische vragen of vragen over de afwegingen rond het beroepsgeheim wordt het advies bij voorkeur gevraagd aan de vertrouwensarts van Veilig Thuis. Daarnaast is het ook wenselijk om advies te vragen aan een terzake deskundige collega.
3. De zorgverlener spreekt met de betrokkenen, tenzij dat niet mogelijk is (bijvoorbeeld als de veiligheid of gezondheid van de patiënt in gevaar is). De arts bespreekt de aanwijzingen en signalen van mensenhandel (gelijktijdig kindermishandeling of huiselijk geweld) met de betrokkenen, en ook zo veel mogelijk met het kind. Dit kan al vanaf jonge leeftijd, mits het gesprek is aangepast aan het niveau van het kind. De arts bespreekt ook de mogelijkheden om tot een oplossing te komen. Indien gewenst kan Veilig Thuis adviseren bij de voorbereiding van het gesprek.
4. De zorgverlener kan – *met* toestemming van de betrokkenen – overleggen met andere hulpverleners die bij het (gezins)systeem betrokken zijn. De zorgverlener kan ook een signaal afgeven aan de Verwijs Index Risicojongeren (VIR). Dit kan zonder toestemming, maar alleen als de arts een vermoeden van kindermishandeling heeft en het nodig is om na te gaan of er andere hulpverleners bij het gezin betrokken zijn die zorgen hebben over het kind/de kinderen.
5. De zorgverlener weegt af of de melding plaats zou moeten vinden. In de meldcode wordt aangenomen dat in de volgende situaties een melding bij Veilig Thuis zou moeten worden gedaan:
   - in gevallen van acute en/of structurele onveiligheid;
   - in niet-acute en/of niet-structureel onveilige situaties waarin de zorgverlener meent dat hij, gelet op zijn competenties, verantwoordelijkheden en professionele grenzen, in onvoldoende mate effectieve hulp kan bieden of organiseren, en
   - als de zorgverlener die hulp biedt of organiseert om betrokkenen te beschermen tegen (het risico op) kindermishandeling en/of huiselijk geweld, constateert dat de onveiligheid niet stopt of zich herhaalt.

Er moet sneller gemeld worden in situaties waarbij mensenhandel overlapt met kindermishandeling. In de KNMG-meldcode is voor kindermishandeling als uitgangspunt genomen dat de zorgverlener een melding doet als er een 'reële kans op schade' bestaat. Bij volwassenengeweld wordt een zwaarder criterium gehanteerd. In beginsel wordt uitgegaan van de zelfbeschikking van de persoon, en wordt niet gemeld. Dit is in beginsel alleen anders als er sprake is van een afhankelijkheidsrelatie of degene minder goed in staat is om zelf op te treden tegen geweld of uitbuiting.

Geheimhoudingsplicht Algemene wet bestuursrecht

Op aanbieders en hulpverleners die namens het college van B&W werkzaamheden uitvoeren bij de toeleiding naar zorg en ondersteuning in het sociaal domein rust ook de algemene geheimhoudingsplicht van de Algemene wet bestuursrecht. Het gaat dan bijvoorbeeld om advieswerkzaamheden of werkzaamheden die 'in mandaat' worden uitgevoerd voor de uitvoering van de Wmo 2015, Jeugdwet of Participatiewet. Als zij daarbij in aanraking komen met vertrouwelijke gegevens zijn zij ten aanzien van die vertrouwelijke informatie verplicht zijn tot geheimhouding, tenzij de verstrekking:

- wettelijk verplicht is, of
- noodzakelijk is voor de uitvoering van de wettelijke, publieke taak van het betreffende bestuursorgaan.

Uitgangspunt hierbij is dat als er sprake is van een **>verenigbare verdere verwerking** deze geheimhoudingsplicht geen beletsel vormt voor de verstrekking van de persoonsgegevens aan een ander persoon of orgaan, mits de ontvanger zelf ook beschikt over een *eigen* wettelijke grondslag om de persoonsgegevens te verwerken.

3 Als er bijzondere persoonsgegevens worden verstrekt, is er een wettelijke grondslag die het verbod om bijzondere persoonsgegevens te verwerken doorbreekt?

Lang niet in alle gevallen zal het voor zorgverleners noodzakelijk zijn om ook bijzondere persoonsgegevens te verstrekken, als signalen en meldingen van mensenhandel worden opgesteld en gedeeld.

>Wat zijn bijzondere persoonsgegevens?

Als de noodzaak daartoe wél bestaat, kan de verstrekking van bijzondere persoonsgegevens mogelijk worden gebaseerd op een van de volgende **>doorbrekingsgronden**. Het zal dan veelal gaan om gezondheidsgegevens of gegevens over het seksuele leven van de betrokkene.

(a) De 'uitdrukkelijke toestemming'

Van rechtsgeldige uitdrukkelijke toestemming in de zin van de AVG is sprake als de toestemming op voldoende informatie berust en in vrijheid gegeven, specifiek en met een ondubbelzinnige, actieve handeling is gegeven. Dat betekent dat betrokkenen in vrijheid hun wil moeten kunnen uiten. Ook mag er geen twijfel zijn of betrokkenen hun toestemming hebben gegeven en voor welke specifieke verwerking zij dit hebben gedaan. De term 'uitdrukkelijk' verwijst verder naar de manier waarop de betrokkene zijn toestemming tot uitdrukking brengt: met een *uitdrukkelijke* verklaring van toestemming. Verder gelden voor *uitdrukkelijke* toestemming **>dezelfde eisen** als voor 'normale', ondubbelzinnige toestemming.

De grondslag '*uitdrukkelijke* toestemming' kan niet zonder meer worden ingeroepen in het sociaal domein. De *Autoriteit Persoonsgegevens heeft geoordeeld* dat de toestemming van de betrokkene géén grondslag kan vormen voor de verwerking van persoonsgegevens door de gemeente voor de 'intake' in het sociaal domein, waaronder de toeleiding naar voorzieningen uit de Wmo 2015 en de Jeugdwet. De burger staat namelijk in een afhankelijkheidsrelatie tot de gemeente. Weigeren mensen toestemming voor het verwerken van hun gegevens, dan kan dat bijvoorbeeld gevolgen hebben voor een gewenste voorziening. Daarom is er in dat soort situaties geen sprake van vrije toestemming in de zin van de AVG. Toestemming kan dan dus niet gelden als de grondslag voor de gegevensverwerking.

Bij de feitelijke dienstverlening zijn situaties mogelijk waarin wél kan worden gesproken van vrije en ondubbelzinnige toestemming. Daarbij moet je steeds nagaan of er sprake is van een afhankelijkheidsrelatie. Kan iemand in vrijheid toestemming geven of weigeren? Zo ja, dan kan je de gegevensverwerking baseren op de grondslag toestemming. Zo nee, dan heb je een andere grondslag nodig voor de verwerking.

(b) Het 'vitale belang ' van de betrokkene (of een ander persoon)

In uitzonderlijke gevallen kan de verstrekking worden gebaseerd op de bescherming van de vitale belang van de betrokkene of van een ander persoon. Er moet dan een dringende noodzaak zijn om de gegevens van de betrokkene te verwerken, terwijl de betrokkene fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is toestemming te geven. Bij vitale belangen kan vanuit een medisch perspectief gedacht worden aan het verwerken van persoonsgegevens die noodzakelijk zijn voor humanitaire doelen, waaronder het monitoren van epidemieën en de verspreiding daarvan of verwerking van persoonsgegevens in humanitaire noodsituaties, zoals natuurrampen of door de mens veroorzaakte rampen.

Praktijkvoorbeeld – Vitale belangen van een zwaar getraumatiseerde slachtoffer
Het kan voorkomen dat een slachtoffer dermate getraumatiseerd is dat hij niet reageert en dus ook géén toestemming kan geven voor het verwerken zijn persoonsgegevens. Als er een medische noodzaak bestaat kan het verstrekken van bijzondere persoonsgegevens in dat geval gebaseerd worden op de bescherming van de vitale belangen van het slachtoffer.

4 Als er strafrechtelijke persoonsgegevens verstrekt worden, is daar een wettelijke grondslag voor?

Voor zorgverleners geldt dat zij strafrechtelijke gegevens mogen verwerken in aanvulling op gezondheidsgegevens, als dat *noodzakelijk* + is met het oog op een goede behandeling of verzorging van de betrokkene. Hierbij kan gedacht worden aan verschillende situaties. Enerzijds kan worden gedacht aan wetenschap over het delict om als zorgverlener (psychische) zorg te kunnen verlenen aan het slachtoffer. Anderzijds kan ook gedacht worden aan de strafrechtelijke gegevens van de dader om eventuele nadere veiligheidsmaatregelen voor de zorgverlener te treffen.

Dit biedt enige basis voor de verstrekking van voor de zorg relevante strafrechtelijke gegevens aan andere zorgverleners of instellingen van gezondheidszorg of maatschappelijke dienstverlening (bijvoorbeeld de aanbieder van een maatwerkvoorziening in de Wmo 2015). Uiteraard geldt ook hier dat de verstrekking alleen kan plaatsvinden als het medisch beroepsgeheim of de wettelijke geheimhoudingsplicht van de Jeugdwet of de Wmo 2015 dat toestaat (**>zie hierover stap 2**).

>Wat zijn strafrechtelijke persoonsgegevens?

