Bijlage

Algemeen juridisch kader gegevensuitwisseling

Europees Verdrag inzake de Rechten van de Mens (EVRM) en Handvest van de grondrechten van de Europese Unie (EU-Handvest)
De verwerking, waaronder de verzameling, van persoonsgegevens is een inmenging van in het privéleven in de zin van art. 8, lid 1, EVRM en, voor zover het gaat om gegevensverwerking waarop EU-recht van toepassing is, artikel 7 en 8 van het EU-Handvest. Art. 8, lid 2, EVRM vereist voor een gerechtvaardigde inbreuk op het recht van privacy allereerst dat deze inbreuk 'bij de wet voorzien' is, in een democratische samenleving noodzakelijk is in het belang van een aantal legitieme doelen. Artikel 8 van het EU-Handvest stelt vergelijkbare voorwaarden. De inmenging moet met voldoende nauwkeurigheid zijn geformuleerd om de burger zo goed mogelijk in staat te stellen zijn gedrag af te stemmen op het geldende recht (voorzienbaarheidseis). De legitieme doelen zijn de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of de bescherming van de rechten en vrijheden van anderen.
Wetgeving die de persoonlijke levenssfeer beperkt, moet volgens de jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) worden gerechtvaardigd door een dringende maatschappelijke behoefte en in overeenstemming zijn met de beginselen van proportionaliteit (de beperking mag niet onevenredig zijn in verhouding tot het nagestreefde doel) en de subsidiariteit (het nagestreefde doel moet niet op een voor de burger minder ingrijpende wijze kunnen worden bereikt).
In jurisprudentie van het EHRM, maar ook van Nederlandse rechters, is de afgelopen jaren duidelijk gemaakt dat, afhankelijk van de specifieke context, een toegespitste wettelijke grondslag voor de verwerking van persoonsgegevens is vereist.

De wettelijke grondslagen waarop de gegevensverwerking in het kader van de bestrijding van terrorisme is gebaseerd, komen hieronder aan de orde.

Algemene verordening gegevensbescherming en Uitvoeringswet (AVG, UAVG)
Een belangrijk deel van het nationaalrechtelijk kader voor de verwerking van persoonsgegevens staat sinds 25 mei 2018 in de Algemene verordening gegevensbescherming (AVG) en de bijbehorende Uitvoeringswet AVG (UAVG).[1] Tot dat moment gold de Wet bescherming persoonsgegevens (Wbp), die de implementatie vormde van de Europese dataprotectierichtlijn (Richtlijn 95/46/EG). De grondslagen voor de verwerking van persoonsgegevens zijn met de komst van de AVG niet fundamenteel veranderd.

Artikel 6 AVG is de bepaling waarin de grondslagen van de gegevensverwerking zijn opgenomen. De bepaling vormt een voortzetting en uitbreiding van artikel 7 Richtlijn 95/46/EG (waarop het oude artikel 8 Wbp was gebaseerd). Gegevensverwerking door de overheid is onder de AVG mogelijk als de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting (onderdeel c) of als de verwerking noodzakelijk is "voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen" (onderdeel e). De verwerking moet in deze gevallen altijd een wettelijke grondslag hebben. De AVG schrijft niet voor dat in de sectorspecifieke wetgeving expliciet is opgenomen dat ten behoeve van de wettelijke taak gegevens verwerkt mogen worden. Indien het noodzakelijk is om voor de uitvoering van de publieke taak persoonsgegevens te verwerken, kan de wettelijke grondslag voor de publieke taak tevens worden beschouwd als grondslag voor de verwerking van persoonsgegevens.[2] Deze lezing strookt ook met artikel 8, tweede lid, EVRM dat vereist dat een beperking van het recht op bescherming van het privéleven voorzienbaar moet zijn bij wet.

