HANDBOEK

Handboek Europese gegevensbeschermings-wetgeving

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Het manuscript van dit handboek is voltooid in april 2014.
Toekomstige actualiseringen zullen worden gepubliceerd op de website van het FRA: fra.europa.eu, de website van de Raad van Europa: www.coe.int/dataprotection, en op de website van het Europees Hof voor de Rechten van de Mens in het menu Jurisprudentie („Case-Law"): echr.coe.int.

Europe Direct helpt u antwoord te vinden op uw vragen over de Europese Unie.

Gratis nummer (*):

00 800 6 7 8 9 10 11

(*) De informatie wordt gratis verstrekt en bellen is doorgaans gratis, maar sommige operatoren, telefooncellen of hotels kunnen kosten aanrekenen.

Foto (voorblad en binnenzijde): © iStockphoto

Meer gegevens over de Europese Unie vindt u op internet via de Europaserver (http://europa.eu).

Catalografische gegevens bevinden zich aan het einde van deze publicatie.

Luxemburg: Bureau voor publicaties van de Europese Unie, 2014

ISBN 978-92-871-9941-6 (Raad van Europa)
ISBN 978-92-9239-497-4 (FRA)
doi:10.2811/73787

Printed in Belgium

GEDRUKT OP CHLOORVRIJ GERECYCLEERD PAPIER (PCF)

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Handboek Europese gegevensbeschermings-wetgeving

Voorwoord

Dit handboek over de Europese gegevensbeschermingswetgeving is een gezamenlijke productie van het Bureau van de Europese Unie voor de grondrechten (Fundamental Rights Agency – FRA), de Raad van Europa en de griffie van het Europees Hof voor de rechten van de mens. Dit is het derde in een reeks juridische handboeken die gezamenlijk door FRA en de Raad van Europa worden geproduceerd. In maart 2011 werd een eerste handboek gepubliceerd, over de Europese non-discriminatiewetgeving, en in juni 2013 verscheen het tweede handboek over het Europese recht op het gebied van asiel, grenzen en immigratie.

Vervolgens besloten we ons te richten op een bijzonder actueel onderwerp waar we allemaal dagelijks mee te maken hebben, namelijk de bescherming van persoonsgegevens. Europa heeft een van de meest beschermende systemen op dit gebied, dat is gebaseerd op Verdrag 108 van de Raad van Europa, instrumenten van de Europese Unie (EU) en de jurisprudentie van het Europees Hof voor de rechten van de mens (EHRM) en van het Hof van Justitie van de Europese Unie (HvJ-EU).

Het handboek beoogt het bewustzijn en de kennis van gegevensbeschermingsregels in de Europese Unie en de lidstaten van de Raad van Europa te vergroten door voor de lezers als het belangrijkste referentiepunt op dit gebied te fungeren. Het handboek is bedoeld voor niet-gespecialiseerde beoefenaars van juridische beroepen, rechters, nationale gegevensbeschermingsautoriteiten en andere personen die werkzaam zijn op het gebied van gegevensbescherming.

Met de inwerkingtreding van het Verdrag van Lissabon in december 2009 werd het Handvest van de grondrechten van de EU wettelijk bindend, waarmee het recht op bescherming van persoonsgegevens de status van een afzonderlijk grondrecht kreeg. Een beter begrip van Verdrag 108 van de Raad van Europa en van de toepasselijke EU-instrumenten, die de weg voor gegevensbescherming in Europa hebben geplaveid, alsmede van de jurisprudentie van het EHRM en het HvJ-EU, is van essentieel belang voor de bescherming van dit grondrecht.

We willen met name de gegevensbeschermingseenheid van de Europese Commissie bedanken voor de ondersteuning die deze ons tijdens het opstellen van dit handboek heeft gegeven. Ook gaat onze dank uit naar het bureau van de Europese Toezichthouder voor gegevensbescherming voor de bijdragen die het heeft geleverd tijdens het opstellen van het handboek. Tot slot bedanken wij Bastiaan Suurmond voor het bijwerken van de Nederlandse vertaling van het handboek.

Philippe Boillat

Directeur-generaal
Mensenrechten en rechtsstaat
Raad van Europa

Morten Kjaerum

Directeur
Bureau voor de grondrechten
Europese Unie

Inhoudsopgave

Afkortingen en acroniemen

CETS	Council of Europe Treaty Series
CRM	Customer relations management
C.SIS	Centraal deel van het Schengeninformatiesysteem
DIS	Douane-informatiesysteem
EDPS	Europese Toezichthouder voor gegevensbescherming
EER	Europese Economische Ruimte
EG	Europese Gemeenschap
EHRM	Europees Hof voor de rechten van de mens
ENISA	Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging
ESMA	Europese Autoriteit voor effecten en markten
eTEN	Trans-Europese telecommunicatienetwerken
EU	Europese Unie
eu-LISA	EU-agentschap voor grootschalige IT-systemen
EuroPriSe	European Privacy Seal
EVA	Europese Vrijhandelsassociatie
EVRM	Europees Verdrag tot bescherming van de rechten van de mens
FRA	Bureau van de Europese Unie voor de grondrechten
GCO	Gemeenschappelijk Controleorgaan
GPS	Global positioning system
Handvest	Handvest van de grondrechten van de Europese Unie
HvJ-EU	Hof van Justitie van de Europese Unie (tot december 2009 Hof van Justitie van de Europese Gemeenschappen (HvJ-EG) geheten)
NEE	Nationale Europol-eenheid
NGO	Niet-gouvernementele organisatie
N.SIS	Nationaal deel van het Schengeninformatiesysteem

OESO	Organisatie voor economische samenwerking en ontwikkeling
PIN	Persoonlijk identificatienummer
PNR	Passenger name record
RvE	Raad van Europa
SEPA	Gemeenschappelijke betalingsruimte voor de euro
SIS	Schengeninformatiesysteem
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UVRM	Universele Verklaring van de rechten van de mens
Verdrag 108	Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (Raad van Europa)
VEU	Verdrag betreffende de Europese Unie
VIS	Visuminformatiesysteem
VN	Verenigde Naties
VWEU	Verdrag betreffende de werking van de Europese Unie

Hoe dit handboek te gebruiken

Dit handboek biedt een overzicht van de wetgeving die van toepassing is op gegevensbescherming met betrekking tot de Europese Unie (EU) en de Raad van Europa (RvE).

Het handboek is bedoeld voor niet in gegevensbescherming gespecialiseerde beoefenaars van juridische beroepen, zoals advocaten, rechters en andere beoefenaars van juridische beroepen, maar ook voor personen die werkzaam zijn voor andere organen, zoals niet-gouvernementele organisaties (ngo's), die in hun werk te maken kunnen krijgen met juridische vraagstukken die verband houden met gegevensbescherming.

In het handboek, dat een eerste referentiepunt over het EU-recht en het Europees Verdrag tot bescherming van de rechten van de mens (EVRM) vormt voor wat betreft gegevensbescherming, wordt uitgelegd hoe dit domein is gereguleerd in het EU-recht, het EVRM en het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108) en andere instrumenten van de RvE. In elk hoofdstuk wordt eerst een tabel met de van toepassing zijnde wettelijke bepalingen gegeven, met inbegrip van belangrijke geselecteerde jurisprudentie van de twee afzonderlijke Europese rechtsstelsels. Vervolgens wordt de desbetreffende wetgeving van deze twee Europese rechtsstelsels na elkaar gepresenteerd zoals deze van toepassing zou kunnen zijn op elk onderwerp. Hierdoor kan de lezer zien op welke punten de twee rechtsstelsels overeenkomen en op welke punten ze van elkaar verschillen.

In de tabellen aan het begin van elk hoofdstuk worden de onderwerpen opgesomd die in dat hoofdstuk worden behandeld en worden de toepasselijke wettelijke bepalingen en ander relevant materiaal, zoals jurisprudentie, genoemd. De volgorde van de onderwerpen kan licht afwijken van de structuur van de tekst indien dit passend wordt geacht voor een beknopte presentatie van de inhoud van het hoofdstuk. In de tabellen wordt zowel wetgeving van de RvE als EU-wetgeving vermeld. Dit zou de gebruikers moeten helpen om de belangrijkste informatie met betrekking tot hun situatie te vinden, met name als ze alleen onder het RvE-recht vallen.

