Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2012–2013

32 669 EU-voorstel: Richtlijn inzake het gebruik van passagiersgegevens voor wethandhavingsdoeleinden COM(2011)321

I

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 6 februari 2013

Al enige tijd is de ontwerprichtlijn Europees PNR[1] in behandeling bij de commissie voor Immigratie en Asiel / JBZ-Raad[2]. Op de verwerking en doorgifte van passagiersgegevens is inmiddels diverse wet- en regelgeving van toepassing, terwijl meer regelgeving in voorbereiding is. Naast de genoemde ontwerprichtlijn Europees PNR zijn dat onder meer de PNR-overeenkomsten met Australië[3] en de Verenigde Staten, de Richtlijn bescherming persoonsgegevens uit 1995 en het Kaderbesluit over de bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële samenwerking in strafzaken.[4] Ook het voorstel voor een algemene verordening gegevensbescherming[5] en het voorstel voor een richtlijn gegevensbescherming opsporing en vervolging[6] zijn relevant. Daarnaast constateert de commissie dat de afgelopen jaren enkele Mededelingen van de Europese Commissie over PNR zijn verschenen.[7] De leden van de commissie hebben behoefte aan inzicht in de samenhang tussen deze regels, zowel de geldende als de toekomstige.
Naar aanleiding daarvan heeft de commissie de minister van Veiligheid en Justitie op 18 december 2012 een brief gestuurd.

---

[1] COM(2011)32. Zie dossier **E110005** op www.europapoort.nl; Richtlijn voor het gebruik van passagiersgegevens voor de preventie, detectie, het onderzoek en vervolging van terroristische daden en zware criminaliteit.

[2] Samenstelling:
Holdijk (SGP), Broekers-Knol (VVD), Slagter-Roukema (SP), Franken (CDA), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA), Duthler (VVD), Koffeman (PvdD), Kuiper (CU), Quik-Schuijt (SP), Strik (GL), De Vries (PvdA), Lokin-Sassen (CDA), Scholten (D66), Th. de Graaf (D66), De Boer (GL), De Lange (OSF), Ter Horst (PvdA) *(voorzitter)*, Beuving (PvdA), Schrijver (PvdA), M. de Graaff (PVV) *(vice-voorzitter),* Reynaers (PVV), Popken (PVV), Huijbregt-Schiedon (VVD), Schouwenaar (VVD), Swagerman (VVD)

[3] Zie de dossiers **E110026** en **E110026a** op www.europapoort.nl

[4] Kaderbesluit 2008/977/JBZ. Zie dossier **E090225** op www.europapoort.nl

[5] COM(2012)11. Zie dossier **E120003** op www.europapoort.nl

[6] COM(2012)10. Zie dossier **E120004** op www.europapoort.nl

[7] COM(2003)826 en COM(2010)492. Zie dossiers **E40099** en **E100051** op www.europapoort.nl

kst-32669-I
ISSN 0921 - 7371
's-Gravenhage 2013

De minister en de staatssecretaris van Veiligheid en Justitie hebben op 5 februari 2013 gereageerd.

De commissie brengt bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier van de vaste commissie voor Immigratie en Asiel / JBZ-Raad,
K. van Dooren

BRIEF AAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Den Haag, 18 december 2012

Al enige tijd is de ontwerprichtlijn Europees PNR[8] in behandeling bij de commissie voor Immigratie en Asiel / JBZ-Raad. Op de verwerking en doorgifte van passagiersgegevens is inmiddels diverse wet- en regelgeving van toepassing, terwijl meer regelgeving in voorbereiding is. Naast de genoemde ontwerprichtlijn Europees PNR zijn dat onder meer de PNR-overeenkomsten met Australië[9] en de Verenigde Staten, de Richtlijn bescherming persoonsgegevens uit 1995 en het Kaderbesluit over de bescherming van persoonsgegevens die worden verwerkt in het kader van politiële en justitiële samenwerking in strafzaken.[10] Ook het voorstel voor een algemene verordening gegevensbescherming[11] en het voorstel voor een richtlijn gegevensbescherming opsporing en vervolging[12] zijn relevant. Daarnaast constateert de commissie dat de afgelopen jaren enkele Mededelingen van de Europese Commissie over PNR zijn verschenen.[13]

De leden van de commissie hebben behoefte aan inzicht in de samenhang tussen deze regels, zowel de geldende als de toekomstige. De verhouding tussen deze regels – de overeenkomsten en verschillen en de hiërarchie – is hen nu niet voldoende duidelijk. Kan de regering de commissie dit gewenste inzicht op een overzichtelijke wijze doen toekomen, waarbij de regering ook de hiërarchie betrekt? Kan de regering meer specifiek aangeven wat de overeenkomsten en verschillen zijn tussen deze regels op het gebied van onder meer:

- doelomschrijving;
- de soort gegevens die verwerkt worden;
- de categorieën betrokkenen;
- de categorieën ontvangers;
- de gerechtvaardigde grondslag voor derdenverstrekking;
- bewaartermijnen;
- beveiligingseisen

en welke regels voorrang hebben in geval van strijdigheid? Ook wensen de leden van de commissie een zo volledig mogelijk overzicht van de informatiestromen waarop deze regels van toepassing zijn.

De commissie voor Immigratie & Asiel / JBZ-raad ziet uit naar uw reactie en ontvangt deze graag uiterlijk in **februari 2013**.

Voorzitter van de commissie voor Immigratie & Asiel / JBZ-raad,
P.L. Meurs

---

[8] COM(2011)32. Zie dossier **E110005** op www.europapoort.nl; Richtlijn voor het gebruik van passagiersgegevens voor de preventie, detectie, het onderzoek en vervolging van terroristische daden en zware criminaliteit.
[9] Zie de dossiers **E110026** en **E110026a** op www.europapoort.nl
[10] Kaderbesluit 2008/977/JBZ. Zie dossier **E090225** op www.europapoort.nl
[11] COM(2012)11. Zie dossier **E120003** op www.europapoort.nl
[12] COM(2012)10. Zie dossier **E120004** op www.europapoort.nl
[13] COM(2003)826 en COM(2010)492. Zie dossiers **E40099** en **E100051** op www.europapoort.nl

BRIEF VAN DE MINISTER EN DE STAATSSECRETARIS VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 5 februari 2013

In haar brief van 18 december 2012 verzoekt de Commissie voor Immigratie en Asiel/JBZ-Raad de regering om inzicht te geven in de samenhang tussen de (huidige en toekomstige) Europese regelgeving die de verwerking, doorgifte en bescherming van persoonsgegevens betreft. Uw commissie verzoekt dit gewenste inzicht op een overzichtelijke wijze aan haar te doen toekomen en daarbij ook de hiërarchie te betrekken. Verder verzoekt zij meer specifiek de overeenkomsten en verschillen tussen deze regels aan te geven ten aanzien van een aantal met name genoemde aspecten, zoals de doelomschrijving en de soort gegevens die verwerkt worden. Ook wil uw commissie weten welke regels voorrang hebben in geval van strijdigheid. Tot slot willen de leden van uw commissie een zo volledig mogelijk overzicht krijgen van de informatiestromen waarop deze regels van toepassing zijn.

In antwoord op uw vragen geven wij een overzicht van de verschillende bestaande en ontwerp EU-wetgeving en verdragen. Eerst schetsen we een schematisch overzicht van het geheel van de juridische kaders. Vervolgens gaan we voor elk juridisch instrument in op de door u genoemde aspecten. Vanwege de omvang van deze per juridisch instrument gerangschikte informatie hebben wij deze in een bijlage bij deze brief gevoegd. De overzichten in deze brief en de bijlage zijn tevens bedoeld om inzicht te bieden in de informatiestromen.
Met het oog op de door u gewenste overzichtelijke wijze van informatievoorziening zullen wij ons in de overzichten beperken tot een aantal hoofdlijnen en daarom uitzonderingen, nuances en details veelal buiten beschouwing laten. Wij laten in deze brief het streven naar overzichtelijkheid zwaarder wegen dan de volledigheid. Mede gezien de informatie die wij eerder aan uw Kamer hebben gestuurd verwachten wij dat deze benadering op uw instemming kan rekenen.

Overzicht

a. Europese verdragsbasis

Het domein of werkingssfeer van een Europese regeling hangt nauw samen met de rechtsgrondslag in het Verdrag betreffende de Werking van de Europese Unie (VWEU) of het Verdrag betreffende de Europese Unie. De bevoegdheid van de Europese Unie om wetgevend te kunnen optreden op een beleidsterrein is alleen aanwezig als er een basis voor is in het VWEU. De bestaande Europese wetgeving ten aanzien van gegevensbescherming bestrijkt verschillende domeinen en is gebaseerd op verschillende hoofdstukken van het VWEU (of van een eerder Europees verdrag).

b. Waarborgen in wetgeving van algemene aard

Er is een onderscheid tussen Europese juridische instrumenten inzake gegevensbescherming van algemene aard respectievelijk van specifieke aard. De richtlijn 95/46/EG van 24 oktober 1995 geeft een algemeen kader voor de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van

die gegevens[14]. Dit instrument geeft waarborgen in verband met de verwerking van persoonsgegevens in relatie tot de bevordering van het vrije verkeer van persoonsgegevens in het kader van de werking van de interne markt. De rechtsgrondslag van deze richtlijn ligt dan ook in het verdragshoofdstuk ten aanzien van de interne markt. Deze richtlijn is de basisregeling waarnaar in latere wetgeving vaak wordt verwezen. De principes die in de richtlijn zijn vastgelegd zijn ook terug te vinden in meer specifieke, sectorale regelgeving. De richtlijn betreft activiteiten die binnen de werkingssfeer van het gemeenschapsrecht (anno 1995) vallen, met uitzondering van het gemeenschappelijk buitenlands en veiligheidsbeleid en van de politiële en justitiële samenwerking in strafzaken. Laatstgenoemd terrein maakte in 1995 deel uit van de zogenaamde derde pijler die een afzonderlijke positie had in het toenmalige Verdrag betreffende de Europese Unie.
Voor de samenwerking in strafzaken is het Kaderbesluit 2008/977/JBZ van 27 november 2008 vastgesteld[15]. Dit kaderbesluit betreft een ander domein dan de richtlijn uit 1995 en geeft een algemeen kader voor het terrein van de samenwerking in strafzaken en staat als zodanig naast en op gelijke voet met de richtlijn van 1995.
De richtlijn is in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens en het kaderbesluit in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.
De richtlijn van 1995 en het kaderbesluit van 2008 vormen de twee voetstukken waarop andere, meer specifieke regelingen voortbouwen. Dit geldt ook voor de wetgeving ten aanzien van passagiersgegevens.