Voor het overgrote deel van de overheidsorganisaties vormt de AVG de grondslag voor de verwerking van persoonsgegevens. Zo verwerkt de NCTV persoonsgegevens voor zover dat noodzakelijk is voor de uitoefening van de taken die op grond van de Paspoortwet en de Tijdelijke

[1] De AVG is niet van toepassing op alle verwerkingen van persoonsgegevens (zie artikel 2 AVG). Gegevensverwerking door inlichtingen- en veiligheidsdiensten is op grond van artikel 4 lid 2 VEU een exclusieve verantwoordelijkheid van de lidstaten. Ook wordt in de AVG de verwerking van politiegegevens en justitiële en strafvorderlijke gegevens uitgezonderd; daarvoor geldt een aparte richtlijn. Richtlijn 2016/680. Zie voor deze categorieën de afzonderlijke beschrijving verderop in dit overzicht.
[2] Memorie van toelichting bij UAVG, Kamerstukken II 2017/18, 34851, nr. 3, p. 34-36.

wet bestuurlijke maatregelen terrorismebestrijding zijn toegekend aan de Minister van Justitie en Veiligheid. Zie voor een uitwerking daarvan verderop in dit overzicht.[3]

Artikel 6, eerste lid, onderdeel e, AVG biedt geen grondslag voor een derde om gegevens te verstrekken aan een bestuursorgaan voor de uitoefening van een publieke taak.[4] Een verwerkingsverantwoordelijke (in dit geval een bestuursorgaan) mag in beginsel alleen gegevens verwerken die voor zijn eigen publieke taak nodig zijn.[5] Dat compliceert de gegevensuitwisseling tussen bestuursorganen onderling. Artikel 6, vierde lid, bevat criteria aan de hand waarvan bepaald kan worden of een verdere verwerking van gegevens kan worden beschouwd als verenigbaar met het oorspronkelijk doel. Ook maakt deze bepaling het onder voorwaarden mogelijk af te wijken van het doelbindingsbeginsel, zodat het onder omstandigheden mogelijk is om gegevens verder te verwerken voor een doel dat onverenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld. Niet-verenigbare verdere verwerking is in slechts twee gevallen toegestaan: met uitdrukkelijke toestemming van de betrokkene dan wel op grond van een Unierechtelijke of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van een belangrijke doelstelling van algemeen belang als bedoeld in artikel 23, eerste lid, AVG.[6]

Wet politiegegevens (Wpg)
Voor zover de gegevens over aan terrorisme en extremisme gerelateerde personen worden verwerkt in het kader van de uitvoering van politietaak, valt de verwerking onder de reikwijdte van de Wet politiegegevens (Wpg).

De verstrekking van politiegegevens aan derden is geregeld in de artikelen 16-24 Wpg, en nader uitgewerkt in de paragrafen 4 en 5 van het Besluit politiegegevens (Bpg). De wet voorziet in de verstrekking van politiegegevens aan gezagsdragers (art. 16 Wpg). Verder voorziet de wet in de verstrekking van politiegegevens aan inlichtingen- en veiligheidsdiensten en aan buitenlandse opsporingsinstanties (art. 17 Wpg).[7]

De Wpg voorziet in een 'semi-gesloten' regime voor de verstrekking van politiegegevens aan derden. Dit wil zeggen dat politiegegevens vanwege een zwaarwegend algemeen belang kunnen worden verstrekt aan de belanghebbende personen en instanties die in de wet of het Besluit politiegegevens zijn aangewezen (paragraaf 4 Bpg). Toepassing van het criterium van het zwaarwegend algemeen belang impliceert een belangenafweging. Het belang dat gediend wordt met de verstrekking van de gegevens wordt afgewogen tegen het belang van de persoonlijke levenssfeer van degene op wie de politiegegevens betrekking hebben. Bij deze belangenafweging moeten ook de beginselen van proportionaliteit en subsidiariteit worden betrokken. Hieruit vloeit voort dat gegevens die minder ingrijpend zijn voor de persoonlijke levenssfeer, eerder mogen worden verstrekt, dan gegevens die meer ingrijpend zijn voor de persoonlijke levenssfeer. Bij de aanwijzing van personen en instanties op grond van dit besluit wordt telkens afgewogen of een zwaarwegend algemeen belang de verstrekking van politiegegevens nodig maakt.