Beoefenaars van juridische beroepen in niet-EU-lidstaten die zijn aangesloten bij de RvE en partij zijn bij het EVRM en Verdrag 108 kunnen de informatie die relevant is voor hun eigen land vinden door rechtstreeks naar de gedeelten over de RvE-wetgeving te gaan. Beoefenaars van juridische beroepen in EU-lidstaten zullen beide

delen moeten gebruiken, omdat deze staten aan beide rechtsordes zijn gebonden. Voor wie behoefte heeft aan meer informatie over een bepaald onderwerp, is een lijst met verwijzingen naar meer gespecialiseerd materiaal opgenomen onder "Aanbevolen literatuur" achterin dit handboek.

De RvE-wetgeving wordt gepresenteerd door middel van korte verwijzingen naar geselecteerde zaken van het Europees Hof voor de rechten van de mens (EHRM). Deze zijn gekozen uit een groot aantal arresten en beslissingen van het EHRM over gegevensbeschermingsvraagstukken.

Het EU-recht is te vinden in de door de EU vastgestelde wetgevingsmaatregelen, in relevante bepalingen van de Verdragen en in het Handvest van de grondrechten van de Europese Unie, zoals uitgelegd in de jurisprudentie van het Hof van Justitie van de Europese Unie (HvJ-EU, tot december 2009 Hof van Justitie van de Europese Gemeenschappen (HvJ-EG) genoemd).

De in dit handboek beschreven of geciteerde jurisprudentie dient als voorbeeld van de uitgebreide jurisprudentie van zowel het EHRM als het HvJ-EU. De richtsnoeren aan het eind van dit handboek zijn bedoeld om de lezer te helpen bij het zoeken naar jurisprudentie op internet.

Voorts worden in tekstvakken en met behulp van hypothetische scenario's praktische voorbeelden gegeven die de toepassing van Europese gegevensbeschermingsregels in de praktijk nader illustreren, in het bijzonder wanneer er geen specifieke jurisprudentie van het EHRM of het HvJ-EU over het desbetreffende onderwerp bestaat.

Het handboek begint met een korte beschrijving van de rol van de twee rechtsstelsels als vastgesteld door het EVRM en het EU-recht (hoofdstuk 1). De hoofdstukken 2 tot en met 8 hebben betrekking op de volgende onderwerpen:

- gegevensbeschermingsterminologie;
- de belangrijkste beginselen van de Europese gegevensbeschermingswetgeving;
- de voorschriften van de Europese gegevensbeschermingswetgeving;
- de rechten van betrokkenen en de handhaving van deze rechten;

- grensoverschrijdend gegevensverkeer;
- gegevensbescherming in het kader van politie en justitie;
- andere specifieke Europese gegevensbeschermingswetgeving.

1

Context en achtergrond van de Europese gegevensbeschermingswetgeving

EU	Behandelde onderwerpen	RvE
Het recht op gegevensbescherming		
Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*richtlijn gegevensbescherming*), PB L 281 van 23.11.1995, blz. 31.		EVRM, artikel 8 (recht op respect voor het privé-, familie- en gezinsleven, de woning en de correspondentie) Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108)
Afweging van rechten		
HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert / Land Hessen*, 9 november 2010	**Algemeen**	
HvJ-EU, zaak C-73/07, *Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy en Satamedia Oy*, 16 december 2008	**Vrijheid van meningsuiting**	EHRM, *Axel Springer AG / Duitsland*, nr. 39954/08, 7 februari 2012 EHRM, *Mosley / Verenigd Koninkrijk*, nr. 48009/08, 10 mei 2011
	Vrijheid van kunsten en wetenschappen	EHRM, *Vereinigung bildender Künstler / Oostenrijk*, nr. 68345/01, 25 januari 2007

EU	Behandelde onderwerpen	RvE
HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, 29 january 2008	Bescherming van eigendom	
HvJ-EU, zaak C-28/08 P, *Europese Commissie / The Bavarian Lager Co. Ltd*, 29 juni 2010	Toegang tot documenten	EHRM, *Társaság a Szabadságjogokért / Hongarije*, nr. 37374/05, 14 april 2009

1.1. Het recht op gegevensbescherming

Belangrijkste punten

- Krachtens artikel 8 van het EVRM is een recht op bescherming tegen de verzameling en het gebruik van persoonsgegevens onderdeel van het recht op respect voor het privé-, familie- en gezinsleven, de woning en de correspondentie.
- Verdrag 108 van de Raad van Europa is het eerste internationale wettelijk bindende instrument dat uitdrukkelijk betrekking heeft op gegevensbescherming.
- In het EU-recht is gegevensbescherming voor het eerst gereguleerd in de richtlijn gegevensbescherming.
- In het EU-recht is gegevensbescherming erkend als een grondrecht.

Het recht op bescherming van natuurlijke personen tegen inbreuken op hun persoonlijke levenssfeer, met name door de staat, is voor het eerst in een internationaal rechtsinstrument vastgelegd in artikel 12 van de Universele Verklaring van de rechten van de mens (UVRM) van de Verenigde Naties (VN) van 1948 inzake de eerbiediging van het privé- en gezinsleven.[1] De UVRM is van grote invloed geweest op de ontwikkeling van andere mensenrechteninstrumenten in Europa.

1 Verenigde Naties (VN), Universele Verklaring van de rechten van de mens (UVRM), 10 december 1948.

1.1.1. Het Europees Verdrag tot bescherming van de rechten van de mens

De Raad van Europa (RvE) is opgericht in de nasleep van de Tweede Wereldoorlog om de staten van Europa te verenigen met het oog op de bevordering van de rechtsstaat, democratie, de mensenrechten en sociale ontwikkeling. Hiertoe heeft de RvE in 1950 het Europees Verdrag tot bescherming van de rechten van de mens (EVRM) aangenomen, dat in 1953 in werking trad.

De lidstaten hebben een internationale verplichting om het EVRM na te leven. Alle lidstaten van de RvE hebben het EVRM inmiddels in hun nationaal recht geïntegreerd of rechtskracht aan het EVRM gegeven, waardoor ze in overeenstemming met de bepalingen van het verdrag moeten handelen.

Om ervoor te zorgen dat de verdragsluitende partijen hun verplichtingen uit hoofde van het EVRM nakomen, is in 1959 het Europees Hof voor de rechten van de mens (EHRM) opgericht, dat is gevestigd in Straatsburg, Frankrijk. Het EHRM zorgt ervoor dat staten hun verplichtingen uit hoofde van het EVRM nakomen door klachten van natuurlijke personen, groepen van natuurlijke personen, ngo's of rechtspersonen naar aanleiding van een vermeende inbreuk op het EVRM te beoordelen. In 2013 telde de RvE 47 lidstaten, waarvan er 28 ook lidstaat van de EU zijn. Iemand hoeft geen onderdaan van een van de lidstaten te zijn om een verzoek bij het EHRM te kunnen indienen. Het EHRM kan ook geschillen tussen staten die door een of meer RvE-lidstaten tegen een andere lidstaat aanhangig zijn gemaakt, aan een onderzoek onderwerpen.

Het recht op bescherming van persoonsgegevens maakt deel uit van de rechten die worden beschermd door artikel 8 van het EVRM, dat het recht op respect voor het privé-, familie- en gezinsleven, de woning en de correspondentie garandeert en waarin de voorwaarden zijn neergelegd waaronder beperkingen van dit recht zijn toegestaan.[2]

In zijn jurisprudentie heeft het EHRM een groot aantal situaties beoordeeld waarin het vraagstuk van gegevensbescherming naar voren kwam, niet in de laatste plaats met betrekking tot de onderschepping van communicatie,[3] verschillende vormen

2 RvE, Europees Verdrag tot bescherming van de rechten van de mens, CETS nr. 005, 1950.

3 Zie bijvoorbeeld EHRM, *Malone / Verenigd Koninkrijk*, nr. 8691/79, 2 augustus 1984; EHRM, *Copland / Verenigd Koninkrijk*, nr. 62617/00, 3 april 2007.

van surveillance[4] en bescherming tegen de opslag van persoonsgegevens door overheidsautoriteiten.[5] Het EHRM heeft verduidelijkt dat artikel 8 van het EVRM staten niet alleen verplicht om zich te onthouden van elke handeling die mogelijk een inbreuk op dit verdragsrecht vormt, maar dat ze in bepaalde omstandigheden ook een positieve verplichting hebben om de effectieve eerbiediging van het privé-, familie- en gezinsleven actief te waarborgen.[6] Op veel van deze zaken zal in de desbetreffende hoofdstukken nader worden ingegaan.