c. Wetgeving van specifieke aard

De richtlijn 2004/82/EG inzake Advance Passenger Information (API) betreft de verplichting voor vervoerders om passagiersgegevens door te geven aan de bevoegde nationale autoriteiten. De bestrijding van illegale immigratie en de verbetering van grenscontroles betreffend passagiers (in de burgerluchtvaart) zijn de doelstelling van de richtlijn[16]. De rechtsgrondslag ligt in het verdragshoofdstuk over asiel, immigratie en grenscontroles[17]. Voor dit domein is er geen afzonderlijke regelgeving die algemene waarborgen geeft voor de bescherming van persoonsgegevens. De API-richtlijn stelt expliciet dat de richtlijn van 1995 van toepassing is en geeft op een aantal punten, zoals voor de bewaartermijn, een nadere uitwerking aan de richtlijn van 1995.
Overigens wijzen wij er volledigheidshalve op dat er nog meer Europese regelgeving is die de grenscontroles van passagiers betreft, zoals het Communautair Douanewetboek[18]. Ook Bijlage VI van de Schengengrenscode geeft voorschriften, te weten voor controles aan de land- zee en luchtgrenzen.
De ontwerp-richtlijn PNR vindt haar rechtsgrondslag in de artikelen van het VWEU ten aanzien van de justitiële en politiële samenwerking in strafzaken. De ontwerp-richtlijn verwijst dan ook voor een aantal aspecten van gegevensbescherming naar bepalingen uit het kaderbesluit van 2008.

---

[14] PB L 281 van 23 nov. 1995, blz. 310
[15] PB EU 20 dec. 2008, blz. 60
[16] Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven. PB EU 6 aug. 2004, L 261/24.
[17] Verdrag tot oprichting van de Europese Gemeenschap
[18] De bevoegdheden van overheidsdiensten, waaronder de Douane en de Koninklijke Marechaussee, werden toegelicht in de antwoorden van de Minister van Veiligheid en Justitie op vragen van het Tweede Kamerlid Schouw, TK 2010–2011, Aanhangsel, nr. 3536).

d. Algemene beginselen/grondrechten

Hoewel er inhoudelijke verschillen zijn tussen de verscheidene regelingen, moeten ze elk voldoen aan de algemene beginselen van bescherming van persoonsgegevens zoals die zijn opgenomen in het Handvest van de grondrechten van de Europese Unie. Dit Handvest legt in artikel 7 het recht vast op respect voor zijn of haar privé en familieleven, woning en communicatie. Artikel 8 van het Handvest bepaalt:

1. Een ieder heeft recht op bescherming van zijn persoonsgegevens.
2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Een ieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.
3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd.

Artikel 52, eerste lid, betreft de beperkingen of de uitoefening van het in het Handvest erkende rechten en vrijheden. Deze moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. «Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen».

Verder is artikel 8 van het Europees Verdrag voor de Rechten van de Mens (en de daarop gebaseerde jurisprudentie) van belang. Dit EVRM-artikel legt vast dat ieder het recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Het tweede lid bepaalt: «Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van 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 voor de bescherming van de rechten en vrijheden van anderen.»

Deze normen vormen de algemene basis en begrenzing voor de uitwerking in Europese wetgeving.

Toekomstige wetgeving

De ontwerp-richtlijn voor een Europees PNR-systeem is nog niet afgerond. De Commissie deed een voorstel voor deze richtlijn op 2 februari 2011. In het voorjaar van 2012 bereikte de JBZ-Raad een algemene oriëntatie over de richtlijn. De volgende stap in de wetgevingsprocedure is dat het Europees Parlement zijn amendementen zal indienen.

De Europese Commissie heeft op 25 januari 2012 voorstellen gedaan voor een algemene Verordening gegevensbescherming en voor een Richtlijn gegevensbescherming opsporing en vervolging. De onderhandelingen hierover zijn gaande. De staatssecretaris van Veiligheid en Justitie informeerde u hierover, laatstelijk in zijn brief van 11 december 2012. De BNC-fiches van 2 maart 2012 (Kamerstukken EK, 2011–2012, 22 112, FH en FI) geven een overzicht van de inhoud en implicaties van de voorstellen.

De genoemde ontwerp-verordening zal de richtlijn uit 1995 vervangen en de voorgestelde richtlijn komt in de plaats van het kaderbesluit uit 2008.

Dit betekent dat de Europese juridische kaders, die een waarborgkarakter hebben inzake bescherming van persoonsgegevens, worden herzien. Dat heeft tot gevolg dat de instrumentele, meer specifieke wetgeving op het gebied van passagiersgegevens waar nodig aangepast zal moeten worden aan de nieuwe kaders. Het kabinet heeft in het BNC-fiche gesteld dat de regels op het gebied van gegevensbescherming in andere bestaande Europese rechtsinstrumenten zo snel mogelijk dienen te worden aangepast.
In de bijlage (onder C) gaan we, in antwoord op uw vragen, kort in op de nieuwe elementen van deze voorstellen ten opzichte van de bestaande regelingen, ten aanzien van de door u genoemde aspecten.

Samenvattend schema
Europese regelgeving gegevensbescherming en passagiersgegevens

Domein: persoonsgegevens die in een bestand worden opgenomen, *met uitzondering van* buitenlands veiligheidsbeleid en politiële & justitiële samenwerking in strafzaken.	**Domein:** persoonsgegevens die in een bestand worden opgenomen in verband met *politiële en justitiële samenwerking* in strafzaken.
Europese wetgeving & rechtsgrondslag	**Europese wetgeving & rechtsgrondslag**
a. Algemene waarborgen: EG-Richtlijn bescherming persoonsgegevens, 1995. **Rechtsgrondslag**: EG-verdrag, art. 95 inzake de interne markt.	***a. Algemene waarborgen:*** Kaderbesluit gegevensbescherming politiële en justitiële samenwerking in strafzaken, 2008. **Rechtsgrondslag**: Verdrag Europese Unie, artt. 30, 31, 34 lid 2 onder b inzake justitiële en politiële samenwerking in strafzaken.
b. Specifiek & instrumenteel: Richtlijn Advance Passenger Information, 2004 (API). **Rechtsgrondslag**: Verdrag tot oprichting v.d. Europese Gemeenschap, artt 62, punt 2, onder a) en 63, punt 3, onder b) inzake grenscontrole, immigratie en asiel.	***b. Specifiek en instrumenteel:*** Ontwerp-richtlijn Passenger Name Records, (Commissievoorstel 2012). **Rechtsgrondslag**: WVEU artikelen 82, eerste lid, onder (d) en 87, tweede lid onder (a) inzake justitiële resp. politiële samenwerking in strafzaken.
Implementatiewetgeving in Nederland	**Implementatiewetgeving in Nederland**
a. Algemene waarborgen: Wet bescherming Persoonsgegevens (Wbp) en Wet gemeentelijke basisadministratie persoonsgegevens (GBA)	***a. Algemene waarborgen:*** Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens.
b. Specifiek inz. API-gegevens: Vreemdelingenwet 2000, art. 4., artt. 2a en 2b Vb 2000, Wbp (voor vervoerders) en Wpg (voor de KMar)	***b. Specifiek inz. PNR-gegevens:*** nog te bepalen na aanneming van de EU-richtlijn PNR.

Basis/grondrechtelijk kader: Algemene beginselen bescherming persoonsgegevens (EVRM, EU-handvest grondrechten)

Verdragen tussen de EU en derde-landen

Op het niveau van de Europese Unie is een aantal verdragen gesloten met betrekking tot de uitwisseling van PNR-gegevens. De Europese wetgeving is uiteraard niet van toepassing op de verdragspartners die geen EU-lid zijn. De Europese Commissie en de lidstaten streven in de onderhandelingen na om zo veel mogelijk van de Europese standaarden in de verdragen op te nemen.
De verdragen bevatten de voorwaarden waaronder derde-landen PNR-gegevens mogen verzamelen en verwerken. De overgrote meerderheid van de EU-lidstaten heeft geen systeem voor het gebruik van PNR-data voor de bestrijding van terrorisme en ernstige criminaliteit en zal dan ook geen PNR-data verzamelen. De verdragen met derde-landen zijn daarom niet wederkerig. Wel is afgesproken dat de autoriteiten van derde-landen analytische informatie die is verkregen uit PNR zullen leveren aan de autoriteiten van de lidstaten en Europol en Eurojust, in concrete zaken die onderzocht worden.
Door de EU is aan de Verenigde Staten voorgesteld een algemeen kader overeen te komen voor de uitwisseling van gegevens voor politie- en justitiedoeleinden. De relatie tussen een dergelijke kaderovereenkomst en de bestaande verdragen is nog onderwerp van overleg.

Type instrument	Strekking	Verdragskader	Doel	Soort gegevens
Verdragen	**Algemeen**	Overeenkomst EU-VS gegevensbescherming (alg. kader; in onderhandeling)	*Bescherming persoonsgegevens bij gegevensuitwisseling tussen diensten van EU, de lidstaten en de VS t.b.v. politie- en justitie-doeleinden*	*In onderhandeling.*
	Specifiek	Overeenkomst EU-VS inzake doorgifte PNR-data	*Voorkoming en bestrijding terrorisme en transnationale zware criminaliteit*	*Reserveringsgegevens van passagiers in de burgerluchtvaart*
		Overeenkomst EU-Australië inzake doorgifte PNR-data	*Voorkoming en bestrijding terrorisme en transnationale zware criminaliteit*	*Reserveringsgegevens van passagiers in de burgerluchtvaart*
		Overeenkomst EU-Canada doorgifte PNR-data (in onderhandeling)	*Voorkoming en bestrijding terrorisme en transnationale zware criminaliteit (in onderhandeling)*	*Reserveringsgegevens van passagiers in de burgerluchtvaart (in onderhandeling)*

Overeenkomsten en verschillen tussen de regelingen

Naast het principiële onderscheid tussen regelingen van algemene aard die een waarborgkarakter hebben en specifieke regelingen die vooral een instrumenteel karakter hebben, zijn er diverse verschillen en overeenkomsten op onderdelen. De verschillen vloeien voort uit het onderscheid in doelstellingen van de regelingen. Wij illustreren dit aan de hand van de Richtlijn inzake Advance Passenger Information (API) respectievelijk de ontwerp-richtlijn Passenger Name Records (PNR). De API-richtlijn heeft tot doel de bestrijding van illegale immigratie en de verbetering van de grenscontrole, terwijl de ontwerp-PNR-richtlijn de bestrijding van terrorisme en zware criminaliteit betreft. Dit verschil heeft tot gevolg dat de bewaartermijn in de API-richtlijn relatief kort is en in principe op 24 uur is gesteld. Het betreft immers een controleproces aan de grens. Als de grenspassage heeft plaatsgehad en de controle is afgerond dan zijn de gegevens in beginsel niet meer nodig. Dit is anders in de PNR-richtlijn. De preventie, opsporing, het onderzoek en de vervolging van terroristische misdrijven en zware criminaliteit strekken zich uit over een langere periode en de bewaartermijn van deze gegevens is dan ook relatief lang, te weten in beginsel vijf jaar.