De aanwijzing van de belanghebbende personen en instanties in paragraaf 4 Bpg is bedoeld voor de structurele verstrekking van politiegegevens op landelijk niveau. Dit betreft verstrekkingen binnen de strafrechtsketen en aan andere instanties waarmee de politie standaard samenwerkt, zoals de raad voor de kinderbescherming, reclasseringswerkers, de stichting slachtofferhulp Nederland en de Dienst Wegverkeer. Daarbij wordt onderscheid gemaakt tussen de politiegegevens die worden verwerkt op grond van artikel 13, eerste lid, onder a en d, Wpg, de artikelen 8 en 13, eerste lid, Wpg en de artikelen 8, 9, 10, eerste lid, onderdelen a en c, en 13 Wpg.

---

[3] Andere taken in het kader van de uitoefening van het openbaar gezag op grond waarvan de NCTV persoonsgegevens verwerkt zijn bevriezingsmaatregelen, maatregelen verankerd in het stelsel bewaken en beveiligen en in het kader van het ontnemen van het Nederlanderschap van personen die zich hebben aangesloten bij terroristische organisaties.
[4] Dit was anders onder de werking van artikel 8, onderdeel e, van de Wbp.
[5] Om dit te benadrukken geldt artikel 6, eerste lid, onderdeel f, AVG (gegevensverwerking in verband met gerechtvaardigd belang) niet voor de gegevensverwerking door overheidsinstanties in het kader van de uitoefening van hun taken.
[6] Zie uitgebreid de nota naar aanleiding van het verslag bij UAVG (Kamerstukken II 34851, nr. 7, p. 43-45).
[7] Op grond van artikel 24 Wpg kan aan de inlichtingen- en veiligheidsdiensten rechtstreeks geautomatiseerde toegang worden verleend. Dat wordt nader uitgewerkt in het (ontwerp) Besluit ex artikel 24 Wpg.

Ten behoeve van de flexibiliteit op regionaal of lokaal niveau biedt de Wpg de verwerkingsverantwoordelijke aanvullend de mogelijkheid te beslissen tot het verstrekken van gegevens aan andere personen of instanties. Ook hiervoor geldt het vereiste van een zwaarwegend algemeen belang. De verwerkingsverantwoordelijke kan slechts beslissen tot verstrekking in overeenstemming met het bevoegde gezag. Dit betreft de burgemeester of de officier van justitie, afhankelijk van de vraag of wordt opgetreden ter handhaving van de openbare orde of ter strafrechtelijke handhaving van de rechtsorde. In de eerste plaats kan de verwerkingsverantwoordelijke in bijzondere gevallen beslissen tot het verstrekken van politiegegevens aan andere personen en instanties (art. 19 Wpg). Dit betreft incidentele verstrekkingen. In de tweede plaats kan de verwerkingsverantwoordelijke besluiten tot het op structurele basis verstrekken van gegevens aan bepaalde partijen in het kader van een samenwerkingsverband (art. 20 Wpg). Deze mogelijkheid kan bijvoorbeeld uitkomst bieden als op regionaal niveau gedurende langere tijd intensief wordt samengewerkt met andere personen of instanties, bijvoorbeeld bij de aanpak van winkelcriminaliteit of bij de aanpak van de jeugdcriminaliteit. Als de verwerkingsverantwoordelijke op basis van deze artikelen beslist tot de verstrekking van politiegegevens, dan is de verstrekking in beginsel beperkt tot de politiegegevens die worden verwerkt overeenkomstig artikel 8 Wpg. De mogelijkheid tot verstrekking is gekoppeld aan bepaalde doelen, namelijk het opsporen van strafbare feiten, het handhaven van de openbare orde, de hulpverlening en het uitoefenen van toezicht op de naleving van wetgeving. Dit betekent dat gegevens verstrekt kunnen worden aan derden, zoals andere overheidsdiensten of instanties buiten de overheid, indien het doel van de verstrekking overeenstemt of verenigbaar is met de politietaak.