1.1.2. Verdrag 108 van de Raad van Europa

Met de opkomst van de informatietechnologie in de jaren zestig van de vorige eeuw ontstond er een toenemende behoefte aan meer gedetailleerde regels om natuurlijke personen bescherming te bieden door hun (persoons)gegevens te beschermen. Medio de jaren zeventig nam het Comité van ministers van de RvE een aantal resoluties over de bescherming van persoonsgegevens aan, onder verwijzing naar artikel 8 van het EVRM.[7] In 1981 werd een Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108)[8] ter ondertekening opengesteld. Verdrag 108 was, en is nog steeds, het enige internationale wettelijk bindende instrument op het gebied van gegevensbescherming.

Verdrag 108 is van toepassing op alle gegevensverwerkingen uitgevoerd door zowel de private als de publieke sector, zoals verwerkingen door de rechterlijke macht en rechtshandhavingsautoriteiten. Het beschermt natuurlijke personen tegen misbruik dat kan plaatsvinden bij de verzameling en verwerking van persoonsgegevens en beoogt tegelijkertijd het grensoverschrijdend verkeer van persoonsgegevens te reguleren. Wat betreft de verzameling en verwerking van persoonsgegevens hebben de beginselen die in het verdrag zijn vastgelegd met name betrekking

4 Zie bijvoorbeeld EHRM, *Klass en anderen / Duitsland*, nr. 5029/71, 6 september 1978; EHRM, *Uzun / Duitsland*, nr. 35623/05, 2 september 2010.

5 Zie bijvoorbeeld EHRM, *Leander / Zweden*, nr. 9248/81, 26 maart 1987; EHRM, *S. en Marper / Verenigd Koninkrijk*, nr. 30562/04 en 30566/04, 4 december 2008.

6 Zie bijvoorbeeld EHRM, *I. / Finland*, nr. 20511/03, 17 juli 2008; EHRM, *K.U. / Finland*, nr. 2872/02, 2 december 2008.

7 RvE, Comité van ministers (1973), Resolutie (73) 22 inzake de bescherming van de persoonlijke levenssfeer bij geautomatiseerde registratiesystemen in de particuliere sector, 26 september 1973; RvE, Comité van ministers (1974), Resolutie (74) 29 inzake de bescherming van de persoonlijke levenssfeer bij geautomatiseerde registratiesystemen in de publieke sector, 20 september 1974.

8 Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (Raad van Europa, CETS nr. 108, 1981).

op een eerlijke en rechtmatige verzameling en automatische verwerking van gegevens, die worden opgeslagen voor duidelijk omschreven en gerechtvaardigde doeleinden, en niet op een wijze die onverenigbaar is met die doeleinden, en die niet langer mogen worden bewaard dan noodzakelijk is. Ook hebben ze betrekking op de kwaliteit van de gegevens, die in het bijzonder toereikend, ter zake dienend, nauwkeurig en niet overmatig (onevenredig) dienen te zijn.

Behalve dat Verdrag 108 garanties biedt ten aanzien van de verzameling en verwerking van persoonsgegevens, verbiedt het, bij ontstentenis van passende wettelijke waarborgen, de verwerking van "gevoelige" gegevens, zoals gegevens betreffende ras, politieke overtuiging, gezondheid, seksuele geaardheid, godsdienst of andere levensbeschouwing of strafrechtelijk verleden.

Ook is in het verdrag het recht vervat van een natuurlijke persoon om te weten welke informatie over hem of haar is opgeslagen en indien nodig om deze te laten corrigeren. Beperkingen van de in het verdrag vastgelegde rechten zijn alleen mogelijk wanneer hogere belangen, zoals de staatsveiligheid of defensie, in het geding zijn.

Hoewel het verdrag voorziet in vrij verkeer van persoonsgegevens tussen staten die partij zijn bij het verdrag, legt het ook enkele beperkingen op aan deze stromen naar staten waarvan de wettelijke bepalingen geen gelijkwaardige bescherming bieden.

Om de in Verdrag 108 neergelegde algemene beginselen en voorschriften verder te ontwikkelen, heeft het Comité van ministers van de RvE diverse aanbevelingen vastgesteld, die niet wettelijk bindend zijn (zie de hoofdstukken 7 en 8).

Alle EU-lidstaten hebben Verdrag 108 geratificeerd. In 1999 is het verdrag gewijzigd om de EU als partij te laten toetreden tot het verdrag.[9] In 2001 is een Aanvullend Protocol bij Verdrag 108 aangenomen, dat bepalingen invoerde inzake grensoverschrijdende gegevensstromen naar niet-verdragspartijen, zogeheten derde landen, en de verplichte oprichting van nationale toezichthoudende autoriteiten voor gegevensbescherming.[10]

9 RvE, wijzigingen in het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108) die het voor de Europese Gemeenschappen mogelijk maakten om toe te treden, aangenomen door het Comité van ministers op 15 juni 1999 in Straatsburg; artikel 23, lid 2, van Verdrag 108 in zijn gewijzigde vorm.

10 RvE, Aanvullend Protocol bij het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, betreffende toezichthoudende autoriteiten en de grensoverschrijdende gegevensstromen, CETS nr. 181, 2001.

Vooruitzichten

Na een besluit om Verdrag 108 te moderniseren maakte een openbare raadpleging in 2011 het mogelijk om de twee belangrijkste doelstellingen van deze exercitie te bekrachtigen: het verbeteren van de bescherming van de privacy in de digitale ruimte en het versterken van de follow-upmechanismen van het verdrag.

Verdrag 108 staat open voor toetreding door niet-lidstaten van de RvE, met inbegrip van niet-Europese landen. Het potentieel van het Verdrag als universele norm en het open karakter ervan zou als basis kunnen dienen voor het bevorderen van gegevensbescherming op mondiaal niveau.

Tot dusver zijn 45 van de 46 partijen bij Verdrag 108 lidstaat van de RvE. Uruguay, het eerste niet-Europese land, trad in augustus 2013 toe, en Marokko, dat door het Comité van ministers is uitgenodigd om tot het verdrag toe te treden, doorloopt op het moment van schrijven de formele procedure voor toetreding.

1.1.3. Gegevensbeschermingswetgeving van de Europese Unie

Het EU-recht bestaat uit verdragen en secundair EU-recht. De Verdragen, te weten het Verdrag betreffende de Europese Unie (VEU) en het Verdrag betreffende de werking van de Europese Unie (VWEU), zijn door alle EU-lidstaten goedgekeurd en worden ook wel aangeduid als het "primaire EU-recht". De verordeningen, richtlijnen en besluiten van de EU zijn vastgesteld door de EU-instellingen waaraan deze bevoegdheid is toegekend door de Verdragen; ze worden vaak "secundair EU-recht" genoemd.

Het belangrijkste wettelijke instrument van de EU op het gebied van gegevensbescherming is 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 (*richtlijn gegevensbescherming*).[11] De richtlijn is vastgesteld in 1995, toen verschillende lidstaten reeds nationale gegevensbeschermingswetgeving hadden aangenomen. Voor het vrije verkeer van goederen, kapitaal, diensten en personen binnen de interne markt was vrij verkeer van gegevens nodig, dat niet

11 Richtlijn gegevensbescherming, PB L 281 van 23.11.1995, blz. 31.

gerealiseerd kon worden totdat de lidstaten konden vertrouwen op een hoog niveau van gegevensbescherming.