Afhankelijk van de aard van de verstrekking, is het verder mogelijk dat zorgverleners in de volgende situaties strafrechtelijke persoonsgegevens mogen verstrekken:

- Een slachtoffer van mensenhandel geeft **>uitdrukkelijk toestemming** voor de verstrekking van zijn persoonsgegevens aan een derde, bijvoorbeeld de politie.
- De verstrekking is nodig voor de bescherming van de vitale belangen van de betrokkene of van een ander persoon, terwijl de betrokkene fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is om toestemming te geven.
- De zorgverlener heeft deze strafrechtelijke gegevens van de politie verkregen en wil deze verder verstrekken aan een derde, dan kan dat als de geheimhoudingsplicht van de Wet politiegegevens (Wpg) deze verdere verstrekking toelaat. Dat mag de zorgverlener als het verstrekken van die politiegegevens wettelijk verplicht is of als dat noodzakelijk is voor de uitvoering van zijn taak (**>zie ook paragraaf 10.2, stap 2**).
- De verwerking gebeurt door of voor publiekrechtelijke samenwerkingsverbanden (zoals het RIEC, het Veiligheidshuis of het Expertisecentrum Mensenhandel en Mensensmokkel (EMM)). Daarbij gelden de volgende twee voorwaarden:
  1. De verwerking is *noodzakelijk* + voor het uitvoeren van de taak van het samenwerkingsverband.
  2. Bij de uitvoering van de samenwerking wordt voorzien in zodanige waarborgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.

5 Kan de verstrekking van de persoonsgegevens worden gebaseerd op een wettelijke grondslag?

Voor de reguliere werkzaamheden van zorgverleners zal het verstrekken van persoonsgegevens in de meeste gevallen gebaseerd zijn op toestemming van de betrokkene **>(grondslag (a))** of omdat het nodig is om uitvoering te geven aan de behandelovereenkomst (grondslag (b) jo. art. 7:446 BW). Bij het verstrekken van signalen van mensenhandel ligt dit anders. Toestemming specifiek ook hiervoor ontbreekt vaak en voor de uitvoering van de behandelovereenkomst is het vrijwel nooit noodzakelijk. In het sociaal domein geldt dat de persoonsgegevens slechts mogen worden verstrekt voor zover dat op grond

van de toepasselijke wet is toegestaan. Van belang daarbij is bovendien dat zowel op grond van de Wmo 2015 als de Jeugdwet geldt dat de **>geheimhoudingsplicht** ertoe kan leiden dat de verstrekking enkel met toestemming van de betrokkene kan plaatsvinden.

In uitzonderlijke situaties waarin een **>conflict van plichten** kan worden aangenomen kan een signaal dan alsnog zonder toestemming verstrekt worden. In andere eveneens uitzonderlijke gevallen kan teruggevallen worden op het verstrekken van de signalen op basis van het gerechtvaardigde belang van een derde (**>grondslag (f)**). Het kan daarbij gaan om het gerechtvaardigde belang van het slachtoffer, het algemene belang dat mensenhandel zoveel mogelijk moet worden voorkomen (ten aanzien waarvan de beoogde ontvanger dan wel een **>wettelijke, publieke taak** moet uitvoeren) of het specifieke belang van de ontvanger (bijvoorbeeld de registratie van dergelijke meldingen). De gegevensverwerking moet daarbij dan noodzakelijk zijn om dat belang te behartigen. De verstrekking kan bovendien alleen plaatsvinden als het gerechtvaardigde belang zwaarder weegt dan de belangen van de betrokkene. Dit houdt in dat deze grondslag niet gebruikt kan worden als de belangen, rechten of fundamentele vrijheden van de betrokkene (hier: het slachtoffer of de daders over wie gegevens verstrekt worden) zwaarder wegen dan het belang om (mogelijke) slachtoffers te beschermen en de belangen die de ontvangende partij heeft. Uitganspunt blijft overigens dat, waar mogelijk, de betrokkene wordt gevraagd om **>toestemming** voor het delen van de informatie.

>Waar moet op gelet worden bij de belangenafweging?

⚠ Vanwege het feit dat de wetgever de rechtsgrond bepaalt voor de verwerking van persoonsgegevens door overheidsinstanties, is de rechtsgrond 'gerechtvaardigd belang' niet van toepassing op verwerkingen door overheidsinstanties in het kader van de uitvoering van hun taken.

⚠ Het enkele feit dat de ontvanger van de persoonsgegevens een wettelijke, publieke taak heeft die verband houdt met de bestrijding van mensenhandel is *onvoldoende* ⊕ om te kunnen spreken van een grondslag voor de verstrekking van persoonsgegevens door de zorgverlener. Er bestaat hiervoor pas een wettelijke grondslag als de zorgverlener een wettelijke grondslag heeft voor de verstrekking én, in het geval van een overheidsinstantie, de *ontvangst* van de persoonsgegevens valt binnen die wettelijke, publieke taak van de ontvangende partij **>(grondslag (e))** of, in het geval van een private partij, deze kan gebaseerd worden op gerechtvaardigd belang **>(grondslag (f))**.

6 Staat het doelbindingsbeginsel de verstrekking ('verdere verwerking') van de persoonsgegevens toe?

Het delen van signalen en meldingen van mensenhandel is een 'verdere verwerking', waarbij de persoonsgegevens voor een ander doel worden verstrekt (bijvoorbeeld voor de opsporing van strafbare feiten), dan waarvoor ze oorspronkelijk zijn verzameld (het bieden van zorg).

Als je op basis van stap 5 hebt vastgesteld dat er een wettelijke grondslag aanwezig is voor de verstrekking van de persoonsgegevens, dan is de verdere verwerking in ieder geval toegestaan. Als een dergelijke wettelijke grondslag ontbreekt, dien je te toetsen of de verdere verwerking in overeenstemming met het doelbindingsbeginsel kan plaatsvinden. De verdere verwerking is op een enkele uitzondering na alleen toegestaan als dit op grond van de **>verenigbaarheidscriteria** als 'verenigbare verwerking' kan worden beschouwd. Hier is voor zorgverleners met name sprake van bij verstrekking die binnen het zorgkader blijven.

>Wat is het doelbindingsbeginsel?

Een relevante wettelijke grondslag die de verdere verwerking van persoonsgegevens ook toestaat is de aangiftebevoegdheid (art. 161 Wetboek van Strafvordering). Deze biedt ook zorgverleners de mogelijkheid om aangifte te doen van strafbare feiten en zo informatie met de politie of bijzondere opsporingsdiensten te delen.

De verdere verwerking van signalen die in het kader van het sociaal domein zijn verkregen zullen door de strikte doelbinding en de geheimhoudingsplichten vaak niet voor verstrekking voor een ander doel in aanmerking komen. Een voorbeeld daarvan is art. 74 lid 2 Wet SUWI dat bepaalt dat gegevens die in het kader van de uitvoering van deze wet worden verwerkt niet mogen worden verstrekt aan derden, tenzij een wettelijke verplichting tot bekendmaking verplicht of de betrokkene schriftelijk toestemming heeft verleend.

7 Wordt er niet meer verstrekt dan de strikt noodzakelijke persoonsgegevens (need to know, in plaats van nice to know)?

De zorgverlener moet bij het verstrekken van de gegevens aan derden en het doorbreken van het medisch beroepsgeheim altijd oog hebben voor de vraag of minder ingrijpende middelen voorhanden zijn (**>'subsidiariteit'**) en de vraag of het voordeel van het doorbreken van het medisch beroepsgeheim opweegt tegen de eventuele schade als gevolg van het doorbreken.

Zie voor meer informatie over de verstrekking aan politie (of bijzondere opsporingsdienst) *de uitleg van de KNMG*: +

> "Met subsidiariteit wordt bedoeld dat de arts zich de vraag moet stellen of de veiligheid van het slachtoffer ook op minder ingrijpende wijze kan worden beschermd dan door de politie in te lichten. Zo ja, dan moet hij kiezen voor het minder ingrijpende alternatief. Als ernstige schade voor de patiënt of voor een ander echter alleen kan worden voorkomen door een schending van het beroepsgeheim, dan is dat toegestaan.
>
> Met proportionaliteit wordt bedoeld dat het voordeel dat de schending met zich meebrengt moet opwegen tegen de schade als gevolg van de schending van het geheim. Als het inschatten van dat voordeel voor de arts in kwestie lastig is, verdient het aanbeveling vertrouwelijk overleg te plegen met een collega of met de KNMG-artseninfolijn."

Kort en goed gelden de volgende uitgangspunten:
- Ga alleen over tot verstrekking van die persoonsgegevens zonder welke de ontvanger zijn taak niet kan uitvoeren.
- Controleer of de gegevens toereikend, echt relevant en niet bovenmatig zijn.
- Stel vast of er geen minder ingrijpende middelen voorhanden zijn.
- Houd bij iedere verstrekking rekening met de verwachting van de betrokkene, de eigen belangen en die van de ontvanger.
- Controleer altijd of de gegevens betrekking hebben op de juiste persoon.
- Controleer of de gegevens betrouwbaar, juist en nauwkeurig zijn aan de hand van al beschikbare bronnen (zachte informatie die niet te verifiëren is moet in beginsel niet worden verstrekt aan derden).
- Vermeld bij de gegevens eventuele contextinformatie als die noodzakelijk is voor de ontvanger om de gegevens goed te begrijpen.

8 Moet de betrokkene worden geïnformeerd over de verstrekking of bestaat daarop een uitzondering?

De verstrekkende partij is verplicht om de betrokkene te informeren over het verstrekken van zijn persoonsgegevens (art. 13 AVG). Als de persoonsgegevens niet van de betrokkene zelf zijn ontvangen moet de verwerkingsverantwoordelijke de betrokkene ook informeren over (art. 14 AVG):
- Het soort persoonsgegevens.
- De bron waar de persoonsgegevens vandaan komen en of de gegevens afkomstig zijn van openbare bronnen.

De verstrekkende partij hoeft de betrokkene daarentegen niet te informeren als:

- De betrokkene al op de hoogte is van de informatie die anders verstrekt wordt (art. 13 lid 4 AVG en art. 14 lid 5, aanhef en onder a, AVG).
- Het voldoen aan de informatieverplichting de doelen van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (deze uitzondering geldt overigens alleen als de gegevens *niet* bij de betrokkene zelf zijn verkregen). Deze situatie kan zich bijvoorbeeld voordoen als informeren ertoe leidt dat een slachtoffer van mensenhandel in gevaar komt.
- Zich een situatie voordoet waarbij het niet informeren van de betrokkene noodzakelijk en evenredig is voor bijvoorbeeld:
  - de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten (art. 23 AVG jo. art. 41 lid 1, aanhef en onder d, Uitvoeringswet AVG (UAVG));
  - een taak op het gebied van toezicht (art. 23 AVG jo. art. 41 lid. 1 aanhef en onder h, UAVG), of
  - de bescherming van de betrokkene of van de rechten en vrijheden van anderen (art. 23 AVG jo. art. 41 lid 1, aanhef en onder j, UAVG).