Wet justitiële en strafvorderlijke gegevens (Wjsg)

De verstrekking van justitiële gegevens is geregeld in de artikelen 8 t/m 17 Wjsg, waarin ook de instanties worden genoemd waaraan de gegevens kunnen worden verstrekt, vergelijkbaar met de Wpg. Een voorbeeld is art. 8 lid 4, dat bepaalt dat justitiële gegevens kunnen worden verstrekt aan een internationaal orgaan of aan een internationaal strafgerecht voor zover dit voortvloeit uit een verdrag. Een ander voorbeeld: justitiële gegevens kunnen ten behoeve van de strafrechtspleging worden verstrekt aan rechterlijke ambtenaren dan wel aan andere autoriteiten in het buitenland (art. 8 lid 5 Wjsg).
Voor strafvorderlijke gegevens geldt dat het College van procureurs-generaal als verantwoordelijke in bepaalde gevallen gegevens kan verstrekken (art. 39a t/m 39h Wjsg). Zie art. 39c voor de voornaamste eisen. Het college kan de gegevens, voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, op basis van art. 39e Wjsg verstrekken aan o.a. aan de Minister van Justitie en Veiligheid (sub b) en andere autoriteiten in het buitenland als bedoeld in onderdeel a en instanties die ingevolge het internationaal recht een taak hebben in het kader van de strafrechtspleging (sub j).
Op grond van de regeling van artikel 39f Wjsg kan het College van procureurs-generaal met het oog op een zwaarwegend algemeen belang strafvorderlijke gegevens verstrekken aan derden. De verstrekking is gebonden aan bepaalde doeleinden, die nauw samen hangen met de strafrechtspleging (onder meer het voorkomen en opsporen van strafbare feiten, het handhaven van de orde en veiligheid en het uitoefenen van toezicht op het naleven van regelgeving).
Ook hier is de gegevensverwerking nader uitgewerkt in een besluit; het Besluit justitiële en strafvorderlijke gegevens (Bjsg). Verstrekking van de justitiële gegevens is nader geregeld in art. 11 t/m 43 van het besluit. Voor wat betreft terrorisme is met name relevant art. 16, onderdeel f, Bjsg, dat bepaalt dat justitiële gegevens desgevraagd worden verstrekt aan de Minister van Justitie en Veiligheid, ten behoeve van het nemen van een beslissing omtrent de toepassing van de art. 2 t/m 4 van de Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding (Twbmt).
De Wpg en de Wjsg zullen wijzigen als gevolg van de implementatie van Richtlijn 2016/680.[8] Deze richtlijn heeft betrekking op zowel nationaal verzamelde en verwerkte persoonsgegevens als de uitwisseling van persoonsgegevens tussen de lidstaten. Inmiddels is een wetsvoorstel ter implementatie van de richtlijn bij de Tweede Kamer ingediend (Kamerstukken 34 889).

Wet op de inlichtingen- en veiligheidsdiensten (Wiv)

In artikel 4 lid 2 van het Verdrag betreffende de Europese Unie is bepaald dat de nationale veiligheid uitsluitend behoort tot de verantwoordelijkheid van de lidstaten. Ingevolge artikel 2 lid

[8] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad

sub a van de AVG is de AVG niet van toepassing op activiteiten die buiten de werkingssfeer van het Unierecht vallen. Dat betekent dat op de gegevensverwerking door de inlichtingen- en veiligheidsdiensten de Europese privacywetgeving niet van toepassing is. Het EVRM is uiteraard wel van toepassing op de inlichtingen- en veiligheidsdiensten.