Omdat het doel van de richtlijn gegevensbescherming de harmonisatie[12] van de gegevensbeschermingswetgeving op nationaal niveau was, staat de richtlijn een zekere mate van specificiteit toe die vergelijkbaar is met die van de (op dat moment) bestaande nationale gegevensbeschermingswetgeving. Het HvJ-EU overweegt dat "richtlijn 95/46 (...) de bescherming van de rechten en vrijheden van personen op het stuk van de verwerking van persoonsgegevens in alle lidstaten op hetzelfde niveau wil brengen. [En] dat de onderlinge aanpassing van de ter zake geldende nationale wetgevingen niet tot een verzwakking van de aldus geboden bescherming mag leiden, maar juist erop gericht moet zijn een hoog beschermingsniveau in de Unie te waarborgen. [Waardoor] de harmonisatie van vorenbedoelde nationale wettelijke regelingen zich niet beperkt tot een minimumharmonisatie, maar in beginsel tot een volledige harmonisatie dient te leiden."[13] Bijgevolg hebben de lidstaten een zekere, zij het beperkte, manoeuvreerruimte bij de tenuitvoerlegging van de richtlijn.

De richtlijn gegevensbescherming is ontworpen om invulling te geven aan de beginselen van het recht op privacy dat reeds was vervat in Verdrag 108, en om dit recht uit te breiden. Het feit dat in 1995 alle 15 EU-lidstaten ook partij bij Verdrag 108 waren, maakt het onmogelijk om tegenstrijdige voorschriften in deze twee rechtsinstrumenten op te nemen. De richtlijn gegevensbescherming maakt echter gebruik van de mogelijkheid die artikel 11 van Verdrag 108 biedt om beschermingsinstrumenten toe te voegen. Met name de invoering van onafhankelijk toezicht als instrument voor het verbeteren van de naleving van gegevensbeschermingsvoorschriften is een belangrijke bijdrage tot de doeltreffende werking van de Europese gegevensbeschermingswetgeving gebleken. (Bijgevolg werd dit kenmerk in 2001 overgenomen in het RvE-recht, in het Aanvullend Protocol bij Verdrag 108.)

De territoriale toepassing van de richtlijn gegevensbescherming strekt zich niet alleen uit tot de 28 EU-lidstaten, maar ook tot de niet-EU-lidstaten die deel uitmaken

12 Zie bijvoorbeeld de overwegingen 1, 4, 7 en 8 van de richtlijn gegevensbescherming.

13 HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24 november 2011, punten 28 en 29.

van de Europese Economische Ruimte (EER)[14] – te weten IJsland, Liechtenstein en Noorwegen.

Het HvJ-EU in Luxemburg heeft rechtsbevoegdheid om te bepalen of een lidstaat zijn verplichtingen uit hoofde van de richtlijn gegevensbescherming heeft vervuld en om bij wijze van prejudiciële beslissing uitspraak te doen over de geldigheid en de interpretatie van de richtlijn om een effectieve en uniforme toepassing daarvan in de lidstaten te waarborgen. Een belangrijke uitzondering op de toepasbaarheid van de richtlijn gegevensbescherming is de zogeheten "uitzondering voor huishoudens", d.w.z. de verwerking van persoonsgegevens door particuliere natuurlijke personen voor uitsluitend persoonlijke of huishoudelijke doeleinden.[15] Dit type verwerking wordt algemeen gezien als onderdeel van de vrijheden van particulieren.

In overeenstemming met het primaire EU-recht dat van kracht was ten tijde van de vaststelling van de richtlijn gegevensbescherming is het materiële toepassingsgebied van de richtlijn beperkt tot internemarktaangelegenheden. De belangrijkste onderwerpen die buiten het toepassingsgebied van de richtlijn vallen zijn politiële en justitiële samenwerking in strafzaken. De gegevensbescherming in het kader van politiële en justitiële samenwerking in strafzaken is geregeld in andere rechtsinstrumenten, die gedetailleerd worden beschreven in hoofdstuk 7.

Omdat de richtlijn gegevensbescherming alleen tot de EU-lidstaten kon worden gericht, was een aanvullend rechtsinstrument nodig om gegevensbescherming in verband met de verwerking van persoonsgegevens door instellingen en organen van de EU te reguleren. Verordening (EG) nr. 45/2001 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens (*verordening gegevensbescherming EU-instellingen*) vervult deze taak.[16]

Voorts zijn zelfs in gebieden die onder de richtlijn gegevensbescherming vallen vaak meer gedetailleerde gegevensbeschermingsbepalingen nodig om de vereiste

14 Overeenkomst betreffende de Europese Economische Ruimte, PB L 1 van 30.11.1994, blz. 6, die in werking trad op 1 januari 1994.

15 Richtlijn gegevensbescherming, artikel 3, lid 2, tweede streepje.

16 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, PB L 8 van 12.1.2001, blz. 1.

duidelijkheid bij het afwegen van rechtmatige belangen te kunnen verwezenlijken. Twee voorbeelden hiervan zijn Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (*richtlijn betreffende privacy en elektronische communicatie*)[17] en Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (*richtlijn gegevensbewaring*, ongeldig verklaard op 8 april 2014).[18] Andere voorbeelden zullen worden besproken in hoofdstuk 8. Deze bepalingen moeten in overeenstemming zijn met de richtlijn gegevensbescherming.

Handvest van de grondrechten van de Europese Unie

De oorspronkelijke verdragen van de Europese Gemeenschappen bevatten geen verwijzing naar de rechten van de mens of de bescherming daarvan. Omdat er zaken voor het toenmalige Hof van Justitie van de Europese Gemeenschappen (HvJ-EG) werden gebracht waarin mensenrechtenschendingen op gebieden die binnen het toepassingsgebied van het EU-recht vielen aan de kaak werden gesteld, ontwikkelde het Hof echter een nieuwe aanpak. Om natuurlijke personen te beschermen, heeft het HvJ-EG grondrechten tot een van de zogeheten algemene beginselen van het Europees recht gemaakt. Volgens het HvJ-EU weerspiegelen deze algemene beginselen de inhoud van de mensenrechtenbescherming die wordt geboden door nationale grondwetten en mensenrechtenverdragen, met name het EVRM. Het HvJ-EU verklaarde te zullen waarborgen dat deze beginselen in het EU-recht zouden worden nageleefd.

Erkennend dat haar beleid consequenties voor de mensenrechten kon hebben en in een poging de EU 'dichter bij' de burgers te brengen, kondigde de EU in 2000 plechtig het Handvest van de grondrechten van de Europese Unie af. Doordat de grondwettelijke tradities en internationale verplichtingen die gemeenschappelijk voor de lidstaten zijn tot één geheel zijn gemaakt, omvat dit Handvest het hele scala aan

17 Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (*richtlijn betreffende privacy en elektronische communicatie*), PB L 201 van 31.7.2002, blz. 37, ongeldig verklaard op 8 april 2014.

18 Richtlijn 2006/24/EG van het Europees Parlement en de Raad betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (*richtlijn gegevensbewaring*), PB L 105 van 13.4.2006, blz. 54.

politieke, economische en sociale en burgerrechten van de Europese Unie. De rechten die in het Handvest worden beschreven, zijn onderverdeeld in zes titels: waardigheid, vrijheden, gelijkheid, solidariteit, burgerschap en rechtspleging.

Hoewel het Handvest aanvankelijk slechts een politiek document was, werd het wettelijk bindend[19] als primair EU-recht (zie artikel 6, lid 1, van het VEU) met de inwerkingtreding van het Verdrag van Lissabon op 1 december 2009.[20]

Het primaire EU-recht bevat ook een bepaling die de EU een algemene bevoegdheid verleent om wetgeving over gegevensbeschermingsaangelegenheden vast te stellen (artikel 16 van het VWEU).