Praktijkvraag – Een zorginstelling vermoedt dat een cliënt slachtoffer is van mensenhandel en besluit dit te bespreken met de politie. *Moet de zorginstelling van tevoren toestemming vragen aan de cliënt of kan de zorginstelling dit achteraf melden? Of is het mogelijk om in overleg met politie te besluiten dat niet te doen, in het belang van een te starten onderzoek? En maakt het dan verschil of de cliënt minderjarig of meerderjarig is?*

Antwoord – De zorgverlener kan zonder toestemming overgaan tot verstrekking van informatie aan de politie als de zorgverlener vindt dat er sprake is van een conflict van plichten (**>zie hierover uitgebreider stap 2**). Het niet melden van de verstrekking aan de betrokkene is goed verdedigbaar bij de noodzaak van de opsporing en de vervolging van strafbare feiten (art. 41 lid 1, aanhef en onder d, UAVG) of het belang van de bescherming van een slachtoffer (art. 41 lid 1, aanhef en onder j, UAVG).

Praktijkvraag – *Moet een cliënt of patiënt ingelicht worden over een casusoverleg van de zorgtafel?*

Antwoord – Bij zorgtafels ontstaat geregeld discussie over het inlichten van cliënten en patiënten over de bespreking die in het kader van de zorgtafel plaatsvindt. In de praktijk wordt hier niet eenduidig mee omgegaan. Op zichzelf is het inderdaad juist dat in beginsel slechts met toestemming van de patiënt informatie wordt gedeeld (ook binnen de zorgtafel). Voor zover toestemming wordt verkregen, is het ook logisch dat de patiënt in dat kader op voorhand wordt geïnformeerd over het casusoverleg. Als daadwerkelijk ernstig gevaar voor de patiënt bestaat, kan dit een aanleiding zijn om met beroep op een conflict van plichten, gezien een zwaarwegend algemeen belang van de patiënt, de patiënt (nog) niet direct te informeren. Daarbij geldt evenwel dat nadat dit gevaar is geweken de patiënt alsnog moet worden geïnformeerd.

10.5 Publieke en private partijen met een meldpunt- of coördinatiefunctie

Er zijn diverse partijen met een meldpunt- of coördinatiefunctie die signalen en meldingen van mensenhandel ontvangen en verwerken. Het gaat om zowel publieke als private partijen. Het is steeds belangrijk om onderscheid te maken tussen de partijen *met* en *zonder* een daartoe strekkende **>wettelijke, publieke taak**.

>Wat is een meldpuntfunctie?
>Wat is een coördinatiefunctie?

Naast de politie, de Koninklijke Marechaussee en bijzondere opsporingsdiensten zoals de ISZW-DO – welke in **>paragraaf 10.2** worden behandeld – is Veilig Thuis de enige publieke partij met een wettelijke, publieke taak. Die is overigens in de eerste plaats om als meldpunt op te treden voor gevallen of vermoedens van huiselijk geweld of kindermishandeling. Deze misdrijven kunnen

een overlap hebben met mensenhandel, maar het aantal situaties waarbij politiegegevens over mensenhandel met Veilig Thuis gedeeld mogen worden blijft daarom beperkt tot die gevallen waarin er van die overlap sprake is.

Voor *zorgcoördinatoren*, *aandachtsfunctionarissen mensenhandel* en *ketenregisseurs* geldt dat het hen aan een specifieke **>wettelijke, publieke taak** ontbreekt. Hierdoor bestaat er langs die weg vaak géén wettelijke grondslag voor deze functionarissen om signalen van mensenhandel met (bijzondere) persoonsgegevens te verwerken.

Er zijn ook diverse private partijen met een (zelfbenoemde of geformaliseerde) meldpunt- of coördinatiefunctie, zoals CoMensha, Stichting WATCH Nederland en Stichting M (Meld Misdaad Anoniem).

In deze paragraaf lichten we toe welke mogelijkheden deze partijen hebben om vanuit hun hoedanigheid als meldpunt- of coördinatiefunctie persoonsgegevens aan andere partijen te verstrekken.

1 Is de AVG of de Wet politiegegevens (Wpg) van toepassing op de verstrekking?

Het verwerken van persoonsgegevens door publieke en private partijen die vanuit hun meldpunt- of coördinatiefunctie handelen valt onder de AVG. Het vindt namelijk plaats in het kader van de uitvoering van bestuursrechtelijke bevoegdheden of in een private context.

Praktijkvraag *– Mogen burgers of professionals zelf signalen doorgeven of meldingen doen?*

Antwoord – Een signaal doorgeven of een melding doen beschouwt een burger vaak als 'burgerplicht'. Vanuit dat oogpunt kan het doorgeven van signalen en het doen van meldingen gerekend worden tot 'zuiver persoonlijke of huishoudelijke activiteiten' van de burger. De AVG is hierop niet van toepassing (art. 2 lid 2, aanhef en onder c, AVG). Bij signalen of meldingen dient het te gaan om kennis en informatie die de burger persoonlijk (en niet beroeps- of arbeidsmatig) heeft. Een overheidsinstantie of een private partij die een dergelijk signaal ontvangt dient echter altijd kritisch te bezien of het ook beschikt over grondslag om de persoonsgegevens binnen dat signaal te mogen ontvangen.

Het is daarentegen niet mogelijk om signalen en meldingen op basis van informatie die is waargenomen in het kader van het uitvoeren van beroepsmatige taken en werkzaamheden aan te merken als een activiteit van zuiver persoonlijke of huishoudelijke aard. Daarnaast kan ook het *intern* verstrekken alleen plaatsvinden als daar een wettelijke grondslag voor bestaat. Het 'zuiver persoonlijke' houdt op vanaf het moment dat die gegevens worden opgeslagen op het informatiesysteem van de organisatie en/of op het moment dat de informatie extern of intern wordt doorgezonden. Zuiver persoonlijk gebruik vormt alleen een wettelijke grondslag voor interne aantekeningen, oftewel aantekeningen die niet (digitaal) toegankelijk zijn voor derden en ook géén onderdeel vormen van een bestand (waaronder een dossier).

2 Vallen de persoonsgegevens onder een geheimhoudingsplicht en zo ja, kan deze worden doorbroken?

Op een aantal publieke en private partijen met een meldpunt- of coördinatiefunctie rust een algemene of specifieke geheimhoudingsplicht. Het is dus altijd van belang om na te gaan of een geheimhoudingsplicht van kracht is, en zo ja, of deze mag worden doorbroken.

>Lees meer over geheimhoudingsplichten en beroepsgeheim

Enkele voorbeelden van geheimhoudingsplichten die relevant kunnen zijn:

- Op iedereen die als (onderdeel van een) bestuursorgaan of als daarvoor werkzame persoon (in welke rechtsverhouding ook) in aanraking komt met vertrouwelijke gegevens rust in beginsel de algemene geheimhoudingsplicht van de Algemene wet bestuursrecht. Deze geheimhoudingsplicht houdt in dat zij ten aanzien van die vertrouwelijke informatie verplicht zijn tot geheimhouding, tenzij de verstrekking:
  - wettelijk verplicht is, of
  - noodzakelijk is voor de uitvoering van de wettelijke, publieke taak van het betreffende bestuursorgaan.

  Uitgangspunt daarbij is dat als er sprake is van een **>verenigbare verdere verwerking**, deze geheimhoudingsplicht geen beletsel vormt voor de verstrekking van de persoonsgegevens aan een ander persoon of orgaan, mits de ontvanger zelf ook beschikt over een *eigen* wettelijke grondslag om de persoonsgegevens te verwerken.
- Partijen in het sociaal domein of in de zorg kunnen gebonden zijn aan een specifieke geheimhoudingplicht of het medisch beroepsgeheim op grond van de Wmo 2015 of Jeugdwet (**>zie uitgebreider paragraaf 10.4, stap 2**).

Praktijkvoorbeeld – Veilig Thuis

Veilig Thuis is gebonden aan de geheimhoudingsplicht van art. 5.3.3 Wmo 2015. Uitgangspunt is dat gegevens alleen aan anderen mogen worden verstrekt als de betrokkene daarvoor toestemming heeft gegeven. Bij een *jongere* dient de wettelijk vertegenwoordiger van deze betrokkene toestemming te geven. Als de betrokkene geen toestemming geeft voor de verstrekking van zijn persoonsgegevens, kan dit alleen plaatsvinden als de verstrekking door de Wmo 2015 is toegestaan. Zo mag Veilig Thuis bijvoorbeeld de geheimhoudingsplicht doorbreken om hulpverleners, de politie of de raad voor de kinderbescherming in te schakelen zonder toestemming van de betrokkene (art. 4.1.1 lid 2, aanhef en onder d en d, Wmo 2015).

3 Als er bijzondere persoonsgegevens worden verstrekt, is er een wettelijke grondslag die het verbod om bijzondere persoonsgegevens te verwerken doorbreekt?

Bij de mogelijkheden voor het verstrekken van bijzondere persoonsgegevens dient een onderscheid gemaakt te worden tussen de publieke en de private partijen.

>Wat zijn bijzondere persoonsgegevens?

Publieke partijen

Publieke partijen met een meldpunt- of coördinatiefunctie dienen steeds aan de hand van de toepasselijke sectorale regelgeving vast te stellen of een dergelijke **>doorbrekingsgrond** bestaat. In veel gevallen zal de verstrekking van bijzondere persoonsgegevens alleen plaats kunnen vinden na de **>uitdrukkelijke toestemming** van de betrokkene. Een expliciete wettelijke grondslag voor de verstrekking van bijzondere persoonsgegevens is namelijk vaak niet aanwezig.