De door u genoemde aspecten soort gegevens, categorieën betrokkenen en ontvangers en bewaartermijnen hangen nauw samen met het doel van een regeling of verdrag. Andere aspecten zijn minder nauw gerelateerd aan de specifieke doelstellingen en vertonen dan ook veel overeenkomsten, zoals de grondslag voor en waarborgen bij derdenverstrekking en de beveiligingseisen.
Op al deze terreinen is overigens sprake van een ontwikkeling die in de loop van de tijd heeft plaatsgehad. In oudere regelingen zoals de richtlijn gegevensbescherming uit 1995 zijn aspecten zoals beveiligingseisen nog minder ver uitgewerkt dan in een meer recent voorstel zoals de ontwerp-algemene verordening gegevensbescherming of de ontwerp-PNR-richtlijn.

In onderstaand schema geven wij een globale schets van de aspecten die u aan de orde hebt gesteld met betrekking tot de nu geldende wetgeving, verdragen en toekomstige wetgeving. Bij elke regeling is een letter en een cijfer opgenomen, die verwijzen naar de uitwerking in de bijlage. De ontwerp richtlijn voor een Europees PNR-systeem is niet alleen in het schema inzake toekomstige wetgeving opgenomen, maar ook in het schema van de geldende wetgeving vanwege de samenhang met het Kaderbesluit van 2008.

Schema A. Overzicht EU-wetgeving

Wetgeving EU	Doel	Soort gegevens	Betrokkenen	Ontvangers	Derdenverstrekking	Bewaartermijnen	Beveiligingseisen
Algemeen Richtlijn gegevensbescherming 1995 **A.1.**	*Evenwicht tussen bescherming persoonlijke levenssfeer en vrij verkeer van persoonsgegevens*	*Persoonsgegevens die in een bestand zijn of worden opgenomen*	*Identificeerbaar, natuurlijk persoon*	*Persoon of instantie aan wie/ waaraan gegevens worden meegedeeld*	*Beoordeling passend beschermingsniveau of onder voorwaarden*	*Niet langer dan voor doeleinden noodzakelijk*	*Passende technische en organisatorische maatregelen. Waarborgen, toezicht en vastlegging.*
Specifiek Richtlijn Advanced Passenger Information (API) **A.2.**	*Bestrijding illegale immigratie en verbetering grenscontroles*	*Identiteitsgegevens (paspoort) van passagiers in de burgerluchtvaart, vluchtgegevens en reisgegevens*	*Luchtvaartpassagiers aan buitengrenzen*	*Autoriteiten belast met controle buitengrenzen (In NL: KMar)*	*Geen bepalingen, dus via richtlijn 1995 (In NL: Wbp en Wpg)*[1]	*Vernietigen na 24 uur, tenzij nodig voor de wettelijke taken grensautoriteiten*	*Geen bepalingen, dus via richtlijn 1995 (In NL: Wbp en Wpg*[2]*)*
Algemeen; politie en justitie Kaderbesluit politie en justitie 2008 **A.3.**	*Bescherming persoonlijke levenssfeer i.v.m. politiële en justitiële samenwerking in strafzaken bij hoog niveau van openbare veiligheid*	*Persoonsgegevens die in een bestand zijn of worden opgenomen*	*Identificeerbaar, natuurlijk persoon*	*Orgaan aan wie de gegevens worden meegedeeld*	*Onder voorwaarden (noodzaak, status ontvangende autoriteit, toestemming lidstaat, toereikend beschermingsniveau)*	*Autoriteit wijst termijn aan bij verstrekking of via nationaal recht ontvangende lidstaat*	*Technische en organisatorische maatregelen. Waarborgen toezicht en vastlegging. Lijst van verplichte maatregelen op lidstaatniveau.*
Specifiek Ontwerprichtlijn EU Passenger Name Records (PNR) **A.4.**	*Voorkoming en bestrijding terrorisme en zware criminaliteit*	*Reserveringsgegevens van passagiers in de burgerluchtvaart*	*Luchtvaartpassagiers buitengrenzen (binnengrens optioneel)*	*Passagiers Informatie Eenheid; in lidstaat aan te wijzen.*	*Alleen als aan KB 2008 is voldaan plus noodzaak, toestemming lidstaat enz.*	*Vijf jaar. Na twee jaar onder voorwaarden toegang.*	*Cfr. KB 2008, plus registratie van elke verwerking voor interne en externe controle.*

[1] Op de verstrekking van de gegevens door de KMar aan derden is in NL de Wet politiegegevens van toepassing sinds de inwerkingtreding van die wet op 1-1-2008. De grenscontrole taak van de KMar is in de Politiewet aangemerkt als politietaak en de gegevens die tbv de politietaak worden verwerkt zijn daarmee politiegegevens geworden, waarop de Wet politiegegevens van toepassing is.
[2] Hiervoor geldt eveneens dat voor zover het betreft de verwerking door de KMar, daarop de Wpg van toepassing is. (Zie opmerking hierboven.)

Schema B. Overzicht van verdragen tussen de EU en derde landen

Verdrag	Doel	Soort gegevens	Betrokkenen	Ontvangers	Derdenverstrekking	Bewaartermijnen	Beveiligingseisen
Overeenkomst EU-VS gegevensbescherming (in onderhandeling)	*Bescherming persoonsgegevens bij gegevensuitwisseling tussen diensten van EU, de lidstaten en de VS t.b.v. politie- en justitiedoeleinden*	*In onderhandeling*	*In onderhandeling*	*In onderhandeling*	*In onderhandeling*	*In onderhandeling*	*In onderhandeling*
Overeenkomst EU-VS inzake doorgifte PNR-data **B.2.**	*Voorkoming en bestrijding terrorisme en transnationale zware criminaliteit*	*Reserveringsgegevens van passagiers in de burgerluchtvaart*	*Passagiers van vluchten tussen EU en VS incl. luchtvaartmaatschappijen die gevestigd zijn of data opslaan in de EU*	*Department of Homeland Security, VS.*	*Onder voorwaarden die stroken met het verdrag & na verificatie. Afspraken over gegevensbescherming. Alleen on-derzochte zaken*	*Vijf jaar in actieve databank. Na zes maanden depersonalisatie en maskering. Nadien maximaal tien jaar in dormant database.*	*Maatregelen en technieken ter bescherming. Waarschuwings- en herstelplicht bij privacy-incident. Registratie van toegang tot PNR.*
Overeenkomst EU-Australië inzake doorgifte PNR-data **B.1.**	*Voorkoming en bestrijding terrorisme en transnationale zware criminaliteit*	*Reserveringsgegevens van passagiers in de burgerluchtvaart*	*Passagiers en bemanningsleden*	*Australian Customs and Border Protection Service*	*Onder voorwaarden. Waarborgen die stroken met het verdrag. In concrete gevallen & binnen verdragsdoel.*	*Vijf en een half jaar. Na drie jaar maskering.*	*Fysieke en organisatorische eisen. Controle en rapportage van toegang. Sancties bij inbreuken. Rapportage bij inbreuken aan Europese Commissie.*
Overeenkomst EU-Canada doorgifte PNR-data (in onderhandeling)	*Voorkoming en bestrijding terrorisme en transnationale zware criminaliteit*	*Reserveringsgegevens van passagiers in de burgerluchtvaart*	*In onderhandeling*	*In onderhandeling*	*In onderhandeling*	*In onderhandeling*	*In onderhandeling*

Schema C. Toekomstige EU-wetgeving (aanhangig)

Wetgeving EU	Doel	Soort gegevens	Betrokkenen	Ontvangers	Derdenverstrekking	Bewaartermijnen	Beveiligingseisen
Algemeen Voorstel (2012) algemene verordening gegevensbescherming **C.1.**	*Bescherming van natuurlijke personen i.v.m. verwerking van persoonsgegevens en regulering vrij verkeer van persoonsgegevens*	*Persoonsgegevens: ledere informatie betreffende een betrokkene*	*een geïdentificeerde natuurlijke persoon of een (in)direct te identificeren natuurlijke persoon*	*de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander orgaan aan wie/ waaraan de gegevens worden meegedeeld*	*Commissie beoordeelt of beschermingsniveau passend is op basis van criteria. Als besluit van Commissie ontbreekt moet derde land juridisch bindende garanties bieden op basis van vastgelegde voorwaarden.*	*Niet langer dan voor de doeleinden waarvoor zij worden verwerkt, noodzakelijk is. Betrokkene heeft recht om te worden vergeten en om data te laten wissen. Criteria zijn vastgelegd.*	*Plicht voor verantwoordelijke en verwerker om reeks maatregelen te treffen. Meldplicht bij inbreuken.*