Het Handvest garandeert niet alleen de eerbiediging van het privé-, familie- en gezinsleven (artikel 7), maar ook het recht op gegevensbescherming (artikel 8), waardoor de status van gegevensbescherming is verhoogd naar het niveau van grondrecht in het EU-recht. De EU-instellingen en de lidstaten moeten dit recht, dat ook van toepassing is op de lidstaten wanneer deze het EU-recht ten uitvoer brengen (artikel 51 van het Handvest) in acht nemen en waarborgen. Artikel 8 van het Handvest, dat jaren na de goedkeuring van de richtlijn gegevensbescherming is geformuleerd, moet worden begrepen als de belichaming van daarvóór reeds bestaande EU-gegevensbeschermingsrecht. In het Handvest wordt daarom niet alleen in artikel 8, lid 1, uitdrukkelijk het recht op gegevensbescherming genoemd, maar worden in artikel 8, lid 2, ook de belangrijkste beginselen van gegevensbescherming vermeld. Tot slot zorgt artikel 8, lid 3, van het Handvest ervoor dat een onafhankelijke autoriteit erop toeziet dat deze beginselen worden nageleefd.

Vooruitzichten

In januari 2012 heeft de Europese Commissie een hervormingspakket inzake gegevensbescherming voorgesteld, waarin de Commissie verklaarde dat de huidige gegevensbeschermingsregels moesten worden gemoderniseerd in het licht van de snelle technologische ontwikkelingen en de globalisering. Het hervormingspakket

19 EU (2012), Handvest van de grondrechten van de Europese Unie, PB C 326 van 26.10.2012, blz. 391.

20 Zie de geconsolideerde versies van het Verdrag betreffende de Europese Unie, PB C 326 van 26.10.2012, blz. 13, en het Verdrag betreffende de werking van de Europese Unie, PB C 326 van 26.10.2012, blz. 47.

bestaat uit een voorstel voor een algemene verordening gegevensbescherming[21], die de richtlijn gegevensbescherming moet vervangen, en een nieuwe richtlijn gegevensbescherming[22], die voorziet in gegevensbescherming op het gebied van politiële en justitiële samenwerking in strafzaken. Ten tijde van de publicatie van dit handboek was de discussie over het hervormingspakket nog gaande.

1.2. Afweging van rechten

Belangrijkste punt

- Het recht op gegevenbescherming is geen absoluut recht; het moet worden afgewogen tegen andere rechten.

Het grondrecht van bescherming van persoonsgegevens uit hoofde van artikel 8 van het Handvest "heeft evenwel geen absolute gelding, maar moet in relatie tot de functie ervan in de maatschappij worden beschouwd".[23] Artikel 52, lid 1, van het Handvest aanvaardt derhalve dat aan de uitoefening van rechten als die welke zijn neergelegd in de artikel en 7 en 8 van het Handvest beperkingen kunnen worden gesteld, voor zover deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten en vrijheden eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, 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.[24]

In het EVRM-stelsel wordt gegevensbescherming gegarandeerd door artikel 8 (eerbiediging van het privé-, familie- en gezinsleven), en net als in het Handveststelsel

21 Europese Commissie (2012), 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*), COM(2012) 11 definitief, Brussel, 25 januari 2012.

22 Europese Commissie (2012), 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 (*algemene richtlijn gegevensbescherming*), COM(2012) 10 definitief, Brussel, 25 januari 2012.

23 Zie bijvoorbeeld het arrest van het HvJ-EU in de gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR (C-92/09) en Hartmut Eifert (C-93/09) / Land Hessen*, punt 48.

24 *Ibid*., punt 50.

moet dit recht worden toegepast met inachtneming van de werkingssfeer van andere, concurrerende rechten. Krachtens artikel 8, lid 2, van het EVRM, is "[g]een inmenging van enig openbaar gezag (...) toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is voor (...) de bescherming van de rechten en vrijheden van anderen".

Bijgevolg hebben het EHRM en het HvJ-EU herhaaldelijk geoordeeld dat er een afweging met andere rechten moet plaatsvinden bij de toepassing en uitleg van artikel 8 van het EVRM en artikel 8 van het Handvest.[25] Met een aantal belangrijke voorbeelden zal hieronder worden geïllustreerd hoe deze afweging wordt bereikt.

1.2.1. Vrijheid van meningsuiting

Een van de rechten die in botsing kunnen komen met het recht op gegevensbescherming is het recht op vrijheid van meningsuiting.

De vrijheid van meningsuiting wordt beschermd door artikel 11 van het Handvest ("Vrijheid van meningsuiting en van informatie"). Dit recht omvat de "vrijheid een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen". Artikel 11 Handvest komt overeen met artikel 10 van het EVRM. Krachtens artikel 52, lid 3, van het Handvest, zijn, voor zover het Handvest rechten bevat die corresponderen met rechten die worden gegarandeerd door het EVRM, "de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend". De beperkingen die bij wet kunnen worden gesteld aan het door artikel 11 van het Handvest gegarandeerde recht kunnen derhalve niet verder gaan dan die waarin wordt voorzien in artikel 10, lid 2, van het EVRM, d.w.z. dat ze wettelijk moeten zijn voorgeschreven en in een democratische samenleving noodzakelijk moeten zijn voor "de bescherming van de goede naam of de rechten van anderen". Dit concept omvat het recht op gegevensbescherming.

25 EHRM, *Von Hannover / Duitsland* (nr. 2) [GC], nrs. 40660/08 en 60641/08, 7 februari 2012; HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24 november 2011, punt 48; HvJ-EU, C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, 29 januari 2008, punt 68. Zie ook Raad van Europa (2013), jurisprudentie van het Europees Hof voor de rechten van de mens inzake de bescherming van persoonsgegevens, DP (2013) Case law, te vinden op: http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP%202013%20Case%20Law_Eng_FINAL.pdf.

De verhouding tussen de bescherming van persoonsgegevens en de vrijheid van meningsuiting wordt geregeld door artikel 9 van de richtlijn gegevensbescherming, getiteld "Verwerking van persoonsgegevens en vrijheid van meningsuiting".[26] Volgens dit artikel dienen de lidstaten te voorzien in uitzonderingen op of beperkingen van de gegevensbescherming, en dus van het fundamentele recht op privéleven als neergelegd in de hoofdstukken II, IV en VI van deze richtlijn. Deze uitzonderingen mogen uitsluitend worden gemaakt voor journalistieke, artistieke of literaire doeleinden, die onder het fundamentele recht van de vrijheid van meningsuiting vallen, en enkel voor zover die uitzonderingen nodig blijken te zijn voor de verzoening van het recht op privéleven met de regels betreffende de vrijheid van meningsuiting.

Voorbeeld: In *Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy en Satamedia Oy*[27] werd het HvJ-EU verzocht om artikel 9 van de richtlijn gegevensbescherming te interpreteren en de verhouding tussen gegevensbescherming en persvrijheid te preciseren. Het HvJ-EU moest de publicatie door Markkinapörssi en Satamedia van belastinggegevens van circa 1,2 miljoen natuurlijke personen die zij rechtmatig van de Finse belastingautoriteiten hadden verkregen, aan een onderzoek onderwerpen. Met name moest het HvJ-EU verifiëren of de verwerking van persoonsgegevens – die de belastingdienst beschikbaar had gesteld – om gebruikers van mobiele telefoons de mogelijkheid te bieden belastinggegevens over andere natuurlijke personen te ontvangen, moest worden beschouwd als een activiteit die uitsluitend voor journalistieke doeleinden werd verricht. Na eerst te hebben geconcludeerd dat de activiteiten van Markkinapörssi en Satamedia als "verwerking van persoonsgegevens" in de zin van artikel 3, lid 1, van de richtlijn gegevensbescherming moesten worden beschouwd, gaf het HvJ-EU een uitleg van artikel 9 van de richtlijn. Daarbij wees het Hof in de eerste plaats op het belang van het recht van vrijheid van meningsuiting in elke democratische samenleving en stelde het dat met deze vrijheid samenhangende begrippen, waaronder het begrip journalistiek, ruim moeten worden geïnterpreteerd. Vervolgens merkte het HvJ-EU op dat om tot een evenwichtige afweging tussen de beide fundamentele rechten te komen, de uitzonderingen op en beperkingen van het recht op gegevensbescherming binnen de grenzen van het strikt noodzakelijke moeten blijven. In deze omstandigheden oordeelde het HvJ-EU dat activiteiten als die welke door Markkinapörssi en Satamedia werden verricht met betrekking tot gegevens afkomstig

26 Richtlijn gegevensbescherming, artikel 9.

27 HvJ-EU, zaak C-73/07, *Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy en Satamedia Oy*, 16 december 2009, punten 56, 61 en 62.

uit documenten die volgens de nationale wetgeving openbaar zijn, kunnen worden aangemerkt als "journalistieke activiteiten" indien zij de bekendmaking aan het publiek van informatie, meningen of ideeën tot doel hebben, ongeacht het overdrachtsmedium. Ook bepaalde het HvJ-EU dat deze activiteiten niet zijn voorbehouden aan mediaondernemingen en een winstoogmerk kunnen hebben. Het HvJ-EU oordeelde echter dat het aan de nationale rechter is om te bepalen of dit in een specifieke zaak het geval is.