Praktijkvoorbeeld – Veilig Thuis

Veilig Thuis vormt een uitzondering en mag zonder toestemming persoonsgegevens van personen die betrokken zijn bij huiselijk geweld of kindermishandeling aan derden verstrekken als uit een melding een vermoeden van huiselijk geweld of kindermishandeling kan worden afgeleid. De verwerking moet dan wel noodzakelijk zijn voor de taak van Veilig Thuis. Die is in de eerste plaats om als meldpunt op te treden voor gevallen of vermoedens van huiselijk geweld of kindermishandeling. Deze misdrijven kunnen een overlap hebben met mensenhandel, maar het aantal situaties waarbij politiegegevens over mensenhandel met Veilig Thuis gedeeld mogen worden blijft daarom dus beperkt tot die gevallen waarin er sprake is van overlap.

Een belangrijk aandachtspunt is de verwerking van bijzondere persoonsgegevens door zorgcoördinatoren, aandachtsfunctionarissen mensenhandel en ketenregisseurs. Zij hebben daarvoor géén expliciete eigen **>wettelijke, publieke taak**. Alleen als ze werkzaam zijn bij een gemeente kunnen ze in sommige gevallen bijzondere persoonsgegevens verwerken. De gemeente moet hiervoor dan over een zelfstandige **>doorbrekingsgrond** beschikken. Daar is in veel gevallen géén sprake van. Bij een zorgcoördinator bijvoorbeeld is een dergelijke doorbrekingsgrond alleen aanwezig voor zover zijn taak kan worden aangemerkt als een beoordeling van de hulp die een persoon op grond van de Wmo 2015 nodig heeft. In dat geval kan een zorgcoördinator waarschijnlijk een beroep doen op de verwerkingsgrondslagen van de gemeente als beschreven in de Wmo 2015 (met name art. 5.1.1 Wmo 2015). Of daar sprake van kan zijn, is ook afhankelijk van de precieze vormgeving van de functie van *zorgcoördinator*.

***Praktijkvraag** – In hoeverre beschikt een aandachtsfunctionaris mensenhandel of een ketenregisseur over een wettelijke taak om persoonsgegevens te verwerken ter bestrijding van mensenhandel?*
Veel gemeenten hebben een *aandachtsfunctionaris mensenhandel* aangesteld die interne en externe signalen ontvangt en beoordeelt. Soms worden deze door de aandachtsfunctionaris ook voor advies voorgelegd aan een *ketenregisseur*. Ketenregisseurs treden op als schakel tussen de ketenpartners binnen de zorg- en hulpverlening en de ketenpartners werkzaam voor overheid en justitie, adviseren de gemeente en bewaren soms ook signalen om na verloop van tijd bij de gemeente te checken of ze verder zijn geholpen (of het signaal opgewerkt is tot casus, de conclusie getrokken is dat er niks aan de hand is of dat er wél een probleem is, maar geen mensenhandel).

De functie van aandachtsfunctionaris mensenhandel en ketenregisseur betreffen echter géén expliciet bij wet aan de gemeente opgedragen taken. De rol van gemeenten bij de bestrijding van mensenhandel is alleen beleidsmatig 'toegewezen'. Hierdoor is het vaak zeer de vraag of de aandachtsfunctionaris en de ketenregisseur deze verwerkingen kunnen baseren op de wettelijke, publieke taak van de gemeente (**>grondslag (e)**). In het verlengde daarvan lijken ook de andere **>wettelijke grondslagen** geen soelaas te bieden. Een en ander zou naar het lijkt alleen anders zijn als de aandachtsfunctionaris en de ketenregisseur tot primaire taak hebben om de toeleiding naar zorg of sociale voorzieningen te borgen (in welk geval zij de verwerkingen mogelijk kunnen baseren op het uitvoeren van de Wmo 2015 of de Jeugdwet). Het enkele verzamelen van signalen kan echter niet als een dergelijke taak worden aangemerkt.

In uitzonderlijke gevallen kan de verstrekking worden gebaseerd op de bescherming van een vitaal belang van de betrokkene of van een ander persoon. Er moet dan een dringende noodzaak zijn om de gegevens van de betrokkene te verwerken, terwijl de betrokkene fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is toestemming te geven.

Praktijkvoorbeeld – Vitale belangen van een zwaar getraumatiseerde slachtoffer
Het kan voorkomen dat een slachtoffer dermate getraumatiseerd is dat hij niet reageert en dus ook géén toestemming kan geven voor het verwerken zijn persoonsgegevens. Als er een medische noodzaak bestaat kan het verstrekken van bijzondere persoonsgegevens in dat geval gebaseerd worden op de bescherming van de vitale belangen van het slachtoffer.

Private partijen
Voor private partijen met een meldpunt- of coördinatiefunctie geldt dat zij vrijwel alleen bijzondere persoonsgegevens mogen verstrekken als zij daarvoor **>uitdrukkelijke toestemming** hebben van de betrokkene.

Daarnaast kunnen ook private partijen in uitzonderlijke gevallen, en onder de voorwaarden zoals hierboven uiteengezet, de verstrekking baseren op de bescherming van de vitale belangen van de betrokkene of van een ander persoon.

4 Als er strafrechtelijke persoonsgegevens verstrekt worden, is daar een wettelijke grondslag voor?

De publieke en private partijen met een meldpunt- of coördinatiefunctie dienen kritisch te bekijken of zij ook strafrechtelijke persoonsgegevens aan derden mogen verstrekken.

>Wat zijn strafrechtelijke persoonsgegevens?

In veel gevallen ontbreekt een expliciete wettelijke grondslag voor de verstrekking. Dit betekent dat dan teruggevallen moet worden op de algemene grondslagen. Enkele voorbeelden zijn:

- Een slachtoffer van mensenhandel geeft **>uitdrukkelijke toestemming** voor het verstrekken van zijn persoonsgegevens aan een derde, bijvoorbeeld de politie.
- De verwerking is noodzakelijk voor de bescherming van de vitale belangen van de betrokkene of van een ander persoon, terwijl de betrokkene fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is toestemming te geven.
- Als de partij met de meldpunt- of coördinatiefunctie strafrechtelijke gegevens heeft verkregen van de politie en deze verder wil verstrekken aan een derde, dan kan dat als de geheimhoudingsplicht van de Wet politiegegevens (Wpg) deze verdere verstrekking toelaat. Dat mag als het verstrekken van die politiegegevens wettelijk verplicht is of als dat noodzakelijk is voor de uitvoering van zijn taak.
- De verwerking gebeurt door of voor publiekrechtelijke samenwerkingsverbanden (zoals het RIEC, het Veiligheidshuis of het Expertisecentrum Mensenhandel en Mensensmokkel (EMM)). Daarbij gelden de volgende twee voorwaarden:
  1. De verwerking is *noodzakelijk* voor het uitvoeren van de taak van het samenwerkingsverband.
  2. Bij de uitvoering van de samenwerking wordt voorzien in zodanige waarborgen dat de persoonlijke levenssfeer niet onevenredig wordt geschaad.

***Praktijkvraag** – Wat mogen partijen binnen het RIEC delen?*

Antwoord – Het doel van de RIEC's is de bestuurlijke en geïntegreerde aanpak van de georganiseerde criminaliteit invulling te geven, waarbij ook specifiek aandacht wordt besteed aan mensenhandel. Een van de werkprocessen die in dat kader plaatsvindt is het verrichten van integrale casusanalyses ten behoeve van het bepalen en uitvoeren van gezamenlijke interventiestrategieën door de *deelnemende partijen*.

Iedere partij moet per concrete casusanalyse vaststellen of, en zo ja in hoeverre het een mogelijkheid heeft om ten behoeve van de casusanalyse persoonsgegevens met de andere deelnemers te delen. Dit kan uiteraard enorm vereenvoudigd worden als teruggevallen wordt op een uitgewerkt protocol dat voor de vaste deelnemers uiteenzet wat de verschillende deelnemers aan elkaar mogen verstrekken, hoe gegevens met elkaar worden gedeeld en vastgelegd en welke waarborgen worden getroffen die de toegang tot deze gegevens strikt beperkt tot de deelnemers die over een wettelijke grondslag beschikken.

Belangrijk hierbij is om op te merken dat met een convenant en privacyprotocol, zoals RIEC-LIEC-convenant en het Privacyprotocol gegevensverwerking, géén nieuwe wettelijke grondslagen worden gecreëerd. Het gaat slechts om een concretisering van reeds bestaande wettelijke grondslagen.

Een 'verruiming' tot gegevensuitwisseling die wél optreedt bij het toetreden tot een samenwerkingsverband zoals een RIEC, is dat sommige wetten een expliciete wettelijke grondslag bevatten voor de verstrekking van gegevens aan dergelijke samenwerkingsverbanden of voor het (daartoe) doorbreken van een geheimhoudingsplicht. Zie bijvoorbeeld art. 20 Wpg dat bepaalt dat politiegegevens onder voorwaarden structureel mogen worden verstrekt aan samenwerkingsverbanden.

***Praktijkvraag** – Wat mag een RIEC met een ander RIEC delen?*

Antwoord- In beginsel dient het RIEC enkel binnen zijn eigen samenwerkingsverband persoonsgegevens te delen. Aannemelijk is evenwel dat in specifieke situaties informatie kan worden gedeeld met een andere RIEC. Bijvoorbeeld omdat bij een casusanalyse blijkt dat het signaal (ook) betrekking heeft op een andere regio. Van belang daarbij is dat het RIEC de verstrekking beperkt tot de informatie die strikt noodzakelijk is voor het RIEC waaraan verstrekt wordt. Een dergelijke noodzaak zal pas bestaan als in voldoende mate is vastgesteld dat de signalen daadwerkelijk relevant zijn en betrekking hebben op daders in de desbetreffende regio.