Voor de gegevensverwerking door of ten behoeve van de inlichtingen- en veiligheidsdiensten geldt de Wet op de inlichtingen- en veiligheidsdiensten 2017. Dit geldt bijvoorbeeld voor gegevens die de AIVD verzamelt bij de uitvoering van haar taken, waaronder de taak "het verrichten van onderzoek met betrekking tot organisaties en personen die door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat" (art. 8 Wiv 2017). Ook de gegevensverwerking door de MIVD wordt door de Wiv 2017 gereguleerd.

Art. 17 t/m 70 Wiv 2017 regelt de verwerking van gegevens door de AIVD en de MIVD. Net als bij de Wbp en de AVG gelden de eisen van zorgvuldigheid, behoorlijkheid en doelgebondenheid (art. 18 Wiv 2017). Art. 19 Wiv 2017 noemt de categorieën personen waarop de gegevens betrekking mogen hebben, zoals die personen die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat. Op grond van art. 19, lid 3, Wiv 2017 mogen de diensten bepaalde categorieën bijzondere persoonsgegevens niet verzamelen (o.a. godsdienst en gezondheid), behoudens de uitzonderingen in lid 4 (`in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is").

Op grond van art. 39 Wiv 2017 zijn de diensten bevoegd zich bij de uitvoering van hun taak, dan wel ter ondersteuning van een goede taakuitvoering, voor het verzamelen van gegevens te wenden tot: bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken. Deze personen/instellingen zijn niet verplicht om gegevens te verstrekken. Art. 39, vijfde lid bepaalt ook dat de bij of krachtens de wet geldende voorschriften voor de verantwoordelijke bij een gegevensverstrekking als hier bedoeld niet van toepassing zijn.

Art. 40 t/m 58 bevat uitgewerkte bepalingen voor de toepassing van bijzondere bevoegdheden. Zie bijvoorbeeld art. 55 en 56 op grond waarvan gegevens betreffende gebruikers van telecommunicatie kunnen worden gevorderd.
Verstrekking van door of ten behoeve van een dienst verwerkte gegevens aan een binnen de dienst of ingevolge artikel 91 ten behoeve van de AIVD werkzame ambtenaar vindt slechts plaats, voor zover dat noodzakelijk is voor een goede uitvoering van de aan de desbetreffende ambtenaar opgedragen taak (art. 61 Wiv 2017).

Op grond van art. 62 Wiv 2017 zijn de AIVD en de MIVD in het kader van een goede taakuitvoering bevoegd om omtrent door of ten behoeve van de dienst verwerkte gegevens mededeling te doen aan:
a. Onze Ministers wie deze aangaan;
b. andere bestuursorganen wie deze aangaan;
c. andere personen of instanties wie deze aangaan;
d. daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, alsmede andere daarvoor in aanmerking komende internationale beveiligings-, verbindingsinlichtingen- en inlichtingenorganen

Hierbij kan de voorwaarde worden gesteld dat de gegevens niet verder aan anderen mogen worden verstrekt (art. art. 65 Wiv 2017). Daarnaast kan de dienst mededeling doen van de gegevens aan het OM als blijkt dat gegevens van belang kunnen zijn voor opsporing (art. 66 Wiv 2017). Daarnaast kan indien bij de verwerking van gegevens door of ten behoeve van een dienst daarvan is gebleken, op grond van een dringende en gewichtige reden schriftelijk mededeling worden gedaan van gegevens aan bij of krachtens AMvB aangewezen personen of instanties die betrokken zijn bij de uitvoering van een publieke taak, voor zover deze gegevens tevens van belang kunnen zijn voor de behartiging van de aan hen in dat kader opgedragen belangen (art. 67 Wiv 2017).