Met betrekking tot de verzoening van het recht op gegevensbescherming met het recht van vrijheid van meningsuiting heeft het EHRM verschillende beginselarresten gewezen.

Voorbeeld: In *Axel Springer AG / Duitsland*[28] oordeelde het EHRM dat een verbod dat door een nationale rechtbank was opgelegd aan een eigenaar van een krant die een artikel over de aanhouding en veroordeling van een bekende acteur wilde publiceren, strijdig was met artikel 10 van het EVRM. Het EHRM herhaalde daarbij de criteria die het had vastgesteld in zijn jurisprudentie over het tegen elkaar afwegen van het recht van vrijheid van meningsuiting en het recht op eerbiediging van het privéleven:

- in de eerste plaats of de gebeurtenis waarop het gepubliceerde artikel betrekking had van algemeen belang was: de aanhouding en veroordeling van een persoon was een openbaar rechtsfeit en was derhalve van publiek belang;
- in de tweede plaats of de betrokken persoon een publieke figuur was: de betrokken persoon was een acteur die voldoende bekend was om als publiek figuur te kunnen worden aangemerkt; en
- in de derde plaats hoe de informatie was verkregen en of de informatie betrouwbaar was: de informatie was verstrekt door het bureau van de openbaar aanklager, en de juistheid van de informatie die beide publicaties bevatten werd door geen van de partijen betwist.

Bijgevolg oordeelde het EHRM dat de beperkingen aan de publicatie die aan het bedrijf waren opgelegd redelijkerwijs niet konden worden beschouwd als evenredig aan het rechtmatige doel om het privéleven van de verzoeker

28 EHRM, *Axel Springer AG / Duitsland* [GC], nr. 39954/08, 7 februari 2012, punten 90 en 91.

te beschermen. Het Hof concludeerde dat artikel 10 van het EVRM was geschonden.

Voorbeeld: In *Von Hannover / Duitsland* (nr. 2)[29] stelde het EHRM geen schending van het recht op eerbiediging van het privéleven uit hoofde van artikel 8 van het EVRM vast nadat een verzoek van prinses Caroline van Monaco om de publicatie van een foto van haar en haar echtgenoot tijdens een skivakantie te verbieden was afgewezen. De foto ging vergezeld van een artikel waarin onder andere melding werd gemaakt van de slechte gezondheid van prins Rainier. Het EHRM concludeerde dat de nationale rechtbanken het recht van vrijheid van meningsuiting van de uitgever zorgvuldig had afgewogen tegen het recht op eerbieding van het privéleven van verzoekster. De karakterisering door de nationale rechtbanken van de ziekte van prins Rainier als een voor de hedendaagse samenleving relevante gebeurtenis kon niet onredelijk worden geacht en het EHRM kon aanvaarden dat de foto, bezien in het licht van het artikel , althans in zekere mate bijdroeg tot een debat van algemeen belang. Het Hof concludeerde dat artikel 8 van het EVRM niet was geschonden.

In de jurisprudentie van het EHRM is een van de cruciale criteria met betrekking tot de afweging van rechten of de uiting in kwestie al dan niet bijdraagt tot een debat van algemeen publiek belang.

Voorbeeld: De zaak *Mosley / Verenigd Koninkrijk*[30] had betrekking op de publicatie van intieme foto's van de verzoeker door een nationaal weekblad. Verzoeker stelde dat er sprake was van een inbreuk op artikel 8 van het EVRM omdat hij voorafgaand aan de publicatie van de desbetreffende foto's geen publicatieverbod had kunnen eisen, aangezien het weekblad niet verplicht was om bij de publicatie van materiaal dat het recht op privacy zou kunnen schenden de betrokken persoon van tevoren van de publicatie in kennis te stellen. Hoewel de verspreiding van dit materiaal in algemene zin meer voor amusements- dan voor educatieve doeleinden had plaatsgevonden, genoot de publicatie zonder twijfel de bescherming van artikel 10 van het EVRM, die mogelijk moest wijken voor de eisen van artikel 8 van het EVRM indien de informatie privé en intiem van aard was en er geen algemeen belang werd gediend met de publicatie ervan. Daarbij diende echter zeer zorgvuldig te worden gekeken

29 EHRM, *Von Hannover / Duitsland (nr. 2)* [GC], nrs. 40660/08 en 60641/08, 7 februari 2012, punten 118 en 124.

30 EHRM, *Mosley / Verenigd Koninkrijk*, nr. 48009/08, 10 mei 2011, punten 129 en 130.

naar beperkingen die zouden kunnen neerkomen op een vorm van censuur voorafgaand aan de publicatie. Met betrekking tot het afschrikwekkende effect ("chilling effect") waartoe een vereiste van voorafgaande kennisgeving mogelijk zou kunnen leiden, en gelet op de twijfels over de doeltreffendheid daarvan en de ruime beoordelingsmarge op dat gebied, concludeerde het EHRM echter dat artikel 8 het bestaan van een wettelijk bindende vereiste van voorafgaande kennisgeving niet verplicht stelde. Bijgevolg concludeerde het Hof dat er geen inbreuk op artikel 8 had plaatsgevonden.

Voorbeeld: In *Biriuk / Litouwen*[31] eiste verzoekster schadevergoeding van een lokaal dagblad omdat dit een artikel had gepubliceerd waarin werd gemeld dat zij hiv-positief was. Deze informatie zou zijn bevestigd door de artsen van het lokale ziekenhuis. Het EHRM was van oordeel dat het desbetreffende artikel niet bijdroeg tot een debat van algemeen belang en herhaalde dat de bescherming van persoonsgegevens, en niet in de laatste plaats van medische gegevens, van fundamenteel belang was voor de uitoefening door een persoon van zijn of haar recht op eerbieding van het privé, familie- en gezinsleven als gegarandeerd door artikel 8 van het EVRM. Het Hof hechtte met name belang aan het feit dat, volgens het verslag in het nieuwsblad, medisch personeel van een ziekenhuis informatie had verstrekt over de hiv-infectie van verzoekster, hetgeen duidelijk in strijd was met hun medische beroepsgeheim. Dientengevolge had de staat verzuimd om het recht op eerbiediging van haar privéleven te waarborgen. Het Hof concludeerde dat er een inbreuk op artikel 8 had plaatsgevonden.

1.2.2. Toegang tot documenten

De vrijheid van informatie beschermt volgens artikel 11 van het Handvest en artikel 10 van het EVRM niet alleen het recht om informatie te verstrekken, maar ook het recht om informatie te *ontvangen*. Het belang van transparant overheidshandelen voor de werking van een democratische samenleving wordt in toenemende mate onderkend. Dienovereenkomstig is in de afgelopen twee decennia het recht op toegang tot documenten die bij overheidsinstanties berusten erkend als een belangrijk recht van iedere EU-burger en elke natuurlijke of rechtspersoon die verblijft of zijn statutaire zetel heeft in een lidstaat.