5 Kan de verstrekking van de persoonsgegevens worden gebaseerd op een wettelijke grondslag?

Bij de vraag of er een **>wettelijke grondslag** voor het verstrekken is, dient een onderscheid te worden gemaakt tussen publieke en private partijen.

Publieke partijen
In de meeste gevallen is er alleen een wettelijke grondslag voor de verstrekking van persoonsgegevens als de verwerking noodzakelijk is voor de uitvoering van de *eigen* wettelijke, publieke taak **>(grondslag (e))**.

In uitzonderlijke gevallen kan de verstrekking plaatsvinden als die noodzakelijk is voor de bescherming van de vitale belangen van de betrokkene of van een ander persoon. Daarbij geldt dan dat de betrokkene zelf fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is zijn toestemming te geven (grondslag (d)).

Praktijkvoorbeeld – Veilig Thuis

Veilig Thuis mag zonder toestemming persoonsgegevens van personen die betrokken zijn bij huiselijk geweld of kindermishandeling aan derden verstrekken als uit een melding een vermoeden van huiselijk geweld of kindermishandeling kan worden afgeleid. De verwerking moet dan wel noodzakelijk zijn voor de taak van Veilig Thuis. Die is in de eerste plaats om als meldpunt op te treden voor gevallen of vermoedens van huiselijk geweld of kindermishandeling. Deze misdrijven kunnen een overlap hebben met mensenhandel, maar het aantal situaties waarbij politiegegevens over mensenhandel met Veilig Thuis gedeeld mogen worden blijft daarom dus beperkt tot die gevallen waarin er van die overlap sprake is.

Praktijkvoorbeeld – Wettelijke verplichting vordering opsporingsambtenaren of officier van justitie

Er is een wettelijke verplichting (grondslag (c)) tot het verstrekken van persoonsgegevens aanwezig als een opsporingsambtenaar of de Koninklijke Marechaussee in het kader van een strafrechtelijk onderzoek naar mensenhandel gegevens vordert (art. 126nd Wetboek van Strafvordering). Voor ambtenaren geldt daarnaast dat op verzoek van de officier van justitie alle inlichtingen verstrekt moeten worden met betrekking tot strafbare feiten met de opsporing waarvan zij zelf niet zijn belast (art. 162 lid 2 Wetboek van Strafvordering).

Praktijkvoorbeeld – Overdracht van dossier zorgcoördinator bij vertrek slachtoffer naar andere regio

Als een slachtoffer van mensenhandel verhuist naar een andere regio, dan geldt als uitgangspunt dat de zorgcoördinator toestemming moet hebben van de betrokkene om het dossier te verstrekken aan een zorgcoördinator in de andere regio. In principe kan de zorgcoördinator dus niet ‘uit bezorgdheid’ zonder overleg met de betrokkene informatie met een zorgcoördinator in die regio delen. Het zonder toestemming van de

betrokkene verstrekken van dergelijke informatie is dan alleen denkbaar als kan worden gesproken van een situatie waarin een **>'conflict van plichten'** kan worden aangenomen. De zorgcoördinator moet dan kunnen aangeven dat er ernstig gevaar op fysieke of psychische schade bestaat voor (de gezondheid van) de betrokkene of anderen. Bij een zorgcoördinator die werkzaam is bij een private zorginstelling kan er in uitzonderlijke omstandigheden ook sprake is zijn van een gerechtvaardigd belang **>(grondslag (f))** om persoonsgegevens te delen.

Private partijen

Private partijen met een meldpunt- of coördinatiefunctie kunnen persoonsgegevens in de meeste gevallen alleen verwerken als er toestemming is van de betrokkene **>(grondslag (a))**.

⚠ Toestemming kan alleen een grondslag vormen voor de eigen persoonsgegevens van de betrokkene. Het verstrekken van persoonsgegevens over een derde (bijvoorbeeld een dader) kan dus géén toereikende grondslag vormen. Het verstrekken van persoonsgegevens van de dader zal daarom altijd gebaseerd moeten zijn op **>grondslag (c)** (wettelijke verplichting) of, in het geval van een overheidsinstantie, op **>grondslag (e)** (wettelijke, publieke taak) dan wel, in het geval van een private partij, op **>grondslag (f)** (gerechtvaardigd belang).

Soms kan het verstrekken van signalen van mensenhandel gebaseerd worden op het gerechtvaardigde belang van een derde (**>grondslag (f)**). Een derde kan het slachtoffer van mensenhandel zelf zijn, andere instanties of de ontvanger. Het kan daarbij gaan om het gerechtvaardigde belang van het slachtoffer, het algemene belang dat mensenhandel zoveel mogelijk moet worden voorkomen (ten aanzien waarvan de beoogde ontvanger dan wel een **>wettelijke, publieke taak** moet uitvoeren) of het specifieke belang van de ontvanger (bijvoorbeeld de registratie van dergelijke meldingen).

De gegevensverwerking moet daarbij dan noodzakelijk zijn om dat belang te behartigen. De verstrekking kan bovendien alleen plaatsvinden als het gerechtvaardigde belang zwaarder weegt dan de belangen van de betrokkene. Dit houdt in dat deze grondslag niet gebruikt kan worden als de belangen, rechten en fundamentele vrijheden van de betrokkene (hier: het slachtoffer of de daders over wie gegevens verstrekt worden) zwaarder wegen dan het belang om (mogelijke) slachtoffers te beschermen en de belangen die de ontvangende partij heeft. Uitganspunt blijft overigens dat, waar mogelijk, de betrokkene wordt gevraagd om **>toestemming** voor het delen van de informatie.

>Waar moet op gelet worden bij de belangenafweging?

⚠ Vanwege het feit dat de wetgever de rechtsgrond bepaalt voor de verwerking van persoonsgegevens door overheidsinstanties, is de rechtsgrond 'gerechtvaardigd belang' niet van toepassing op verwerkingen door overheidsinstanties in het kader van de uitvoering van hun taken.

Praktijkvoorbeeld – De Stichting Meld Misdaad Anoniem

De Stichting Meld Misdaad Anoniem (M) betreft een meldlijn voor burgers om anoniem informatie over criminaliteit door te geven. M. verzamelt deze informatie en verstrekt deze gegevens vervolgens aan politie, inlichtingdiensten en andere relevante organisaties. De stichting heeft met de betreffende partijen overeenkomsten gesloten om waarborgen te treffen voor een verantwoord en zorgvuldig gebruik van deze gegevens. Het verwerken van persoonsgegevens kan worden gebaseerd op het algemene belang (grondslag (e)) dat criminaliteit wordt bestreden en het belang dat dergelijke signalen tijdig terecht komen bij de politie.
De Autoriteit Persoonsgegevens (destijds nog het College Bescherming Persoonsgegevens) heeft dit bevestigd. De algemene belangen prevaleren volgens de Autoriteit Persoonsgegevens boven de belangen van de degenen over wie meldingen worden gedaan. In deze afweging komt veel

gewicht toe aan de waarborgen die de partijen waaraan M. verstrekt bieden.

***Praktijkvraag** – Mag een baliemedewerker signalen van mensenhandel intern bespreken en delen met de politie?*

Antwoord – Als een baliemedewerker bij het uitvoeren van zijn werk op informatie stuit die mogelijk relevant is voor opsporingsambtenaren, zoals die van de politie, mag hij deze informatie met een opsporingsambtenaar delen als die verstrekking op de aangiftebevoegdheid van art. 161 Wetboek van Strafvordering gebaseerd kan worden. De gemeente mag echter géén zelfstandig register van signalen bijhouden, ook niet op de 'G-schijf'. Aannemelijk is evenwel dat een mogelijk signaal wél eerst kortstondig intern kan worden besproken ('sparren'), voordat wordt besloten of het zinvol is dat de baliemedewerker het zelf of door tussenkomst van bijvoorbeeld de aandachtsfunctionaris mensenhandel of ketenregisseur doorgeeft.

***Praktijkvraag** – In hoeverre mogen medewerkers van lagere en middelbare scholen en hoger onderwijs signalen van mensenhandel verzamelen en verstrekken aan derden?*

Antwoord – De directie heeft – als bevoegd gezag van een lagere of middelbare school – de taak om de veiligheid en het welzijn van leerlingen op school te borgen. Het gaat daarbij om de sociale, psychische en fysieke veiligheid van leerlingen. Hoewel dit met name ziet op de veiligheid binnen de desbetreffende school, zal in het veiligheidsbeleid aandacht moeten zijn voor het herkennen van signalen van mensenhandel. De bestrijding van mensenhandel vormt géén expliciete taak van de school. Wél is het gebruik van de meldcode voor huiselijk geweld en kindermishandeling verplicht gesteld voor medewerkers van de school (art. 4b van de Wet op het primair onderwijs en art. 3c van de Wet op het voortgezet onderwijs.). Bij het doorlopen van de stappen van de meldcode mag de school signalen van huiselijk geweld of kindermishandeling in kaart brengen. Dit kan een overlap hebben met mensenhandel. Als de school hier een medewerker voor heeft aangesteld – bijvoorbeeld een aandachtfunctionaris – dan mag deze een overzicht bij houden van dossiers en relevante signalen van huiselijk geweld en kindermishandeling. Dit kan dus ook om signalen van mensenhandel gaan, voor zover er een overlap bestaat met huiselijk geweld of kindermishandel.

Aannemelijk is ook dat bij strafbare feiten op grond van artikel 161 Wetboek van Strafvordering aangifte kan worden gedaan bij de politie.

Ook voor private partijen geldt dat in uitzonderlijke gevallen de verstrekking kan plaatsvinden als die noodzakelijk is voor de bescherming van de vitale belangen van de betrokkene of van een ander persoon (grondslag (d)). Daarbij geldt dan dat de betrokkene zelf fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is zijn toestemming te geven.