Wetgeving EU	Doel	Soort gegevens	Betrokkenen	Ontvangers	Derdenverstrekking	Bewaartermijnen	Beveiligingseisen
Algemeen (strafzaken) Voorstel (2012) richtlijn gegevensbescherming opsporing en vervolging **C.2.**	*Bescherming van natuurlijke personen i.v.m. verwerking van persoonsgegevens door autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen*	*Persoonsgegevens: ledere informatie betreffende een betrokkene*	*een geïdentificeerde natuurlijke persoon of een (in)direct te identificeren na-tuurlijke persoon*	*een natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of enig ander lichaam aan wie/ waaraan de gegevens worden verstrekt*	*Commissie beoordeelt of beschermingsniveau passend is op basis van criteria. Als besluit van Commissie ontbreekt moet derde land jur. bindende garanties bieden op basis van. vastgelegde voorwaarden*	*Niet langer dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt. Betrokkene heeft recht om gegevens te laten wissen. Criteria zijn vastgelegd.*	*Plicht voor verantwoordelijke en verwerker om reeks maatregelen te treffen. Meldplicht bij inbreuken.*
Specifiek Ontwerprichtlijn EU Passenger Name Records (PNR) **C.3.**	*Voorkoming en bestrijding terrorisme en zware criminaliteit*	*Reserveringsgegevens van passagiers in de burgerluchtvaart*	*Luchtvaartpassagiers buitengrenzen (binnengrens optioneel)*	*Passagiers Informatie Eenheid; in lidstaat aan te wijzen.*	*Alleen als aan KB 2008 is voldaan plus noodzaak, toestemming lidstaat enz.*	*Vijf jaar. Na twee jaar onder voorwaarden toegang.*	*Cfr. KB 2008, plus registratie van elke verwerking voor interne en externe controle.*

Hiërarchie en voorrang

U verzoekt verduidelijking te geven ten aanzien van de hiërarchie van de instrumenten en een antwoord op de vraag welke regels voorrang hebben in geval van strijdigheid.
In het voorgaande schetsten wij een algemeen beeld van de relatie tussen de verschillende regelingen en verdragen. Wij onderscheidden algemene regelingen, die een waarborgkarakter hebben, van specifieke regelingen die primair instrumenteel van aard zijn en een bepaalde sector betreffen. Verder wezen we op de verschillen op onderdelen die samenhangen met de verscheidene doelen van de regelingen en op de overeenkomsten tussen onderdelen die niet direct afhankelijk zijn van de doelbinding. Ook brachten we de verschillende rechtsgrondslagen in Europese verdragen naar voren.
Deze analyse impliceert dat de verhouding tussen de regelingen per onderwerp bekeken moet worden. De vraag naar de voorrang van de ene regeling ten opzichte van de andere laat zich niet in algemene zin beantwoorden. Bij de beoordeling van de relatie tussen de regelingen met het oog op de hiërarchie of voorrang is steeds de doelbinding het uitgangspunt.
Een concrete regeling kan bepalingen bevatten die een relatie leggen met andere relevante Europese wetgeving. We noemen ter illustratie de richtlijn inzake API-gegevens. Overweging 12 van de API-richtlijn zegt dat de richtlijn uit 1995 van toepassing is op de verwerking van persoonsgegevens door de autoriteiten van de lidstaten. Artikel 6 inzake de verwerking van API-gegevens verwijst ten aanzien van uitzonderlingen op de bewaartermijn expliciet naar de bepalingen van de (algemene) richtlijn uit 1995. Ook voor het gebruik van persoonsgegevens voor wetshandhavingsdoeleinden resp. de informatieverstrekking aan passagiers verwijst de API-richtlijn (in de artt. 3, 10 en 11) naar de richtlijn uit 1995. Hiernaast verwijst de API-richtlijn op een aantal punten naar de Europese Schengenregelgeving.
Het is uiteraard niet uit te sluiten dat in een concreet geval toch vragen rijzen over de relatie tussen verschillende regelingen. Afhankelijk van de

vraagstelling zal de nationale of Europese rechter zich hierover uiteindelijk kunnen uitspreken.

Mededelingen van de Europese Commissie

U wijst op twee mededelingen van de Europese Commissie, te weten COM(2003)826 en COM(2010)492.

a. *De mededeling van 2003* is te kwalificeren als een beleidsdocument en betreft een allesomvattende EU-aanpak voor de doorgifte van passagiersgegevens (PNR). De Commissie somde in dit document een aantal kwesties op die in 2003 op de agenda stonden in de verhouding tussen de VS en de EU. Het Europees Parlement had verzocht maatregelen te nemen met betrekking tot de doorgifte van PNR-gegevens naar de VS om te garanderen dat met de Europese belangen inzake gegevensbescherming rekening werd gehouden. De Commissie heeft in de mededeling de elementen voor een meervoudige EU-aanpak op een rij gezet. Dit betrof het realiseren van een wettelijk kader voor de PNR-doorgiften naar de VS, het verstrekken van informatie aan de passagiers, de vervanging van de «pullmethode» voor doorgifte door de «pushmethode», het ontwikkelen van een EU-standpunt over gebruik van passagiersgegevens om de veiligheid van het luchtverkeer en van de grenzen te verhogen en het opzetten van een kader voor de doorgifte van PNR-gegevens binnen de Internationale Burgerluchtvaartorganisatie (ICAO).
b. *De mededeling van 2010* is een vervolg op die van 2003. De Commissie beschrijft hierin de uitvoering van het beleid dat in 2003 werd uiteengezet en internationale ontwikkelingen op PNR-gebied. Ze stelt vast dat internationale ontwikkelingen erop wijzen dat «het gebruik van PNR-gegevens toeneemt en steeds meer wordt beschouwd als een regulier en noodzakelijk aspect van de rechtshandhaving. Het gebruik van PNR-gegevens impliceert evenwel de verwerking van persoonsgegevens, wat belangrijke vragen oproept in verband met de fundamentele rechten op bescherming van het privéleven en van persoonsgegevens.»[19] De mededeling heeft als belangrijkste doel het vaststellen van een reeks algemene criteria die kunnen dienen als basis voor toekomstige onderhandelingen over PNR-overeenkomsten met derde landen. De Commissie doet aanbevelingen voor onderhandelingen over PNR-overeenkomsten met derde landen waarbij minimaal de in de mededeling vastgelegde algemene criteria in acht worden genomen. De fundamentele rechten die zijn opgenomen in het EVRM en in het Handvest van de grondrechten van de EU zijn hierbij het vertrekpunt. De Commissie wil op deze wijze de «vraag» vanuit derde-landen meer gestructureerd tegemoet treden met als gevolg dat de diverse overeenkomsten geringere verschillen zullen vertonen. Op langere termijn vooruitblikkend op de ontwikkeling van PNR-initiatieven overal in de wereld, vindt de Commissie dat de EU de mogelijkheid moet onderzoeken om de bilaterale overeenkomsten te vervangen door een multilaterale overeenkomst tussen alle landen die PNR-gegevens gebruiken.

Slot

Wij trachten door middel van deze brief inzicht te geven in de Europese regelgeving ten aanzien van de verwerking, doorgifte en bescherming van persoonsgegevens en gaan daarbij in het bijzonder in op de uitwisseling van gegevens van vliegtuigpassagiers. Deze regelgeving is soms

[19] Blz. 3 van COM(2010)492, d.d. 21 september 2010, Mededeling van de Commissie over de algemene aanpak van de doorgifte van passagiersgegevens (Passenger Name Record – PNR) aan derde landen

algemeen, soms sectoraal opgezet, heeft een inhoudelijke ontwikkeling in de tijd doorgemaakt en is gebaseerd op verschillende opeenvolgende Europese verdragen. De voorstellen van de Europese Commissie van 2011 en 2012 laten zien dat de ontwikkeling niet is afgerond. Deze veelvormigheid van regelingen neemt niet weg dat de inhoud van de waarborgen voor de gegevensbescherming steeds genormeerd is en blijft door algemene beginselen. In de concrete uitwerking zullen de belangen van bescherming van de persoonlijke levenssfeer en van de veiligheid steeds evenwichtig moeten worden afgewogen.

Een afschrift van deze brief sturen wij aan de Voorzitter van de Tweede Kamer van de Staten-Generaal.

De minister van Veiligheid en Justitie,
I.W. Opstelten

De staatssecretaris van Veiligheid en Justitie,
F. Teeven

BIJLAGE

De Europese juridische instrumenten ten aanzien van gegevensbescherming; een overzicht.

A. Wetgeving

1. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

De richtlijn van 1995 is op Europees niveau de referentietekst op het gebied van de bescherming van persoonsgegevens. De richtlijn heeft een algemeen of horizontaal karakter en is niet toegesneden op een bepaalde beleidssector of op een bepaald type gegevens. De richtlijn is in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens (Stb. 2000, 302) en in de Wet houdende regels ter zake van de gemeentelijke basisadministratie van persoonsgegevens (GBA).

De richtlijn omvat onder meer algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens en verplicht tot het aanwijzen van een onafhankelijke autoriteit in elke lidstaat die belast wordt met het toezicht op de toepassing van de nationale wetgeving die ter uitvoering van de richtlijn door de lidstaten wordt vastgesteld.

a. doelomschrijving

Het kader van de richtlijn heeft tot doel een evenwicht tot stand te brengen tussen een hoog niveau van bescherming van de persoonlijke levenssfeer en het vrij verkeer van persoonsgegevens in de Europese Unie.

b. soort gegevens

De richtlijn is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
De richtlijn is niet van toepassing op activiteiten die niet binnen de werkingssfeer van het (in 1995 geldende) Gemeenschapsrecht vallen, zoals de openbare veiligheid, defensie en de veiligheid van de staat, noch op strafrechtelijk gebied.
Onder «persoonsgegevens» wordt verstaan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (in de richtlijn verder «betrokkene» genoemd).

c. categorieën betrokkenen

Als identificeerbaar wordt beschouwd een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of van een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.

d. categorieën ontvangers

De richtlijn verstaat onder «ontvanger» de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam aan wie of waaraan de gegevens worden meegedeeld.

e. grondslag voor derdenverstrekking

Hoofdstuk IV van de richtlijn regelt de doorgifte van persoonsgegevens naar derde landen.
Persoonsgegevens die verwerkt worden mogen slechts naar een derde land worden doorgegeven als dat land een passend beschermingsniveau waarborgt. Het passend karakter van het door een derde land geboden beschermingsniveau wordt beoordeeld met inachtneming van alle omstandigheden die op de doorgifte van gegevens of op een categorie gegevensdoorgiften van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doeleinde en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken derde land gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in die landen worden nageleefd. De Europese Commissie beoordeelt of een derde land waarborgen voor een passend beschermingsniveau biedt. Bij een negatief oordeel van de Commissie nemen de lidstaten de nodige maatregelen om doorgifte van gegevens van dezelfde aard naar het betrokken land te voorkomen. Lidstaten kunnen bepalen dat doorgiften naar een derde land mogen plaatsvinden naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt, mits aan voorwaarden wordt voldaan. Bijvoorbeeld als de betrokkene zijn toestemming heeft gegeven.

f. bewaartermijnen

Hoofdstuk II van de richtlijn omvat algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens. In artikel 6 onder e) is opgenomen dat de persoonsgegevens «niet langer mogen worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, noodzakelijk is».
De bewaartermijn is derhalve verbonden met het beginsel van doelbinding: persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen en vervolgens niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden.

g. beveiligingseisen

h. De voor de verwerking verantwoordelijke moet passende technische en organisatorische maatregelen ten uitvoer leggen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking. Deze maatregelen moeten een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich brengen. De voor de verwerking verantwoordelijke moet bij verwerking ten dienste van hemzelf een verwerker kiezen die voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen en moet toezien op de naleving van die maatregelen. De relatie tussen de verwerker en de voor de verwerker verantwoordelijke moet contractueel worden vastgelegd.

2. Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven. (De «API-richtlijn»)

Dit betreft Advance Passenger Information (API). Deze richtlijn is in Nederland geïmplementeerd via artikel 4 van de Vreemdelingenwet 2000.

a. doelomschrijving

Het doel van de richtlijn is de grenscontroles te verbeteren en de illegale immigratie te bestrijden door erin te voorzien dat de vervoerders de passagiersgegevens vooraf aan de bevoegde nationale autoriteiten verstrekken.
Overeenkomstig hun nationale recht en de in Richtlijn 95/46/EG opgenomen bepalingen inzake gegevensbescherming kunnen de lidstaten de persoonsgegevens ook voor (bepaalde) wetshandhavingsdoeleinden gebruiken.

b. soort gegevens

Het betreft informatie die vervoerders verplicht zijn om aan de autoriteiten te verstrekken over de passagiers die zij zullen vervoeren naar een aangewezen grensdoorlaatpost via welke deze personen het grondgebied van een lidstaat binnenkomen. De richtlijn somt deze informatie op: het nummer en de aard van het gebruikte reisdocument, de nationaliteit, de volledige naam, de geboortedatum, de grensdoorlaatpost van binnenkomst op het grondgebied van de lidstaten, het vervoermiddel, het tijdstip van vertrek en aankomst van het vervoermiddel, het totale aantal met dat vervoermiddel vervoerde passagiers en het eerste instappunt.
In het Vreemdelingenbesluit 2000 zijn deze gegevens aangevuld met gegevens die behoren tot de in de internationale praktijk gehanteerde standaard API-set (nml. geslacht, staat van afgifte van het reisdocument, vervaldatum van het reisdocument, overige reisroutegegevens en Passenger Name Record-bestandslocatie).

c. categorieën betrokkenen

Het betreft vliegtuigpassagiers die de buitengrenzen overschrijden.

d. categorieën ontvangers

De ontvangers zijn de autoriteiten die belast zijn met de controle van personen aan de buitengrenzen. In Nederland is dit de Koninklijke Marechaussee.

e. grondslag voor derdenverstrekking

De richtlijn geeft geen grondslag voor verstrekking van gegevens aan derde-landen.

f. bewaartermijnen

Nadat de passagiers het grondgebied zijn binnengekomen vernietigen de autoriteiten de gegevens binnen 24 uur na de toezending ervan, tenzij deze later nodig zijn voor de uitoefening van de wettelijke taken van de autoriteiten die belast zijn met de controle van personen aan de buitengrenzen.

g. beveiligingseisen

De API-richtlijn stelt geen specifieke eisen aan de beveiliging.

3. Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken

Het Kaderbesluit van 2008 betreft het terrein van de samenwerking in strafzaken en is niet toegespitst op een specifiek type gegevens. Het toepassingsgebied van het kaderbesluit is beperkt tot de verwerking van persoonsgegevens die worden verstrekt of beschikbaar gesteld *tussen* lidstaten. Het kaderbesluit is in Nederland geïmplementeerd in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.

a. doelomschrijving

Doel van dit kaderbesluit is een hoge mate van bescherming te waarborgen van de fundamentele rechten en vrijheden, in het bijzonder het recht op een persoonlijke levenssfeer, van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de politiële en justitiële samenwerking in strafzaken terwijl een hoog niveau van openbare veiligheid wordt gegarandeerd.

b. soort gegevens / c. categorieën betrokkenen

Het kaderbesluit betreft de geautomatiseerde verwerking van persoonsgegevens, alsmede de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen. Onder persoonsgegevens wordt verstaan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon; deze wordt verder in het Kaderbesluit «betrokkene» genoemd.

d. categorieën ontvangers

De ontvanger is het orgaan aan wie de gegevens worden meegedeeld.

e. grondslag voor derdenverstrekking

Persoonsgegevens die door de bevoegde autoriteit van een andere lidstaat zijn verstrekt of beschikbaar gesteld, mogen uitsluitend worden doorgegeven aan derde landen of internationale organen indien:

a) dit noodzakelijk is met het oog op de preventie, het onderzoek, de opsporing of de vervolging van strafbare feiten en de tenuitvoerlegging van straffen;
b) de ontvangende autoriteit in het derde land of het ontvangende internationale orgaan belast is met de preventie, het onderzoek, de opsporing of de vervolging;
c) de lidstaat waarvan de gegevens afkomstig zijn heeft toegestemd in de doorgifte met inachtneming van het nationale recht, en
d) het betrokken derde land of internationale orgaan een toereikend beschermingsniveau voor de voorgenomen gegevensverwerking waarborgt.

In een aantal omschreven situaties kan van het onder d) genoemde beginsel worden afgeweken.

Of het onder d), bedoelde beschermingsniveau toereikend is, wordt beoordeeld met inachtneming van alle omstandigheden die op de doorgifte van gegevens of op een groep van gegevensverstrekkingen van

invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doel en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land of het internationale orgaan van eindbestemming van de gegevens, de algemene en sectorale rechtsregels die in het derde land of het internationale orgaan gelden, alsmede de beroepscodes en de veiligheidsmaatregelen die in het land of voor het orgaan van toepassing zijn.

f. bewaartermijnen

De verstrekkende autoriteit kan bij het verstrekken of beschikbaar stellen van de gegevens de termijnen voor het bewaren van de gegevens aangeven, na afloop waarvan ook de ontvanger de gegevens moet wissen of afschermen of moet nagaan of zij nog steeds nodig zijn. Deze verplichting geldt niet indien de gegevens bij het verstrijken van de termijnen nodig zijn voor een lopend onderzoek, de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.
Indien de verstrekkende autoriteit heeft nagelaten om de termijnen voor het bewaren van gegevens aan te geven dan is het nationaal recht van de ontvangende lidstaat van toepassing.

g. beveiligingseisen

De lidstaten moeten voorschrijven dat de bevoegde autoriteiten passende technische en organisatorische maatregelen treffen om persoonsgegevens te beveiligen tegen onbedoelde of onrechtmatige vernietiging, tegen wijziging, ongeoorloofde mededeling of toegang en tegen alle andere vormen van onrechtmatige verwerking. Deze maatregelen moeten een passend beveiligingsniveau garanderen. De lidstaten moeten maatregelen treffen ten aanzien van de geautomatiseerde verwerking van gegevens met het oog op: controle op de toegang tot de apparatuur, controle op de gegevensdragers, opslagcontrole, gebruikerscontrole, controle op de toegang tot de gegevens, transmissiecontrole, invoercontrole, vervoerscontrole, herstel, betrouwbaarheid en integriteit van het systeem.
Verwerkers kunnen alleen worden aangewezen als ze garanderen de vereiste maatregelen te zullen treffen en de instructies over de vertrouwelijkheid te zullen opvolgen. Er moet worden toegezien op de nakoming. Een verwerker mag persoonsgegevens alleen op grond van een wettelijke regeling of een schriftelijke overeenkomst verwerken.

B. Verdragen

1. Overeenkomst tussen de Europese Unie en Australië inzake de verwerking en doorgifte van persoonsgegevens van passagiers (PNR) door luchtvaartmaatschappijen aan de Australische dienst Douane en grensbescherming

Deze overeenkomst is op 29 september 2011 ondertekend en is op 1 juni 2012 in werking getreden.

a. doelomschrijving

De «Australian Customs and Border Protection Service» (ACBPS) mag PNR-data alleen verwerken voor het doel van voorkomen, opsporen, onderzoeken en vervolgen van terroristische delicten of ernstige transnationale criminaliteit.

b. soort gegevens

PNR data betreffen de informatie die verwerkt wordt in de EU door luchtvaartmaatschappijen inzake de vereiste reisgegevens van elke passagier zoals opgenomen in bijlage 1 bij het verdrag. Deze bevat de informatie bevat die nodig is voor het verwerken en beheren van reserveringen door de reserverende en deelnemende luchtvaartmaatschappijen.

c. categorieën betrokkenen

Het betreft de passagiers of bemanningsleden inclusief de piloot.

d. categorieën ontvangers

De Australian Customs and Border Protection Service ontvangt en verwerkt de PNR-data. De ACBPS verzekert de beschikbaarheid van relevante analytische informatie die verkregen is uit PNR-data ten behoeve van politie of justitiële autoriteiten van de betrokken lidstaat van de EU of Europol of Eurojust binnen de grenzen van hun mandaten.
Een politie of justitiële autoriteit van een lidstaat of Europol of Eurojust kunnen toegang vragen tot PNR-data of relevante analytische informatie die verkregen is uit PNR-data en die noodzakelijk is in een specifiek geval om terroristische delicten of ernstige transnationale criminaliteit te voorkomen, op te sporten, te onderzoeken of te vervolgen.