Persoonsgegevens worden door de betrokken minister of namens deze het hoofd van de dienst schriftelijk medegedeeld, indien de persoon of instantie waaraan de desbetreffende mededeling wordt gedaan naar aanleiding van die mededeling jegens de desbetreffende persoon bevoegd is maatregelen te treffen (art. 68 Wiv 2017). Art. 20 en 21 Wiv 2017 regelen de vernietiging.

De artikelen 88 t/m 95 wiv 2017 regelen de samenwerking van de diensten met andere instanties.[9] Op grond van art. 89 kunnen de diensten gegevens verstrekken aan samenwerkende diensten van andere landen ten behoeve van door deze instanties te behartigen belangen, voor zover:

a. deze belangen niet onverenigbaar zijn met de belangen die de diensten hebben te behartigen, en
b. een goede taakuitvoering door de diensten zich niet tegen verstrekking verzet.

Paspoortwet

Er is op grond van art. 4a Paspoortwet een Register reisdocumenten, waarvan de gegevens kunnen worden gedeeld op grond van het zesde lid van dit artikel (o.a. indien en waarom een reisdocument vervallen is) aan instellingen en personen, belast met een publiekrechtelijke taak, voor zover de gegevens noodzakelijk zijn voor de vervulling van hun taak.
Op grond van artikel 23 van de Paspoortwet kan de Minister die het aangaat (lees: de NCTV) signaleren dat het gegronde vermoeden bestaat dat de betrokken persoon buiten het Koninkrijk handelingen zal verrichten die een bedreiging vormen voor de veiligheid en andere gewichtige belangen van het Koninkrijk of een of meerdere landen van het Koninkrijk dan wel de veiligheid van met het Koninkrijk bevriende mogendheden. Op grond van de artikelen 23a en 23b kan een dergelijke signalering ook plaatsvinden als een betrokken persoon zich dreigt te onttrekken aan een tegen hem ingestelde strafvervolging of tenuitvoerlegging, dan wel indien aan iemand een uitreisverbod op grond van de Twbmt is opgelegd. Het signaleringsverzoek is op grond van art. 25 lid 1 Paspoortwet gericht aan de minister van BZK (lees: de RVIG).
De rechter heeft geoordeeld dat een gemeente kan besluiten om pasfoto's te verstrekken op verzoek aan opsporingsambtenaren aangezien voor die verstrekking een grondslag bestaat in de Paspoortwet (art. 3 lid 8 en 59 Paspoortwet jo art. 73 Paspoortuitvoeringsregeling).[10]

Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding (Twbmt)

Op grond van de Twbmt kunnen vrijheidsbeperkende maatregelen worden opgelegd ter bescherming van de nationale veiligheid aan personen die op grond van hun gedragingen in verband kunnen worden gebracht met terroristische activiteiten of ondersteuning daarvan. De minister van Justitie en Veiligheid (lees: de NCTV) kan, ten behoeve van het nemen van een beslissing over de toepassing van de artikelen 2 tot en met 4 van deze wet, justitiële gegevens vorderen (art. 16 sub f Besluit justitiële en strafvorderlijke gegevens). Daarnaast kunnen voor een dergelijke beslissing aan de minister politiegegevens worden verstrekt op basis van art. 4:4 Bpg. Ook kunnen aan bestuursorganen politiegegevens en justitiële gegevens worden verstrekt voor een beslissing over de toepassing van art. 6 Twbmt (art. 4:3 lid 1 sub n Bpg en art. 15a Bjsg), op grond waarvan zij een aanvraag voor een subsidie, vergunning, ontheffing of erkenning kunnen afwijzen of een reeds genomen beschikking ter zake van een subsidie, vergunning, ontheffing of erkenning kunnen intrekken indien ernstig gevaar bestaat dat de subsidie, vergunning, ontheffing of erkenning mede zal worden gebruikt ten behoeve van terroristische activiteiten of de ondersteuning daarvan.