6 Staat het doelbindingsbeginsel de verstrekking ('verdere verwerking') van de persoonsgegevens toe?

Het delen van signalen en meldingen van mensenhandel is een 'verdere verwerking'. Behoudens voor de politie, de Koninklijke Marechaussee en bijzondere opsporingsdiensten zoals de ISZW-DO – welke in **>paragraaf 10.2** zijn behandeld – worden de persoonsgegevens waar het om gaat namelijk voor een ander doel verstrekt (bijvoorbeeld voor de opsporing van strafbare feiten), dan waarvoor ze oorspronkelijk zijn verzameld.

Als je op basis van stap 5 hebt vastgesteld dat er een wettelijke grondslag aanwezig is voor de verstrekking van de persoonsgegevens, dan is de verdere verwerking in ieder geval toegestaan. Als een dergelijke wettelijke grondslag ontbreekt, dien je te toetsen of de verdere verwerking in overeenstemming met het doelbindingsbeginsel kan plaatsvinden.

De verdere verwerking is op een enkele uitzondering na alleen toegestaan als dit op grond van de **>verenigbaarheidscriteria** als 'verenigbare verwerking' kan worden beschouwd.

>Wat is het doelbindingsbeginsel?

Een relevante wettelijke grondslag die de verdere verwerking van persoonsgegevens ook toestaat is de aangiftebevoegdheid (art. 161 Wetboek van Strafvordering). Deze biedt de mogelijkheid om aangifte te doen van strafbare feiten en zo informatie aan de politie of bijzondere opsporingsdiensten te verstekken.

⚠ De verdere verwerking van signalen die in het kader van het sociaal domein zijn verkregen zullen door de strikte doelbinding en de geheimhoudingsplichten vaak niet voor verstrekking voor een ander doel in aanmerking komen. Een voorbeeld daarvan is art. 74 lid 2 Wet SUWI dat bepaalt dat gegevens die in het kader van de uitvoering van deze wet worden verwerkt niet mogen worden verstrekt aan derden, tenzij een wettelijke verplichting tot bekendmaking verplicht of de betrokkene schriftelijk toestemming heeft verleend.

7 Wordt er niet meer verstrekt dan de strikt noodzakelijke persoonsgegevens (need to know, in plaats van nice to know)?

Als uit voorgaande stappen volgt dat de verstrekking plaats kan vinden geldt verder nog dat de concrete verstrekking moet voldoen aan het **>noodzakelijkheidsbeginsel**.

Hieruit volgt dat de privacyinbreuk die gepaard gaat met de verstrekking van de persoonsgegevens evenredig moet zijn met het doel waarvoor de persoonsgegevens worden verstrekt (de zorg voor het slachtoffer van mensenhandel of de bestrijding van mensenhandel). Daarnaast mag een partij alleen gegevens verstrekken als het doel niet met minder vergaande maatregelen kan worden bereikt ('subsidiariteit').

Het noodzakelijkheidsbeginsel heeft ook gevolgen voor de omvang en de aard van de persoonsgegevens die door de betreffende partij mogen worden verstrekt. De persoonsgegevens dienen toereikend en direct relevant te zijn en moeten beperkt blijven tot het strikt noodzakelijke. Dit houdt in dat alleen '*need to know*'-informatie verstrekt mag worden (en dus geen '*nice to know*'-informatie).

Kort en goed gelden de volgende uitgangspunten:
- Ga alleen over tot verstrekking van die persoonsgegevens zonder welke de ontvanger zijn taak niet kan uitvoeren.
- Controleer of de gegevens toereikend, echt relevant en niet bovenmatig zijn.
- Stel vast of er geen minder ingrijpende middelen voorhanden zijn.
- Houd bij iedere verstrekking rekening met de verwachting van de betrokkene, de eigen belangen en die van de ontvanger.
- Controleer altijd of de gegevens betrekking hebben op de juiste persoon.
- Controleer of de gegevens betrouwbaar, juist en nauwkeurig zijn aan de hand van al beschikbare bronnen (zachte informatie die niet te verifiëren is moet in beginsel niet worden verstrekt aan derden).
- Vermeld bij de gegevens eventuele contextinformatie als die noodzakelijk is voor de ontvanger om de gegevens goed te begrijpen.

8 Moet de betrokkene worden geïnformeerd over de verstrekking of bestaat daarop een uitzondering?

De verstrekkende partij is verplicht om de betrokkene te informeren over het verstrekken van zijn persoonsgegevens (art. 13 AVG). Als de persoonsgegevens niet van de betrokkene zelf zijn ontvangen moet de verwerkingsverantwoordelijke de betrokkene ook informeren over (art. 14 AVG):
- Het soort persoonsgegevens.

- De bron waar de persoonsgegevens vandaan komen en of de gegevens afkomstig zijn van openbare bronnen.

De verstrekkende partij hoeft de betrokkene niet te informeren als:
- De betrokkene al op de hoogte is van de informatie die anders verstrekt wordt (art. 13 lid 4 AVG en art. 14 lid 5, aanhef en onder a, AVG).
- Het voldoen aan de informatieverplichting de doelen van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (deze uitzondering geldt overigens alleen als de gegevens *niet* bij de betrokkene zelf zijn verkregen). Deze situatie kan zich bijvoorbeeld voordoen als informeren ertoe leidt dat een slachtoffer van mensenhandel in gevaar komt.
- Zich een situatie voordoet waarbij het niet informeren van de betrokkene noodzakelijk en evenredig is voor bijvoorbeeld:
  - de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten (art. 23 AVG jo. art. 41 lid 1, aanhef en onder d, Uitvoeringswet AVG (UAVG));
  - een taak op het gebied van toezicht (art. 23 AVG jo. art. 41 lid. 1 aanhef en onder h, UAVG), of
  - de bescherming van de betrokkene of van de rechten en vrijheden van anderen (art. 23 AVG jo. art. 41 lid 1, aanhef en onder j, UAVG).

10.6 Niet-strafrechtelijke partners binnen de vreemdelingenketen

Binnen de vreemdelingenketen werken verschillende partijen onder de regie van het ministerie van Justitie en Veiligheid aan de uitvoering van het vreemdelingenrecht:
- De politie (Afdeling Vreemdelingenpolitie, Identificatie en Mensenhandel (AVIM)) houdt toezicht op de naleving van de Vreemdelingenwet.
- De Koninklijke Marechaussee is onder meer belast met het grenstoezicht.
- De Immigratie- en Naturalisatiedienst (IND) behandelt alle aanvragen van vreemdelingen die in Nederland willen verblijven of die Nederlander willen worden. Ook is de IND verantwoordelijk voor de uitvoering van de verblijfsregeling voor slachtoffers en getuige-aangevers van mensenhandel.
- Het Centraal Orgaan opvang asielzoekers (COA) zorgt voor de opvang en begeleiding van vreemdelingen.
- De Dienst Terugkeer en Vertrek van het ministerie van Justitie en Veiligheid regisseert het daadwerkelijk vertrek van de vreemdelingen die geen recht hebben op verblijf in Nederland.

In deze paragraaf gaan we in op de uitwisseling van persoonsgegevens door deze partijen onderling en door deze partijen met derden buiten de vreemdelingenketen.

1 Is de AVG of de Wet politiegegevens (Wpg) van toepassing op de verstrekking?

Het verwerken van persoonsgegevens door partijen in de vreemdelingenketen valt onder de AVG. Het gaat hier namelijk om persoonsgegevens die de partijen bij de uitvoering van hun bestuursrechtelijke bevoegdheden in het kader van het uitvoeren van 'VW-taken' hebben verkregen.

Let op!

De politie en de Koninklijke Marechaussee hebben een dubbelrol. Enerzijds zijn zij belast met wettelijke taken voor de uitvoering van de Vreemdelingenwet. Deze verwerking valt onder de AVG en staat centraal in deze paragraaf. De **>strafrechtelijke taken** van de politie en de Koninklijke Marechaussee vallen onder de reikwijdte van de Wet politiegegevens (Wpg).

2 Vallen de persoonsgegevens onder een geheimhoudingsplicht en zo ja, kan deze worden doorbroken?

De Vreemdelingenwet bevat geen bijzondere geheimhoudingsplicht. Dit houdt in dat de partijen binnen de Vreemdelingenketen alleen zijn gebonden aan de algemene geheimhoudingsplicht van de Algemene wet bestuursrecht. Deze geheimhoudingsplicht houdt in dat een ambtenaar bij vertrouwelijke informatie verplicht is tot geheimhouding, tenzij de verstrekking:

- wettelijk verplicht is, of
- noodzakelijk is voor de uitvoering van de wettelijke, publieke taak van het bestuursorgaan.

Uitgangspunt daarbij is dat als er sprake is van een **>verenigbare verdere verwerking**, deze geheimhoudingsplicht geen beletsel vormt voor de verstrekking van de persoonsgegevens aan een ander persoon of orgaan, mits de ontvanger zelf ook beschikt over een *eigen* wettelijke grondslag om de persoonsgegevens te verwerken.

3 Als er bijzondere persoonsgegevens worden verstrekt, is er een wettelijke grondslag die het verbod om bijzondere persoonsgegevens te verwerken doorbreekt?

Binnen de vreemdelingenketen is er een algemene doorbrekingsgrond voor het verwerken van bijzondere persoonsgegevens (art. 107a lid 1 Vreemdelingenwet). De gegevens mogen worden verwerkt als dat noodzakelijk is voor het uitvoeren van de 'VW-taken':

- de doelmatige en doeltreffende uitvoering van de visumverlening;
- de grensbewaking;
- de toelating;
- het verblijf;
- de uitzetting van vreemdelingen, of
- het toezicht op grond van de Vreemdelingenwet of de Schengengrenscode.

>Wat zijn bijzondere persoonsgegevens?

⚠ Het COA kan geen beroep doen op art. 107a Vreemdelingenwet en moet daarom terugvallen op de algemene **>doorbrekingsgronden.**

Bijzondere persoonsgegevens kunnen door of namens de minister van Justitie en Veiligheid en de eerder beschreven partners binnen de Vreemdelingenketen worden verwerkt, met uitzondering van het COA (art. 107a lid 2 Vreemdelingenwet).