31 EHRM, *Biriuk / Litouwen*, nr. 23373/03, 25 november 2008.

In het RvE-recht kan worden verwezen naar de beginselen die zijn vervat in de Aanbeveling inzake de toegang tot officiële documenten, die als inspiratiebron heeft gediend voor de opstellers van het Verdrag betreffende de toegang tot documenten (*Verdrag 205*).[32] **In het EU-recht** wordt het recht op toegang tot documenten gegarandeerd door Verordening (EG) nr. 1049/2001 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie (*verordening inzake de toegang tot documenten*).[33] Artikel 42 van het Handvest en artikel 15, lid 3, van het VWEU hebben dit recht op toegang uitgebreid "tot documenten van de instellingen, organen en instanties van de Unie, ongeacht de informatiedrager waarop zij zijn vastgelegd". Overeenkomstig artikel 52, lid 2, van het Handvest wordt het recht op toegang tot documenten ook uitgeoefend onder de voorwaarden en binnen de grenzen van artikel 15, lid 3, van het VWEU. Dit recht kan botsen met het recht op gegevensbescherming indien door het geven van inzage in een document persoonsgegevens van anderen bekend zouden worden. Verzoeken om inzage in documenten of informatie die bij overheidsinstanties berusten moeten worden afgewogen tegen het recht op gegevensbescherming van personen van wie in de opgevraagde documenten persoonsgegevens zijn opgenomen.

Voorbeeld: In het arrest *Commissie / Bavarian Lager*[34] heeft het HvJ-EU de reikwijdte van de bescherming van persoonsgegevens gedefinieerd in de context van de toegang tot documenten van EU-instellingen en de verhouding tussen Verordening (EG) nr. 1049/2001 (*verordening inzake de toegang tot documenten*) en Verordening (EG) nr. 45/2001 (*verordening gegevensbescherming*). Bavarian Lager, opgericht in 1992, importeert gebotteld Duits bier in het Verenigd Koninkrijk, voornamelijk voor verkoop in cafés en bars. Daarbij ondervond het bedrijf echter moeilijkheden omdat de Britse autoriteiten nationale producenten de facto een voorkeursbehandeling gaven. In reactie op de klacht van Bavarian Lager besloot de Europese Commissie een procedure in te leiden tegen het Verenigd Koninkrijk wegens niet-nakoming van zijn verplichtingen, wat ertoe leidde dat de betwiste bepalingen werden aangepast en in

32 Raad van Europa, Comité van ministers (2002), Aanbeveling Rec (2002) 2 van het Comité van ministers aan de lidstaten inzake de toegang tot officiële documenten, 21 februari 2002; Raad van Europa, Verdrag betreffende de toegang tot officiële documenten, CETS nr. 205, 18 juni 2009. Het Verdrag is nog niet in werking getreden.

33 Verordening (EG) nr. 1049/2001 van het Europees Parlement en de Raad van 30 mei 2011 inzake de toegang van het publiek tot documenten van het Europees Parlement, de Raad en de Commissie, PB L 145 van 31.5.2001, blz. 43.

34 HvJ-EU, zaak C-28/08 P, *Europese Commissie / The Bavarian Lager Co. Ltd.*, 29 juni 2010, punten 60, 63, 76, 78 en 79.

overeenstemming met het EU-recht werden gebracht. Vervolgens verzocht Bavarian Lager de Commissie, naast andere documenten, om een kopie van de notulen van een vergadering die was bijgewoond door vertegenwoordigers van de Commissie, de Britse autoriteiten en de Confédération des Brasseurs du Marché Commun (CBMC). De Commissie stemde ermee in om bepaalde documenten die verband hielden met de vergadering openbaar te maken, maar maakte vijf namen in de notulen onleesbaar, namelijk van twee personen die uitdrukkelijk bezwaar hadden gemaakt tegen de bekendmaking van hun identiteit en van drie personen die de Commissie niet had weten te bereiken. Bij een besluit van 18 maart 2004 verwierp de Commissie een nieuw verzoek van Bavarian Lager om verkrijging van de volledige notulen van de vergadering, waarbij ze in het bijzonder de bescherming van het privéleven van deze personen als gegarandeerd door de verordening gegevensbescherming aanvoerde. Aangezien Bavarian Lager geen genoegen nam met dit standpunt, maakte de onderneming een procedure aanhangig bij het Gerecht van eerste aanleg, dat het besluit van de Commissie bij arrest van 8 november 2007 (zaak T-194/04, *Bavarian Lager / Commissie*) nietig verklaarde, overwegende met name dat de loutere vermelding van de namen van de personen in kwestie in de lijst van personen die een vergadering hadden bijgewoond namens het orgaan dat ze vertegenwoordigden, geen aantasting van hun privéleven inhield en de privélevens van deze personen niet in gevaar bracht.

Nadat de Commissie hiertegen beroep had ingesteld, vernietigde het HvJ-EU het arrest van het Gerecht van eerste aanleg. Het HvJ-EU oordeelde dat de verordening inzake de toegang tot documenten voorziet in "een specifieke en versterkte regeling van bescherming van personen wier persoonsgegevens, in voorkomend geval, openbaar kunnen worden gemaakt". Volgens het HvJ-EU worden, wanneer een verzoek op grond van de verordening inzake de toegang tot documenten strekt tot het verkrijgen van toegang tot documenten die persoonsgegevens bevatten, de bepalingen van de verordening gegevensbescherming in volle omvang van toepassing. Het HvJ-EU concludeerde dat de Commissie het verzoek om toegang tot de volledige notulen van de vergadering van oktober 1996 terecht had verworpen. Bij het ontbreken van toestemming van de vijf deelnemers aan die vergadering heeft de Commissie zich in voldoende mate aan haar transparantieverplichting gehouden door een versie van het document waarin hun namen onleesbaar waren gemaakt openbaar te maken.

Bovendien stelde het HvJ-EU dat "[a]angezien Bavarian Lager geen enkele uitdrukkelijke en legitieme rechtvaardigingsgrond en evenmin enig overtuigend argument tot staving van de noodzaak van de doorgifte van deze persoonsgegevens heeft aangevoerd, (...) de Commissie de verschillende belangen van de betrokken partijen niet tegen elkaar [heeft] kunnen afwegen. De Commissie heeft evenmin kunnen nagaan of er geen reden bestond om aan te nemen dat door deze doorgifte de rechtmatige belangen van de betrokkenen worden geschaad", zoals vereist door de verordening gegevensbescherming.

Volgens dit arrest is er voor inmenging in het recht op gegevensbescherming in verband met de toegang tot documenten een specifieke en gerechtvaardigde reden nodig. Het recht op toegang tot documenten mag niet automatisch voorrang krijgen boven het recht op gegevensbescherming.[35]

Een specifiek aspect van een verzoek om toegang kwam aan de orde in het hiernavolgende arrest van het EHRM.

Voorbeeld: In de zaak *Társaság a Szabadságjogokért / Hongarije*[36] had de verzoeker, een mensenrechten-ngo, het Hongaarse constitutioneel hof om toegang tot informatie over een nog lopende zaak verzocht. Zonder het parlementslid dat de zaak bij het constitutioneel hof aanhangig had gemaakt te raadplegen, had het hof het verzoek om toegang verworpen op grond van het argument dat bij het hof ingediende klachten alleen met goedkeuring van de klager aan buitenstaanders bekend mochten worden gemaakt. Nationale rechtbanken hadden deze weigering bekrachtigd met het argument dat andere rechtmatige belangen, waaronder de toegankelijkheid van openbare informatie, niet mochten prevaleren boven de bescherming van deze persoonsgegevens. De verzoeker was opgetreden als "maatschappelijke waakhond", van wie de activiteiten soortgelijke bescherming rechtvaardigden als de bescherming die de pers geniet. In verband met de persvrijheid had het EHRM consequent vastgesteld dat het publiek het recht had om informatie van algemeen belang te ontvangen. De informatie waarom de verzoeker had verzocht was

35 Zie echter de gedetailleerde beraadslagingen van de Europese Toezichthouder voor gegevensbescherming (EDPS) (2011) in "Public access to documents containing personal data after the Bavarian Lager ruling", Brussel, 24 maart 2011, beschikbaar op: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 EHRM, *Társaság a Szabadságjogokért / Hongarije*, nr. 37374/05, 14 april 2009; zie de punten 27 en 36-38.