e. grondslag voor derdenverstrekking

De ACBPS mag PNR-data alleen met andere overheidsdiensten van Australië delen als deze diensten op een lijst staan (bijlage 2 bij het verdrag) en als aan een aantal voorwaarden is voldaan.
De ACBPS mag PNR-data alleen doorgeven aan bepaalde autoriteiten van derde landen als voldaan wordt aan de volgende waarborgen. Deze betreffen: de instemming van de autoriteit van het derde land met toepassing van de waarborgen die in de overeenkomst zijn opgenomen, de autoriteit van het derde land moet taken hebben die direct betrekking hebben op voorkomen, opsporen onderzoeken en vervolgen van terroristische delicten of ernstige transnationale criminaliteit, data mogen alleen worden overgedragen voor de doelen die in het verdrag zijn genoemd en alleen in concrete gevallen (case-by-case). Voorafgaand aan de overdracht moet de ACBPS de relevantie van de over te dragen data zorgvuldig beoordelen. Alleen de specifieke data-elementen waarvan duidelijk is aangetoond dat ze noodzakelijk zijn in specifieke omstandigheden, mogen overgedragen worden. In elk geval wordt de overdracht van data zo veel mogelijk tot het minimum beperkt. Als de ACBPS weet dat de data een inwoner of ingezetene van een lidstaat betreffen zal de ACBPS de bevoegde autoriteiten van de betreffende lidstaat informeren. De ontvangende autoriteit van een derde land moet ermee instemmen PNR-data alleen te bewaren totdat het betreffende onderzoek of de vervolging is afgerond of dat de betreffende straf is afgedwongen of niet langer nodig zijn voor de doelen van het verdrag en in ieder geval niet langer dan noodzakelijk. De ontvangende autoriteit mag de data niet doorsturen. Waar passend wordt de passagier geïnformeerd over de overdracht van zijn of haar PNR-data.

f. Bewaartermijnen

PNR-data mogen niet langer dan vijf en een half jaar bewaard worden, vanaf de datum van eerste ontvangst door de ACBPS. Gedurende deze periode mogen de data alleen bewaard worden in het PNR-systeem voor

het doel van voorkoming, opsporing, onderzoek en vervolging van terroristische misdrijven of ernstige transnationale criminaliteit. Dit op de volgende manier:

a. de eerste drie jaar zijn alle PNR-data toegankelijk voor een beperkt aantal ambtenaren van de ACBPS die specifiek zijn geautoriseerd door de chief executive officer van de ACBPS om passagiers te identificeren die mogelijk van belang zijn;
b. in de periode van drie tot vijf en een half jaar moeten alle data-elementen die kunnen dienen tot identificatie van de passagier gemaskeerd worden. De gedepersonaliseerde PNR-data zullen alleen toegankelijk zijn voor een beperkt aantal ambtenaren om analyses uit te voeren. Volledige toegang tot PNR-data kan alleen worden toegestaan door een lid van de senior executive service van de ACBPS als het noodzakelijk is om onderzoek te doen voor het doel van het voorkomen, opsporen, onderzoeken en vervolgen van terroristische delicten en ernstige transnationale criminaliteit.

PNR-data die vereist zijn voor een specifiek onderzoek, vervolging of ten uitvoerlegging van straffen voor terroristische delicten of ernstige transnationale criminaliteit mogen voor dat doel verwerkt worden en dan bewaard worden totdat het betreffende onderzoek of de vervolging is afgerond of totdat de straf ten uitvoer is gelegd.
Na verloop van de bewaartermijnen moeten de PNR-data permanent verwijderd worden.

g. Beveiligingseisen

Het verdrag bevat bepalingen met het oog op het voorkomen van onbedoelde of onrechtmatige vernietiging of verloren gaan, wijziging, ongeautoriseerde toegang of onrechtmatige verwerking van de data. De apparatuur moet in een veilige fysieke omgeving geplaatst zijn en voorzien zijn van systemen van hoog niveau en controlemaatregelen inzake binnendringen. De PNR-data moeten afzonderlijk van andere data bewaard worden. Bij de vergelijking van data mogen de PNR-data het systeem niet verlaten richting andere databanken. Toegang tot het PNR-systeem is begrensd tot een beperkt aantal ambtenaren binnen de ACBPS die specifiek geautoriseerd zijn. Deze ambtenaren mogen het PNR-systeem alleen inzien op veilige werklocaties die niet toegankelijk zijn voor niet-geautoriseerde personen. De toegang wordt gecontroleerd via veiligheids-toegangssystemen. De toegang wordt gecontroleerd en gerapporteerd. De overdracht van data door de ACBPS aan andere autoriteiten moet op een beveiligde manier geschieden. Het PNR-systeem moet voorzien in storingsdetectie en rapportage. De PNR-data moeten beveiligd worden tegen manipulatie, wijziging, aanvulling of aantasting door slecht functioneren van het systeem. Er mogen geen kopieën van de PNR-databank gemaakt worden, anders dan vanwege een back-up bij calamiteiten.
Elke inbreuk op de data-veiligheid is onderworpen aan doelmatige en afschrikwekkende sancties.
De ACBPS zal elke inbreuk op de data-veiligheid rapporteren aan het bureau van de Australische Informatie Commissaris en de Europese Commissie van deze rapportage op de hoogte stellen.

2. Overeenkomst tussen de Verenigde Staten van Amerika en de Europese Unie inzake het gebruik en de doorgifte van persoonsgegevens van passagiers aan het Amerikaanse Ministerie van Binnenlandse Veiligheid[20]. (Betreft PNR)

Deze overeenkomst is op 14 december 2011 in Brussel ondertekend en op 1 juli 2012 in werking getreden.

a. doelomschrijving

Artikel 1 van het verdrag noemt als doelstelling het verzekeren van de veiligheid en de bescherming van het leven en de veiligheid van het publiek.
De VS verzamelt, gebruikt en verwerkt PNR voor de doelen van voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en andere delicten met een strafbedreiging van een gevangenisstraf van drie jaar of meer, die transnationaal van aard zijn.
PNR mogen gebruikt en verwerkt worden op case-by-case basis als dit noodzakelijk is met het oog op een ernstige bedreiging en voor de bescherming van vitale belangen van een persoon of op last van een rechter.

b. soort gegevens

Het betreft PNR zoals vastgelegd in de richtlijnen van de Internationale Organisatie voor de Burgerluchtvaart (ICAO). Dit wil zeggen de gegevensregistratie die luchtvaartmaatschappijen of hun agenten maken voor elke reis die gereserveerd wordt door passagiers en bewaard wordt in hun reserveringssystemen, vertrek controlesystemen of gelijksoortige systemen met deze functionaliteit. De datasoorten zijn opgesomd in een bijlage bij het verdrag.

c. categorieën betrokkenen

Het verdrag betreft luchtvaartmaatschappijen die vluchten uitvoeren tussen de EU en de VS en maatschappijen die gevestigd zijn of data opslaan in de EU en vluchten uitvoeren naar of vanuit de VS.
De rechten voor passagiers zijn van toepassing op elke persoon ongeacht zijn nationaliteit, land van herkomst of plaats van vestiging. Dit betreft de toegang of rectificatie of van PNR of het instellen van een rechtsmiddel.

d. categorieën ontvangers

De data worden gestuurd naar het Department of Homeland Security (DHS) van de regering van de VS. DHS mag alleen na zorgvuldige beoordeling gegevens delen met andere overheidsdiensten van de VS, mits voldaan wordt aan een aantal voorwaarden. De doorgifte moet binnen de doelbinding passen en de ontvangende diensten moeten dezelfde of vergelijkwaardige waarborgen bieden als genoemd in het verdrag. Verder mogen PNR-data alleen worden gedeeld ten behoeve van concrete zaken die onderzocht worden en overeenkomstig schriftelijke afspraken en het recht van de VS betreffend de uitwisseling van informatie tussen binnenlandse overheidsdiensten. Deze voorwaarden gelden ook bij doorgifte van analytische informatie die gebaseerd is op PNR-data.
DHS zal relevante analytische informatie die is verkregen uit PNR leveren aan politie of justitiële autoriteiten van de lidstaten en Europol en Eurojust, in zaken die in onderzoek zijn met het oog op het voorkomen,

[20] PB EU 4 juli 2012, L 174. (Nederlandse tekst)

opsporen, onderzoeken of vervolgen van transnationale ernstige criminaliteit of gedrag betreffend terroristische delicten in de EU.
Een politiële of justitiële autoriteit van een lidstaat van de EU of Europol of Eurojust kan toegang tot PNR verzoeken of tot analytische informatie, die nodig is in een specifieke zaak.
DHS zal PNR alleen delen na zorgvuldige beoordeling en mits voldaan is aan een aantal voorwaarden.

e. grondslag voor derdenverstrekking

De VS mag PNR alleen doorgeven aan bevoegde overheidsdiensten van derde landen onder voorwaarden die stroken met het verdrag en alleen na verificatie dat het gebruik dat de ontvanger beoogt past binnen deze voorwaarden.
Afgezien van noodsituaties zal een doorgifte van data alleen geschieden overeenkomstig expliciete afspraken waarin gegevensbeschermingsvoorzieningen zijn opgenomen die vergelijkbaar zijn met die van het verdrag. De doorgifte is alleen mogelijk ten behoeve van zaken die onderzocht worden. Als DHS weet dat PNR van een ingezetene of inwoner van een EU lidstaat overgedragen worden zal DHS de autoriteiten van de betreffende lidstaten informeren. Deze voorwaarden zijn ook van toepassing bij doorgifte van analytische informatie die gebaseerd is op PNR-data.

f. bewaartermijnen

DHS bewaart PNR tot vijf jaar in een actieve databank. Na de eerste zes maanden van deze periode worden de PNR gedepersonaliseerd en gemaskeerd. Toegang tot de actieve databank zal in beginsel begrensd zijn tot een beperkt aantal specifiek geautoriseerde ambtenaren. Om depersonalisatie te realiseren wordt persoonlijk identificeerbare informatie gemaskeerd. Na de actieve periode wordt de PNR overgedragen naar een slapende databank (dormant database) voor een periode van maximaal tien jaar. Deze slapende databank is onderworpen aan aanvullende controlemaatregelen, waaronder een beperkter aantal gemachtigde ambtenaren en een vereist hoger toezichtsniveau voor de benodigde toestemming. Deze PNR mogen alleen tot een persoon terugherleid worden (repersonalisatie) in verband met rechtshandhavingsoperaties in verband met een identificeerbare zaak, dreiging of risico. De repersonalisatie mag niet langer duren dan vijf jaar.
Na de «slapende periode» moeten de data volledig geanonimiseerd worden.
Data die een concrete zaak of onderzoek betreffen mogen bewaard worden in een actieve PNR databank totdat de zaak gearchiveerd is.
Eén jaar na inwerkingtreding van het verdrag zal de uitvoering hiervan worden beoordeeld. Na vier jaar wordt het verdrag geëvalueerd. In het kader van de evaluatie wordt de noodzaak van de tienjarige slapende periode bezien.