De bijzondere persoonsgegevens mogen ook worden verstrekt aan derden. Daarbij geldt:

1. de verwerking moet noodzakelijk zijn voor de doelmatige en doeltreffende uitvoering van de visumverlening, de grensbewaking, de toelating, het verblijf en de uitzetting van vreemdelingen en het toezicht op vreemdelingen op grond van de Vreemdelingenwet of de Schengengrenscode, en
2. de verstrekking van deze gegevens moet zijn geregeld in de Vreemdelingencirculaire 2000.

Het gaat bij deze 'derden' om de partijen die niet onder de minister van Justitie en Veiligheid vallen en niet zijn belast met het toezicht op en de uitvoering van de Vreemdelingenwet. Daarbij valt met name te denken aan de minister van Buitenlandse Zaken (en onder hem vallende ambtenaren) die met individuele ambtsberichten adviseert over asielaanvragen. Ook kan worden gedacht aan artsen van de GGD of van de Medische opvang asielzoekers. De wetgever sluit namelijk niet uit dat in een concreet geval een institutionele of particuliere derde met een bijzondere expertise de beschikking moet krijgen over bijzondere persoonsgegevens. In specifieke gevallen kan dit ook de Inspectie SZW zijn.

In uitzonderlijke gevallen kan de verstrekking worden gebaseerd op de bescherming van de vitale belangen van de betrokkene of van een ander persoon. Er moet dan een dringende noodzaak zijn om de gegevens van de betrokkene te verwerken, terwijl de betrokkene fysiek (bijvoorbeeld bewusteloos) of juridisch (bijvoorbeeld handelingsonbekwaam) niet in staat is toestemming te geven. Bij vitale belangen kan in de context van de vreemdelingenketen gedacht worden aan het verwerken van persoonsgegevens die

noodzakelijk zijn voor humanitaire doelen, waaronder het monitoren van epidemieën en de verspreiding daarvan of verwerking van persoonsgegevens in humanitaire noodsituaties, zoals natuurrampen of door de mens veroorzaakte rampen.

Praktijkvoorbeeld – Vitale belangen van een zwaar getraumatiseerd slachtoffer
Het kan voorkomen dat een slachtoffer dermate getraumatiseerd is dat hij niet reageert en dus ook geen toestemming kan geven voor het verwerken zijn persoonsgegevens. Als er een medische noodzaak bestaat kan het verstrekken van bijzondere persoonsgegevens in dat geval gebaseerd worden op de bescherming van de vitale belangen van het slachtoffer.

4 Als er strafrechtelijke persoonsgegevens verstrekt worden, is daar een wettelijke grondslag voor?

Binnen de vreemdelingenketen is er een algemene grondslag voor de verwerking van strafrechtelijke gegevens (art. 107a lid 1 Vreemdelingenwet). De gegevens mogen worden verwerkt als dat noodzakelijk is voor het uitvoeren van de *'VW-taken'*. +

>Wat zijn strafrechtelijke persoonsgegevens?

⚠ Het COA kan geen beroep doen op art. 107a Vreemdelingenwet en moet daarom terugvallen op de **>algemene grondslagen>**.

5 Kan de verstrekking van de persoonsgegevens worden gebaseerd op een wettelijke grondslag?

De belangrijkste informatiebron van de vreemdelingenketen is de *vreemdelingenadministratie*. + Deze wordt beheerd door de minister van Justitie en Veiligheid. De administratie bevat onder meer gezichtsopnamen en vingerafdrukken, andere persoons- en verwijsgegevens van vreemdelingen en andere persoonsgegevens die van belang zijn voor het uitvoeren van *'VW-taken'* + of de Rijkswet op het Nederlanderschap. De gegevens mogen worden verwerkt om de Vreemdelingenwet uit te kunnen voeren.

Aangezien de IND de *verblijfsvergunning voor bepaalde tijd* + verleent aan (vermoedelijke) slachtoffers en getuige-aangevers van mensenhandel (art. 3.48 Vreemdelingenbesluit), kan de vreemdelingenadministratie gegevens over mensenhandel bevatten. Het startpunt van zo'n traject kan zijn dat de Koninklijke Marechaussee de IND informeert bij signalen van mensenhandel over een vreemdeling die Nederland inreist. De IND verleent de bedenktijd alleen als het OM en de politie hiermee akkoord gaan. Ook in dat kader vindt gegevensuitwisseling plaats. De IND merkt bovendien een kennisgeving van aangifte of het verlenen van medewerking aan het strafproces ambtshalve aan als een aanvraag tot het verlenen van een verblijfsvergunning, zodra deze door de politie is doorgestuurd naar de IND.

De Vreemdelingenwet bevat diverse grondslagen voor de verstrekking van persoonsgegevens. Hierbij geldt dat de verstrekking niet mag plaatsvinden als de persoonlijke levenssfeer van de betrokkene daar onevenredig door wordt geschaad.

>Wat zijn verwerkingsgrondslagen?

De minister van Justitie en Veiligheid kan andere bestuursorganen (waaronder het COA) 'normale' persoonsgegevens uit de vreemdelingenadministratie verstrekken, zoals gegevens over de verblijfsrechtelijke positie van de vreemdelingen, als zij die nodig hebben voor de uitvoering van hun taak.

Gezichtsopnames en vingerafdrukken zijn hiervan uitgezonderd (art. 107 lid 4 Vreemdelingenwet). Gezichtsopnames en vingerafdrukken van vreemdelingen mogen wél beschikbaar worden gesteld voor bijvoorbeeld de opsporing en vervolging van mensenhandel en andere strafbare feiten (art. 107 lid 5 Vreemdelingenwet). Een dergelijke verstrekking vindt alleen plaats in geval van een misdrijf waarvoor voorlopige hechtenis is toegelaten, zoals mensenhandel, en na schriftelijke machtiging van de rechter-commissaris op vordering van de officier van justitie. Daarnaast dient er een redelijk vermoeden te bestaan dat:

a) de verdachte een vreemdeling is, of
b) dit noodzakelijk is in het belang van het onderzoek en het opsporingsonderzoek op een dood spoor is beland, dan wel snel resultaten nodig zijn voor de opheldering van het misdrijf.

Bestuursorganen zijn bevoegd uit eigen beweging en desgevraagd verplicht de minister van Justitie en Veiligheid de 'normale persoonsgegevens' en inlichtingen te verstrekken die de minister nodig heeft voor het uitvoeren van *'VW-taken'* en de Rijkswet op het Nederlanderschap.

Praktijkvoorbeeld – Wettelijke verplichting vordering opsporingsambtenaren of officier van justitie

Er is een wettelijke verplichting (grondslag (c)) tot het verstrekken van persoonsgegevens aanwezig als een opsporingsambtenaar of de Koninklijke Marechaussee in het kader van een strafrechtelijk onderzoek naar mensenhandel gegevens vordert (art. 126nd Wetboek van Strafvordering). Voor ambtenaren geldt daarnaast dat op verzoek van de officier van justitie alle inlichtingen verstrekt moeten worden met betrekking tot strafbare feiten met de opsporing waarvan zij zelf niet zijn belast (art. 162 lid 2 Wetboek van Strafvordering).

Praktijkvraag – Het COA krijgt regelmatig verzoeken van zorgcoördinatoren om informatie over vreemdelingen die slachtoffer zijn geworden van mensenhandel. *Hoe dient het COA om te gaan met deze verzoeken? Mag het COA informatie verstrekken aan zorgcoördinatoren?*

Antwoord – Hier doen zich twee problemen voor. Allereerst bestaat er geen wettelijke grondslag voor de verstrekking van persoonsgegevens door het COA aan zorgcoördinatoren. Dit is alleen anders als het slachtoffer **>toestemming** geeft voor de verstrekking. Daarbij geldt bovendien dat de zorgcoördinator in de meeste gevallen niet beschikt over een **>eigen toereikende wettelijke grondslag** om persoonsgegevens van slachtoffers van mensenhandel te verwerken. Dit is vrijwel alleen anders als het gaat om een zorgcoördinator werkzaam bij een private zorginstelling en sprake is van een gerechtvaardigd belang (grondslag (f)) of de verwerking kan worden gebaseerd op toestemming **>(grondslag (a))**.

Praktijkvraag – *In hoeverre mag het COA signalen van mensenhandel verstrekken aan Veilig Thuis?*

Antwoord – Het COA heeft onder meer de taak om de veiligheid en het vluchtelingen te borgen. Het gaat daarbij om de sociale, psychische en fysieke veiligheid van vluchtelingen. De bestrijding van mensenhandel vormt géén expliciete taak van het COA. Wél is het gebruik van de meldcode voor huiselijk geweld en kindermishandeling verplicht gesteld voor medewerkers van het COA (art. 9a Wet Centraal Orgaan opvang asielzoekers). Bij het doorlopen van de stappen van de meldcode mag het COA signalen van huiselijk geweld of kindermishandeling in kaart brengen. Dit kan dus ook om signalen van mensenhandel gaan, voor zover er een overlap bestaat met huiselijk geweld of kindermishandel.

6 Staat het doelbindingsbeginsel de verstrekking ('verdere verwerking') van de persoonsgegevens toe?

Het delen van signalen en meldingen van mensenhandel is een 'verdere verwerking', waarbij de persoonsgegevens waar het om gaat voor een ander doel worden verstrekt (bijvoorbeeld voor de opsporing van strafbare feiten), dan waarvoor ze oorspronkelijk zijn verzameld (uitvoering van 'VW-taken').

Als je op basis van stap 5 hebt vastgesteld dat er een wettelijke grondslag aanwezig is voor de verstrekking van de persoonsgegevens, dan is de verdere verwerking in ieder geval toegestaan. Als een dergelijke wettelijke grondslag ontbreekt, dien je te toetsen of de verdere verwerking in overeenstemming met het doelbindingsbeginsel kan plaatsvinden. Er dient daarbij onderscheid te worden gemaakt tussen de verstrekking van persoonsgegevens binnen de vreemdelingenketen (oftewel de verstrekking tussen partijen in de vreemdelingenketen voor het uitvoeren van '*VW-taken*' ⊕) en de verstrekking aan derden buiten de vreemdelingenketen.