Wetgeving inzake passenger name record (PNR) en Advance Passenger Information (API)

Bij de Tweede Kamer is het wetsvoorstel ter implementatie van de PNR-richtlijn 2016/681 ingediend.[11] Deze richtlijn beoogt de veiligheid waarborgen, het leven van personen te beschermen en een wettelijk kader te scheppen voor de bescherming van passagiersgegevens (PNR-gegevens, Passenger Name Record) bij de verwerking ervan door bevoegde autoriteiten.[12]

Het wetsvoorstel verplicht luchtvaartmaatschappijen PNR-gegevens te verstrekken aan de nieuw op te richten Passagiersinformatie-eenheid Nederland (Pi-NL).[13] Het wetsvoorstel is van toepassing

---

[9] Op grond van artikel 91, eerste lid, Wiv 2017 verrichten de daarin genoemde ambtenaren (zoals bijvoorbeeld de korpschef, de commandant van de KMar, de Hoofddirecteur IND) werkzaamheden voor de AIVD. De feitelijke uitvoering is in de praktijk echter opgedragen aan door de betrokken minister aangewezen ondergeschikten van deze ambtenaren. Deze verrichten onder andere werkzaamheden in het kader van de CT infobox.
[10] HR 13 november 2012, ECLI:NL:HR:2012:BX8079.
[11] Kamerstukken II 2017-2018, 34 861, nr. 2. Richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit. Deze richtlijn moet uiterlijk op 25 mei 2018 geïmplementeerd zijn.
[12] Zie punt 5 van de considerans van de PNR-richtlijn.
[13] Artikel 4 van het wetsvoorstel.

op vluchten naar of vanuit derde landen, alsmede vluchten binnen de EU.[14]
Onder PNR-gegevens worden PNR- en API-gegevens begrepen. PNR-gegevens zijn de gegevens die passagiers aan luchtvaartmaatschappijen verstrekken bij de reserveringen voor vluchten. Deze gegevens bevatten informatie over gereserveerde en eerder gevolgde reisroutes, medepassagiers, bagage en contact- en betalingsgegevens. API-gegevens (Advance Passenger Information) zijn gegevens over een identiteitsdocument, nationaliteit, naam, geboortedatum en vluchtgegevens van de individuele passagier.[15]

De PNR-gegevens mogen door de Pi-NL alleen worden verwerkt en geanalyseerd met het doel om terroristische misdrijven en ernstige misdrijven te voorkomen, op te sporen, te onderzoeken en te vervolgen. Onder 'terroristische misdrijven' vallen de misdrijven opgesomd in art. 83 en 83b van het Wetboek van Strafrecht. Onder 'ernstige misdrijven' worden begrepen categorieën strafbare feiten genoemd in Bijlage 2 bij het wetsvoorstel (gelijkluidend aan Bijlage II bij de PNR-richtlijn), zoals deelneming aan een criminele organisatie, mensenhandel, seksuele uitbuiting van kinderen en kinderpornografie, illegale handel in drugs en wapens, witwassen, corruptie, fraude en computercriminaliteit.
De Pi-NL beoordeelt passagiers voor hun geplande aankomst in of gepland vertrek uit Nederland teneinde te bepalen welke personen moeten worden onderworpen aan een nader onderzoek door de bevoegde instanties (zoals politie of OM) of Europol, omdat deze personen betrokken zouden kunnen zijn bij een terroristisch misdrijf of ernstige criminaliteit. De Pi-NL vergelijkt de door de luchtvaartmaatschappijen aangeleverde PNR-gegevens met gegevens in databanken van gesignaleerde personen of toetst de PNR-gegevens aan vooraf vastgestelde risico-criteria.[16] Bij een positieve overeenkomst na een geautomatiseerde vergelijking van de PNR-gegevens kan de Pi-NL het verwerkingsresultaat uitwisselen met PIU's (Passenger Information Unit) van andere lidstaten of Europol.[17] Voorts kan de Pi-NL onder voorwaarden PNR-gegevens aan derde landen doorgeven. In tegenstelling tot de uitwisseling van gegevens met PIU's betreft doorgifte aan derde landen echter geen verplichte taak van de Pi-NL.