g. beveiligingseisen

DHS moet maatregelen nemen om persoonsgegevens en persoonsinformatie die in PNR zijn opgenomen te beschermen tegen onbedoeld, onrechtmatig of ongeautoriseerde vernietiging, verloren gaan, opening, wijziging, toegang verwerking of gebruik. DHS moet technieken gebruiken om de gegevensbescherming, veiligheid, vertrouwelijkheid en integriteit te verzekeren. In het geval van een privacy-incident moet DHS zorgen dat de betrokken personen gewaarschuwd worden, het risico op schade beperken en herstellende maatregelen treffen. DHS zal de relevante Europese autoriteiten informeren over gevallen van incidenten betreffend PNR van EU-ingezetenen of -inwoners. De VS bevestigt dat bestuurlijke,

civiele en strafrechtelijke handhavingsmaatregelen beschikbaar zijn onder het recht van de VS voor privacy-incidenten. DHS kan disciplinaire maatregelen treffen tegen verantwoordelijke personen. Alle toegang tot PNR wordt geregistreerd. DHS voorziet in een automatisch systeem om gevoelige data uit PNR te filteren en maskeren. Toegang tot gevoelige data wordt in uitzonderlijke omstandigheden toegestaan, als het leven van een persoon in gevaar komt of wordt geschaad. De toegang is dan onderworpen aan toestemming van een senior leidinggevende van DHS op basis van een concreet geval waarbij gebruik gemaakt wordt van beperkende procedures.
Gevoelige gegevens worden permanent verwijderd na maximaal dertig dagen na ontvangst. Niettemin mogen gevoelige data voor een specifiek onderzoek, vervolging of een handhavingsactiviteit bewaard worden voor de periode die is gespecificeerd in het recht van de VS.

C. Toekomstige wetgeving

1. Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene verordening gegevensbescherming)

Het betreft een voorstel van de Europese Commissie van 25 januari 2012. Een overzicht van kernpunten van dit voorstel is opgenomen in het BNC-fiche (kamerstukken EK, 2011–2012, 22 112, FI). De volgende, door uw Kamer genoemde, aspecten worden gewijzigd.

– rechtsgrondslag

Dit voorstel is gebaseerd op artikel 16 VWEU, de nieuwe rechtsgrondslag voor de vaststelling van voorschriften inzake gegevensbescherming, die is ingevoerd bij het Verslag van Lissabon.

– grondslag voor derdenverstrekking

Artikel 40 stelt dat de verplichtingen in dat hoofdstuk van toepassing zijn op elke doorgifte van persoonsgegevens naar derde landen of internationale organisaties, met inbegrip van verdere doorgifte.
Artikel 41 bevat de criteria, voorwaarden en procedures voor de vaststelling van een besluit waarbij een beschermingsniveau door de Commissie passend wordt verklaard en is gebaseerd op artikel 25 van Richtlijn 95/46/EG. Voorts wordt bepaald aan de hand van welke criteria de Commissie beoordeelt of het beschermingsniveau al dan niet passend is, tot welke criteria uitdrukkelijk de rechtsstaat, de toegang tot rechtsmiddelen en onafhankelijk toezicht behoren.
Het artikel voorziet ook uitdrukkelijk in de mogelijkheid dat de Commissie het beschermingsniveau beoordeelt dat door een gebied of een verwerkingssector in een derde land geboden wordt.

Indien de Commissie geen besluit heeft vastgesteld waarbij een beschermingsniveau passend wordt verklaard, moeten krachtens artikel 42 voor doorgifte naar derde landen passende garanties worden geboden, zoals modelbepalingen inzake gegevensbescherming, bindende bedrijfsvoorschriften en contractbepalingen. De mogelijkheid om gebruik te maken van modelbepalingen inzake gegevensbescherming van de Commissie is gebaseerd op artikel 26, lid 4, van Richtlijn 95/46/EG. Nieuw is dat dergelijke modelbepalingen inzake gegevensbescherming kunnen worden vastgesteld door een toezichthoudende autoriteit en algemeen geldig kunnen worden verklaard door de Commissie. Bindende bedrijfsvoor-

schriften worden nu specifiek genoemd in deze verordening. De mogelijkheid van contractbepalingen biedt de voor de verwerking verantwoordelijke of verwerker zekere flexibiliteit, maar vereist wel voorafgaande toestemming van de toezichthoudende autoriteiten.
In artikel 43 worden de voorwaarden voor doorgifte verder gespecificeerd in de vorm van bindende bedrijfsregels op basis van de huidige praktijken en vereisten van de toezichthoudende autoriteiten.

In artikel 44 worden de uitzonderingsbepalingen voor gegevensdoorgifte uiteengezet en verklaard, gebaseerd op de bestaande bepalingen van artikel 26 van Richtlijn 95/46/EG. Dit heeft in het bijzonder betrekking op doorgiften van gegevens die vereist en noodzakelijk om gewichtige redenen van algemeen belang, zoals in geval van internationale doorgifte van gegevens tussen mededingingsautoriteiten, belasting- of douanediensten, of diensten met bevoegdheid op het gebied van de sociale zekerheid of visserijbeheer. Voorts kan een gegevensdoorgifte onder beperkte voorwaarden gerechtvaardigd zijn in verband met de gerechtvaardigde belangen van de voor de verwerking verantwoordelijke of de verwerker, maar slechts nadat de omstandigheden van deze doorgifte zijn geëvalueerd en gedocumenteerd.
Artikel 45 voorziet uitdrukkelijk in mechanismen voor internationale samenwerking inzake de bescherming van persoonsgegevens tussen de Commissie en de toezichthoudende autoriteiten van derde landen, met name die waarvan het beschermingsniveau als passend is beoordeeld, rekening houdende met de aanbeveling van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) van 12 juni 2007 inzake grensoverschrijdende samenwerking bij de handhaving van wetgeving ter bescherming van de privacy.

– bewaartermijnen

Artikel 5 sub e): de persoonsgegevens moeten niet langer in een vorm die het mogelijk maakt de betrokkenen te identificeren, worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt, noodzakelijk is. Persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de gegevens uitsluitend voor historische, statistische of wetenschappelijke doeleinden worden verwerkt overeenkomstig de bepalingen en voorwaarden van artikel 83 en mits periodiek wordt beoordeeld of de gegevens nog steeds opgeslagen moeten blijven.
Artikel 17 van de voorgestelde verordening gaat uit van het recht van betrokkene om te worden vergeten en om gegevens te laten wissen in de volgende omstandigheden:
a) de gegevens zijn niet langer nodig in verband met de doeleinden waarvoor zij werden verzameld of anderszins verwerkt;
b) de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, onder a), is gebaseerd, in of de toegestane termijn voor opslag is verstreken terwijl een andere grond voor de verwerking van de gegevens ontbreekt;
c) de betrokkene maakt bezwaar tegen de verwerking van de persoonsgegevens overeenkomstig artikel 19;
d) de verwerking van de gegevens voldoet op andere gronden niet aan deze verordening.

De voor de verwerking verantwoordelijke gaat onverwijld tot het wissen over, zij het niet voor zover het nodig is de persoonsgegevens te bewaren:
a) voor de uitoefening van het recht op vrijheid van meningsuiting overeenkomstig artikel 80;
b) om redenen van algemeen belang op het gebied van de volksgezondheid overeenkomstig artikel 81;

c) voor historische, statistische of wetenschappelijke doeleinden overeenkomstig artikel 83;
d) ter voldoening aan een wettelijke verplichting tot bewaring van de persoonsgegevens op grond van EU-wetgeving of de wetgeving van de lidstaat waaraan de voor de verwerking verantwoordelijke onderworpen is; de nationale wetgeving moet beantwoorden aan een doelstelling van algemeen belang, de wezenlijke inhoud van het recht op de bescherming van persoonsgegevens eerbiedigen en evenredig zijn aan het nagestreefde rechtmatige doel.
e) in de in lid 4 bedoelde gevallen.

Lid 4. De voor de verwerking verantwoordelijke beperkt de verwerking van persoonsgegevens in plaats van deze te wissen wanneer:
a) de juistheid ervan door de betrokkene wordt betwist, gedurende een periode die de voor de verwerking verantwoordelijke in staat stelt de juistheid van de gegevens te controleren;
b) de voor de verwerking verantwoordelijke de persoonsgegevens niet langer voor de uitvoering van zijn taken nodig heeft, maar die gegevens nog moeten worden bewaard ten behoeve van bewijsvoering;
c) de verwerking ervan onrechtmatig is en de betrokkene zich tegen het wissen ervan verzet en in de plaats daarvan om beperking van het gebruik ervan verzoekt;
d) de betrokkene verzoekt om doorgifte van de persoonsgegevens naar een ander geautomatiseerd verwerkingssysteem overeenkomstig artikel 18, lid 2.

– beveiligingseisen.

Krachtens artikel 30 moeten de voor de verwerking verantwoordelijke en de verwerker passende maatregelen treffen voor de beveiliging van de verwerking. Deze bepaling is gebaseerd op artikel 17, lid 1, van Richtlijn 95/46/EG, maar breidt de verplichting uit tot de verwerkers, ongeacht hun contract met de voor de verwerking verantwoordelijke. Bij de artikelen 31 en 32 wordt de verplichting ingevoerd om inbreuken in verband met persoonsgegevens te melden. Deze bepaling bouwt voort op artikel 4, lid 3, van Richtlijn 2002/58/EG (e-privacyrichtlijn).

2. Voorstel voor een Richtlijn van het Europees Parlement en de Raad 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 (Richtlijn gegevensbescherming opsporing en vervolging)

De Europese Commissie deed dit voorstel op 25 januari 2012. Een overzicht van kernpunten van dit voorstel is opgenomen in het BNC-fiche (kamerstukken EK, 2011–2012, 22 112, FH).

– rechtsgrondslag

Het voorstel is gebaseerd op artikel 16, lid 2, VWEU, een nieuwe specifieke bepaling die in het Verdrag van Lissabon is opgenomen met het oog op de vaststelling van voorschriften betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en door de lidstaten

bij de uitvoering van activiteiten die binnen de werkingssfeer van het Unierecht vallen, alsook voorschriften betreffende het vrije verkeer van dergelijke gegevens.