>Wat is het doelbindingsbeginsel?

Het doelbindingsbeginsel staat de verstrekking van persoonsgegevens tussen partijen binnen de vreemdelingenketen voor het uitvoeren van hun 'VW-taken' niet in de weg als deze daarvoor noodzakelijk zijn. Het doelbindingsbeginsel vormt hier geen beletsel omdat de Vreemdelingenwet zelf diverse grondslagen bevat. Art. 107 lid 4 Vreemdelingenwet bepaalt dat gegevens en inlichtingen uit de vreemdelingenadministratie (met uitzondering van gezichtsopnames en vingerafdrukken) aan bestuursorganen kunnen worden verstrekt. De doelbinding volgt uit art. 107 lid 9 Vreemdelingenwet. Uit deze bepaling volgt dat onder meer het doorleveren van gegevens en de gevallen waarin het verstrekken van gegevens en inlichtingen in ieder geval plaats moet vinden, bij algemene maatregel van bestuur kunnen worden geregeld.

Doordat de doelbinding van de persoonsgegevens in de vreemdelingenadministratie strikt is geregeld bestaat er weinig ruimte om in andere, niet wettelijk geregelde gevallen terug te vallen op de algemene mogelijkheid om een verdere verwerking op grond van de **>verenigbaarheidscriteria** als verenigbare verwerking te beschouwen. Voor wat betreft biometrische gegevens heeft de wetgever zelfs uitdrukkelijk het standpunt ingenomen dat de verdere verwerking dient te volgen uit art. 107 Vreemdelingenwet. Aannemelijk is evenwel dat de IND het COA kan informeren over een signaal van mensenhandel, als dit nodig is voor het treffen van de nodige maatregelen voor deze personen in de opvang.

Een relevante wettelijke grondslag die de verdere verwerking van persoonsgegevens ook toestaat is de aangiftebevoegdheid (art. 161 Wetboek van Strafvordering). Deze biedt de mogelijkheid om aangifte te doen van strafbare feiten en zo informatie met de politie of bijzondere opsporingsdiensten te delen.

7 Wordt er niet meer verstrekt dan de strikt noodzakelijke persoonsgegevens (need to know, in plaats van nice to know)?

Als uit voorgaande stappen volgt dat de verstrekking plaats kan vinden geldt verder nog dat de concrete verstrekking moet voldoen aan het **>noodzakelijkheidsbeginsel**.

Hieruit volgt dat de privacyinbreuk die gepaard gaat met de verstrekking van de persoonsgegevens evenredig moet zijn met het doel waarvoor de persoonsgegevens worden verstrekt (de zorg voor het slachtoffer van mensenhandel of de bestrijding van mensenhandel). Daarnaast mag een partij alleen gegevens verstrekken als het doel niet met minder vergaande maatregelen kan worden bereikt ('subsidiariteit').

Het noodzakelijkheidsbeginsel heeft ook gevolgen voor de omvang en de aard van de persoonsgegevens die door de betreffende partij mogen worden verstrekt. De persoonsgegevens dienen toereikend en direct relevant te zijn en moeten beperkt blijven tot het strikt noodzakelijke. Dit houdt in dat alleen '*need to know*'-informatie verstrekt mag worden (en dus geen '*nice to know*'-informatie).

Kort en goed gelden de volgende uitgangspunten:

- Ga alleen over tot verstrekking van die persoonsgegevens zonder welke de ontvanger zijn taak niet kan uitvoeren.
- Controleer of de gegevens toereikend, echt relevant en niet bovenmatig zijn.
- Stel vast of er geen minder ingrijpende middelen voorhanden zijn.
- Houd bij iedere verstrekking rekening met de verwachting van de betrokkene, de eigen belangen en die van de ontvanger.
- Controleer altijd of de gegevens betrekking hebben op de juiste persoon.
- Controleer of de gegevens betrouwbaar, juist en nauwkeurig zijn aan de hand van al beschikbare bronnen (zachte informatie die niet te verifiëren is moet in beginsel niet worden verstrekt aan derden).
- Vermeld bij de gegevens eventuele contextinformatie als die noodzakelijk is voor de ontvanger om de gegevens goed te begrijpen.

Tips & Tricks

In de Vreemdelingencirculaire 2000 is aangegeven welke gegevens strikt noodzakelijk zijn voor het uitvoeren van *'VW-taken'*. Een voorbeeld is de uitwerking van de noodzakelijke gegevens voor de beoordeling van een verblijfsvergunning aan een slachtoffer of getuige-aangever van mensenhandel die geen aangifte kan of wil doen of geen medewerking kan of wil verlenen in verband met ernstige bedreiging of een medische of psychische beperking. De volgende bewijsmiddelen worden dan noodzakelijk geacht:

- een verklaring van de politie waaruit blijkt dat de vreemdeling slachtoffer is van mensenhandel, en
- als dit van toepassing is: een verklaring van de politie waaruit blijkt dat van de vreemdeling niet verwacht kan worden medewerking te verlenen aan het strafproces in verband met ernstige bedreigingen in Nederland door de mensenhandelaar (als deze verklaring wordt overgelegd, wordt hiermee ook aannemelijk geacht dat betrokkene zich niet aan de bedreigingen kan onttrekken als hij zich zou vestigen in het land van herkomst, omdat mensenhandelbendes vrijwel altijd opereren over de grenzen heen), en
- als dit van toepassing is: medische informatie waaruit blijkt dat een fysieke of psychische aandoening aan het verlenen van medewerking aan het strafproces in de weg staat (de medische informatie moet afkomstig zijn van een behandelaar die of in het register van Beroepen in de Individuele Gezondheidszorg of het register van het Nederlands Instituut van Psychologen is ingeschreven).

8 Moet de betrokkene worden geïnformeerd over de verstrekking of bestaat daarop een uitzondering?

De verstrekkende partij is verplicht om de betrokkene te informeren over het verstrekken van zijn persoonsgegevens (art. 13 AVG). Als de persoonsgegevens niet van de betrokkene zelf zijn ontvangen moet de verwerkingsverantwoordelijke de betrokkene ook informeren over (art. 14 AVG):

- Het soort persoonsgegevens.
- De bron waar de persoonsgegevens vandaan komen en of de gegevens afkomstig zijn van openbare bronnen.

De verstrekkende partij hoeft de betrokkene daarentegen niet te informeren als:

- De betrokkene al op de hoogte is van de informatie die anders verstrekt wordt (art. 13 lid 4 AVG en art. 14 lid 5, aanhef en onder a, AVG).
- Het voldoen aan de informatieverplichting de doelen van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen (deze uitzondering geldt overigens alleen als de gegevens *niet* bij de betrokkene zelf zijn verkregen). Deze situatie kan zich bijvoorbeeld voordoen als informeren ertoe leidt dat een slachtoffer van mensenhandel in gevaar komt.
- Zich een situatie voordoet waarbij het niet informeren van de betrokkene noodzakelijk en evenredig is voor bijvoorbeeld:
  - de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten (art. 23 AVG jo. art. 41 lid 1, aanhef en onder d, Uitvoeringswet AVG (UAVG));
  - een taak op het gebied van toezicht (art. 23 AVG jo. art. 41 lid. 1 aanhef en onder h, UAVG), of
  - de bescherming van de betrokkene of van de rechten en vrijheden van anderen (art. 23 AVG jo. art. 41 lid 1, aanhef en onder j, UAVG).

Checklist voor als het ‘verkeerd’ gaat

De vraag rijst welke stappen moeten worden gezet als achteraf is gebleken dat de verstrekking niet had mogen plaatsvinden. In een dergelijk geval kan het (samen met de functionaris voor gegevensbescherming) doorlopen van de volgende stappen helpen.

1. Beoordeel of de verstrekking is aan te merken als een datalek (art. 4 lid 12 AVG). In veel gevallen zal sprake zijn geweest van de ongeoorloofde of onrechtmatige verwerking van persoonsgegevens (aan een onbevoegde ontvanger). Dit betreft een inbreuk op de vertrouwelijkheid en daarmee een datalek.

2. Neem contact op met de partij aan wie de persoonsgegevens of het signaal is verstrekt en verzoek deze de informatie te verwijderen. Vraag in dat kader ook of de desbetreffende partij de informatie heeft (door) verstrekt. Voor zover dit het geval is, zorg (eventueel met hulp van de partij aan wie de gegevens oorspronkelijk zijn verstrekt) dat ook die ontvangers overgaan tot verwijdering van de desbetreffende informatie.

3. Beoordeel of het datalek meldingswaardig is en wie de melding doet. Een datalek dient bij de Autoriteit Persoonsgegevens te worden gemeld, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Als de melding een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet (in aanvulling op de melding bij de Autoriteit Persoonsgegevens) óók een melding worden gedaan bij de betrokkenen die door het datalek zijn getroffen.

4. Registreer het datalek in het datalekregister via het Meldloket datalekken Autoriteit Persoonsgegevens.

5. Beoordeel hoe en op welke wijze de betrokkene wordt geïnformeerd over de fout.

6. Voor zover de fout directe gevolgen heeft voor een strafrechtelijk onderzoek of de veiligheid van een slachtoffer van mensenhandel, tref de nodige spoedmaatregelen om eventuele schade te beperken.

7. Evalueer of de het incident aanleiding vormt om werkinstructies, het privacy protocol of bestaande convenanten aan te scherpen. Dit ter voorkoming van toekomstige fouten.

>>Checklist voor als het ‘verkeerd’ gaat

Deze brochure is een uitgave van:

Ministerie van Justitie en Veiligheid
Postbus 20301 | 2500 EH Den Haag
t 070 370 79 11 (ma t/m vrij 8.00 tot 20.00 uur)

Oktober 2020 | Publicatie-nr. 20405415