Overig
Het Wetboek van Strafvordering kent een aantal bepalingen over het vorderen van gegevens ten behoeve van de opsporing van strafbare feiten (artikelen 126nc/ni en 126uc/ui Sv). Daarbij wordt onderscheid gemaakt tussen identificerende gegevens en andere gegevens. Er is een specifieke regeling voor het vorderen van telecommunicatiegegevens van aanbieders van telecommunicatiediensten (artikelen 126n/nb en 126u/ub Sv). Het wetboek voorziet in bijzondere bevoegdheden tot opsporing van terroristische misdrijven (Titel VB). De bevoegdheden van deze titel kunnen worden ingezet bij *aanwijzingen* van een terroristisch misdrijf - een ruimer begrip 'redelijk vermoeden' uit het normale proces van strafvordering. Verder kan een opsporingsambtenaar bij verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is, beslag leggen op o.a. gegevensbestanden (art. 96 en 96a Sv). Voor openbare colleges en ambtenaren kan op grond van artikel 162 lid 1 sub c Sv (misdrijven waardoor inbreuk op of onrechtmatig gebruik wordt gemaakt van een regeling waarvan de uitvoering of de zorg voor de naleving aan hen is opgedragen) en lid 2 Sv een verplichting bestaan tot het doen van aangifte en daarbij gegevens te verstrekken.

Art. 15 en 16 Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) verplichten bij AMvB aangewezen private partijen, zoals banken, advocaten en accountants, om bij de Financial Intelligence Unit – Nederland (FIU-NL) melding te doen van ongebruikelijke transacties – dit ter voorkoming van de financiering van terrorisme. FIU-NL heeft als taak o.a. het verstrekken van persoonsgegevens en andere gegevens in overeenstemming met de Wwft en het bij of krachtens de Wpg bepaalde (art. 13 en 14 Wwft).

Uitwisseling gegevens in samenwerkingsverbanden
Een grondslag[18] voor verdere verwerking van persoonsgegevens die niet verenigbaar is met het doel waarvoor de gegevens aanvankelijk zijn verzameld, is ook nodig voor een samenwerkingsverband van diverse overheidsorganisaties, zoals bijvoorbeeld in de lokale aanpak van terrorismebestrijding. Waar dit voor de casuïstiek noodzakelijk is, werken de betrokken landelijke en lokale partijen intensief samen in een casusoverleg. De deelnemende casuspartners wisselen daar waar nodig en mogelijk informatie uit en stellen aan de hand daarvan een integraal

[14] Artikel 3 van het wetsvoorstel.
[15] Zie Bijlage 1 bij het wetsvoorstel, gelijkluidend aan Bijlage I bij de PNR-richtlijn.
[16] Artikel 6 van het wetsvoorstel.
[17] Artikelen 10 en 12 van het wetsvoorstel.
[18] Zoals vereist op grond van de AVG, de Wpg en de Wjsg.

plan van aanpak op. Voor de totstandkoming en uitvoering van het integraal plan van aanpak is het noodzakelijk en onvermijdelijk dat partners relevante gegevens, waaronder ook persoonsgegevens, verwerken. Om een dergelijke lokale samenwerking te faciliteren is het modelconvenant persoonsgerichte aanpak voorkoming radicalisering en extremisme opgesteld, dat houvast kan bieden aan lokale partners en waarin bovenstaande juridische kaders zijn verwerkt. In het convenant zijn de relevante wettelijke taken van de betrokken partijen expliciet benoemd, zodat duidelijk is op grond waarvan zij dan ook bevoegd zijn gegevens te verwerken en, zo nodig aan andere partners in het casusoverleg te verstrekken.