– doelomschrijving

Het voorstel beoogt een consequent hoog niveau van gegevensbescherming op dit gebied te verzekeren, teneinde het wederzijds vertrouwen van de politiële en justitiële autoriteiten van de verschillende lidstaten te versterken en het vrije verkeer van gegevens en de samenwerking tussen die autoriteiten te bevorderen.
Anders dan het Kaderbesluit van 2008 is de ontwerp-richtlijn van toepassing op de verwerking van persoonsgegevens, *ongeacht* of de gegevens aan andere landen worden verstrekt. Op deze wijze vindt harmonisatie plaats van de regimes voor gegevensbescherming binnen de lidstaten voor de verwerking van persoonsgegevens ten behoeve van de rechtshandhaving.

– categorieën betrokkenen

De Commissie stelt voor dat de richtlijn ook van toepassing is op de gegevensverwerking in strafzaken door de zittende magistratuur. In Nederland valt deze verwerking onder de reikwijdte van de Wbp.

– grondslag voor derdenverstrekking

De ontwerp-richtlijn bevat geen specifieke regels voor de doelbinding bij de verstrekking van persoonsgegevens aan andere lidstaten. Dit wijkt af van het Kaderbesluit uit 2008.
Het systeem voor de verstrekking van persoonsgegevens aan derde landen wordt verder uitgewerkt dan nu het geval is. De nieuwe regels bieden meer houvast voor het maken van afwegingen in concrete gevallen. De beoordeling of een derde land een passend beschermingsniveau biedt, geschiedt in de toekomst door de Commissie. De elementen waarop de Commissie moet toetsen worden expliciet opgesomd en zijn uitvoeriger dan in het huidige Kaderbesluit 2008.
Als de Commissie het beschermingsniveau niet toereikend vindt, dan moeten de lidstaten erop toezien dat aan het betreffende derde land of de internationale organisatie, geen persoonsgegevens worden doorgegeven. Als de Commissie voor een bepaald land geen beoordeling heeft uitgevoerd dan kunnen de lidstaten besluiten of gegevens kunnen worden doorgegeven. In die situatie is het vereist dat in een juridisch bindend instrument passende garanties voor de bescherming van de persoonsgegevens zijn geboden of dat de voor de verwerking verantwoordelijke of de verwerker alle omstandigheden in verband met de doorgifte van persoonsgegevens heeft beoordeeld en geconcludeerd heeft dat er passende waarborgen bestaan voor de bescherming van persoonsgegevens.
De richtlijn geeft een limitatieve lijst van uitzonderingen op de genoemde hoofdregels.

– bewaartermijnen

Artikel 4, sub e) zegt dat de lidstaten bepalen dat persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren, maar niet langer dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor de persoonsgegevens worden verwerkt.
Artikel 16 regelt het recht van betrokkene om gegevens te laten wissen.

– beveiligingseisen

Het voorstel van de Commissie verplicht de verantwoordelijke en de verwerker om een reeks van technische en organisatorische maatregelen te treffen en omvat een meldplicht bij de toezichthouder, in geval van datalekken.

3. Voorstel voor een richtlijn inzake het gebruik van Passenger Name Record data voor de preventie, opsporing, onderzoek en vervolging van terroristische misdrijven en ernstige criminaliteit (Ontwerp-richtlijn «Europees PNR»)[21]

Het betreft een voorstel van de Europese Commissie van 2 februari 2011.

a. doelomschrijving

De overeenkomstig de richtlijn verzamelde PNR-gegevens mogen uitsluitend worden verwerkt om terroristische misdrijven en zware criminaliteit te voorkomen, op te sporen, te onderzoeken en te vervolgen.

b. soort gegevens

PNR gegevens; een bestand met de reisgegevens van iedere passagier, dat informatie bevat die de boekende en deelnemende luchtvaartmaatschappijen nodig hebben om reserveringen te kunnen verwerken en controleren bij elke reis die door of namens iemand wordt geboekt.

c. categorieën betrokkenen

Passagiers, d.w.z. een ieder, met uitzondering van de bemanningsleden, die met toestemming van de luchtvaartmaatschappij in een luchtvaartuig wordt vervoerd of zal worden vervoerd en die staat vermeld op de passagierslijst. Dus ook de transferpassagiers en de transitpassagiers.

d. categorieën ontvangers

Elke lidstaat wijst een instantie aan die bevoegd is terroristische misdrijven en zware criminaliteit te voorkomen, op te sporen, te onderzoeken of te vervolgen, de taak toe op te treden als zijn passagiersinformatie-eenheid (PIE). In de Engelse basistekst wordt dit een PIU genoemd: passenger information unit. Deze PIE of PIU is ermee belast de PNR-gegevens van de luchtvaartmaatschappijen te verzamelen, op te slaan en te verwerken en de gegevens of het resultaat van de gegevensverwerking mee te delen aan de bevoegde instanties. Elke lidstaat stelt een lijst op van de instanties die bevoegd zijn om van de PIE's gegevens op te vragen of te ontvangen teneinde deze informatie nader te onderzoeken of de nodige maatregelen te treffen voor het voorkomen, opsporen, onderzoeken en vervolgen van de terroristische misdrijven en zware criminaliteit.
De PIE is ook belast met de uitwisseling van de gegevens of het resultaat van de gegevensverwerking met de PIE's van andere lidstaten.

e. grondslag voor derdenverstrekking

Artikel 8 van de ontwerp-richtlijn betreft de doorgifte van gegevens aan derde landen. Doorgifte door een lidstaat aan een derde land is uitsluitend toegestaan *per geval* en mits:

---

[21] Dit betreft toekomstige regelgeving. Vanwege de samenhang met bestaande regelingen is deze ontwerp-richtlijn onder paragraaf A (Wetgeving) opgenomen.

a) aan de voorwaarden van artikel 13 Kaderbesluit 2008/977/JBZ van de Raad is voldaan;
b) de doorgifte noodzakelijk is voor de in artikel 1, lid 2, van de richtlijn vastgestelde doeleinden,
c) het derde land ermee instemt de gegevens alleen aan een ander derde land door te geven als dit noodzakelijk is voor de in artikel 1, lid 2, van deze richtlijn vastgestelde doeleinden, en behoudens uitdrukkelijke toestemming van de lidstaat die de gegevens aan het derde land heeft verstrekt; en
d) aan voorwaarden zoals die in artikel 7, lid 2, is voldaan. (Artikel 7 betreft onder meer de eis dat de opvraging van de gegevens behoorlijk moet worden gemotiveerd. Ook bevat artikel 7 een verwijzing naar artikel 9 lid 3 dat de bewaartermijn betreft. Als de termijn van twee jaar is verstreken dan is mededeling van de volledige PNR-gegevens uitsluitend toegestaan als redelijkerwijze wordt aangenomen dat dit noodzakelijk is in een concreet geval binnen de doelbinding van de richtlijn behoudens toestemming door een rechterlijke of andere nationale instantie die volgens het nationale recht bevoegd is om na te gaan of aan de voorwaarden voor mededeling is voldaan.)

f. bewaartermijnen

– De PIE bewaart de PNR-gegevens in een database gedurende een termijn van vijf jaar nadat de gegevens zijn doorgestuurd aan de PIE van de lidstaat waar de vlucht aankomt of vertrekt.
– Na het verstrijken van een termijn van twee jaar na de overdracht van de data wordt een aantal gegevenselementen waaruit de identiteit van de passagier waarop de PNR-gegevens betrekking heeft, rechtstreeks zou kunnen worden afgeleid door afscherming geanonimiseerd (naam, adres en contactgegevens, alle betalingsinformatie, informatie betreffende frequent reizen *(frequent flyers),* algemene opmerkingen in relatie tot de identiteit van de passagier, op voorhand af te geven API-gegevens – voor zover verzameld).
– Na de termijn van twee jaar wordt mededeling van de volledige PNR-gegevens uitsluitend toegestaan als dat nodig is voor een concreet geval binnen de doelbinding en met in achtneming van toestemming door een rechterlijke of andere nationale instantie die volgens het nationale recht bevoegd is om na te gaan of aan de voorwaarden voor mededeling is voldaan.
– Na de termijn van vijf jaar worden de PNR-gegevens gewist. Deze verplichting geldt niet indien bepaalde PNR-gegevens zijn doorgegeven aan een bevoegde instantie en worden gebruikt in het kader van een specifieke zaak met het oog op het voorkomen, opsporen, onderzoeken of vervolgen. In dat geval geschiedt het bewaren onder het regime van het nationale recht van de lidstaat.
– Een PIE van een lidstaat kan de PNR-gegevens verwerken voor het beoordelen van de passagiers voor hun geplande aankomst of vertrek om te bepalen welke personen moeten onderworpen aan een nader onderzoek omdat ze betrokken zouden kunnen zijn bij een terroristisch misdrijf of bij zware criminaliteit. Als deze verwerkingsmethode tot resultaat leidt dan bewaart de PIE het resultaat niet langer dan noodzakelijk is om een overeenstemming te kunnen melden aan de bevoegde instanties.

g. beveiligingseisen.

– De bepalingen die ter uitvoering van de artikelen 21 en 22 van genoemd Kaderbesluit zijn vastgesteld betreffende de vertrouwelijkheid en de beveiliging van gegevens zijn van toepassing.

– Verwerking van PNR-gegevens waaruit ras, etnische afstemming, religieuze, levensbeschouwelijke of politieke overtuiging, vakbondslidmaatschap, gezondheid of seksleven van de betrokkene blijken, is verboden. Als de PIE PNR-gegevens ontvangt waaruit dergelijke informatie blijkt, dan worden deze onverwijld gewist.
– De PIE en de bevoegde instanties moeten iedere verwerking registreren of documenteren, zodat kan worden gecontroleerd of de gegevens verwerking rechtmatig is, interne controle kan worden uitgeoefend en de integriteit van de gegevens en de beveiliging van de gegevensverwerking kunnen worden gewaarborgd, met name door de nationale toezichthoudende autoriteiten voor gegevensbescherming. Deze logbestanden worden – behoudens concrete uitzonderingen – gedurende vijf jaar bewaard.