"direct beschikbaar" en vereiste niet de verzameling van gegevens. In dergelijke omstandigheden had de staat een verplichting om de door de verzoeker gewenste informatiestroom niet te verhinderen. Samengevat concludeerde het EHRM dat obstakels die bedoeld zijn om de toegang tot informatie van algemeen belang te belemmeren, personen die in de media of op aanverwante gebieden werkzaam zijn zouden kunnen verhinderen om hun cruciale rol van "openbare waakhond" te vervullen. Het Hof concludeerde dat er een inbreuk op artikel 10 had plaatsgevonden.

In het EU-recht is het belang van transparantie stevig verankerd. Het beginsel van transparantie is vervat in de artikel en 1 en 10 van het VEU en in artikel 15, lid 1, van het VWEU.[37] Volgens overweging 2 van Verordening (EG) nr. 1049/2001 maakt deze transparantie een betere deelneming van de burgers aan het besluitvormingsproces mogelijk en waarborgt ze een grotere legitimiteit en meer doelmatigheid en verantwoordelijkheid van de administratie ten opzichte van de burgers binnen een democratisch systeem.[38]

Deze redenering volgend, vereisen Verordening (EG) nr. 1290/2005 van de Raad betreffende de financiering van het gemeenschappelijk landbouwbeleid en Verordening (EG) nr. 259/2008 van de Commissie tot vaststelling van de uitvoeringsbepalingen daarvan de publicatie van informatie over de begunstigden van bepaalde EU-fondsen in de landbouwsector en de per begunstigde ontvangen bedragen.[39] De publicatie zou moeten bijdragen tot de openbare controle van het doeltreffend gebruik van overheidsgelden door de administratie. De evenredigheid van deze publicatie is door diverse begunstigden bestreden.

37 EU (2012), geconsolideerde versies van het Verdrag betreffende de Europese Unie (VEU) en het Verdrag betreffende de werking van de Europese Unie (VWEU), PB C 326 van 26.10.2012, blz. 13 en blz. 47.

38 HvJ-EU, zaak C-41/00 P, *Interporc Im- und Export GmbH / Commissie van de Europese Gemeenschappen*, 6 maart 2003, punt 39; en HvJ-EU, zaak C-28/08 P, *Europese Commissie / The Bavarian Lager Co. Ltd.*, 29 juni 2010, punt 54.

39 Verordening (EG) nr. 1290/2005 van de Raad van 21 juni 2005 betreffende de financiering van het gemeenschappelijk landbouwbeleid, PB L 209 van 11.8.2005, blz. 1, en Verordening (EG) nr. 259/2008 van de Commissie van 18 maart 2008 tot vaststelling van uitvoeringsbepalingen van Verordening (EG) nr. 1290/2005 van de Raad met betrekking tot de bekendmaking van informatie over de begunstigden van financiële middelen uit het Europees Landbouwgarantiefonds (ELGF) en het Europees Landbouwfonds voor Plattelandsontwikkeling (ELFPO), PB L 76 van 19.3.2008, blz. 28.

Voorbeeld: In *Volker und Markus Schecke en Hartmut Eifert / Land Hessen*[40] moest het HvJ-EU de evenredigheid van de door de EU-wetgeving verplichte publicatie van de namen van de begunstigden van landbouwsubsidies van de EU en de door hen ontvangen bedragen beoordelen.

Het HvJ-EU, dat opmerkte dat het recht op gegevensbescherming niet absoluut is, argumenteerde dat de publicatie op een website van gegevens waarin de begunstigden van twee landbouwsteunfondsen van de EU en de precieze door hen ontvangen bedragen werden genoemd inmenging in hun privéleven in het algemeen en in de bescherming van hun persoonsgegevens in het bijzonder vormde.

Het HvJ-EU stelde dat deze aantasting van de in de artikel en 7 en 8 erkende rechten bij wet was gesteld en beantwoordde aan een door de Unie erkende doelstelling van algemeen belang, namelijk, onder meer, het vergroten van de transparantie wat het gebruik van communautaire middelen betreft. Het HvJ-EU oordeelde echter dat de publicatie van de namen van natuurlijke personen die begunstigden van EU-landbouwsteun uit deze twee fondsen waren en van de precieze door hen ontvangen bedragen een onevenredige maatregel was die gelet op artikel 52, lid 1, van het Handvest niet was gerechtvaardigd. Bijgevolg verklaarde het Hof de EU-wetgeving inzake de publicatie van informatie over de begunstigden van Europese landbouwfondsen deels ongeldig.

1.2.3. Vrijheid van kunsten en wetenschappen

Een ander recht waartegen het recht op eerbiediging van het privéleven en het recht op gegevensbescherming moeten worden afgewogen is het recht van vrijheid van kunsten en wetenschappen, dat uitdrukkelijk wordt beschermd door artikel 13 van het Handvest. Dit recht is hoofdzakelijk afgeleid uit het recht van vrijheid van gedachte en meningsuiting en moet worden uitgeoefend met inachtneming van artikel 1 van het Handvest (menselijke waardigheid). Het EHRM is van oordeel dat de vrijheid van kunsten wordt beschermd krachtens artikel 10 van het EHRM.[41] Ook aan het krachtens artikel 13 van het Handvest gegarandeerde recht kunnen beperkingen worden gesteld op grond van artikel 10 van het EVRM.[42]

40 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert / Land Hessen*, punten 47-52, 58, 66-67, 75, 86 en 92.

41 EHRM, *Müller en anderen / Zwitserland*, nr. 10737/84, 24 mei 1988.

42 Toelichtingen bij het Handvest van de grondrechten, PB C 303 van 14.12.2007, blz. 17.

Voorbeeld: In *Vereinigung bildender Künstler / Oostenrijk*[43] hadden de Oostenrijkse rechtbanken de verzoekende vereniging verboden om een schilderij tentoon te stellen dat foto's bevatte van de hoofden van verschillende publieke figuren in seksuele posities. Een Oostenrijkse parlementariër, van wie een foto was gebruikt in het schilderij, maakte een procedure aanhangig tegen de verzoekende vereniging waarin hij om een verbod op de tentoonstelling van het schilderij vroeg. De nationale rechtbank honoreerde zijn verzoek en vaardigde een verbod uit. Het EHRM herhaalde dat artikel 10 van het EVRM van toepassing is op de communicatie van ideeën die de staat of een deel van de bevolking beledigen, schokken of verontrusten. Personen die kunstwerken creëren, uitvoeren, verspreiden of tentoonstellen dragen bij tot de uitwisseling van ideeën en opinies en de staat heeft de verplichting om hun vrijheid van meningsuiting niet te veel aan te tasten. Aangezien het schilderij een collage was waarin alleen gebruik werd gemaakt van foto's van de hoofden van personen, terwijl hun lichamen op onrealistische en overdreven wijze waren geschilderd, waarmee duidelijk niet werd beoogd de werkelijkheid weer te geven of zelfs maar te suggereren, bepaalde het EHRM voorts dat "het schilderij moeilijk kan worden gezien als een weergave van details van het privéleven [van de afgebeelde persoon], maar betrekking heeft op zijn publieke statuur als politicus" en dat de afgebeelde persoon "in deze hoedanigheid een grotere tolerantie tegenover kritiek tentoon dient te spreiden". Na een afweging van de verschillende belangen die in het geding waren oordeelde het EHRM dat het onbegrensde verbod op de verdere tentoonstelling van het schilderij onevenredig was. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 10 van het EVRM.

Met betrekking tot wetenschap is in de Europese gegevensbeschermingswetgeving bewust rekening gehouden met de bijzondere waarde van wetenschap voor de samenleving. Daarom zijn de algemene restricties betreffende het gebruik van persoonsgegevens ingeperkt. De richtlijn gegevensbescherming en Verdrag 108 staan beide toe dat gegevens worden bewaard voor wetenschappelijke doeleinden zodra ze niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld. Voorts moet het verdere gebruik van persoonsgegevens voor wetenschappelijk onderzoek niet als een onverenigbaar doel worden beschouwd. In het nationale recht moeten meer gedetailleerde bepalingen worden ontwikkeld, met inbegrip van de noodzakelijke waarborgen, om het belang van wetenschappelijk onderzoek te verzoenen met het recht op gegevensbescherming (zie ook de paragrafen 3.3.3 en 8.4).

43 EHRM, *Vereinigung bildender Künstler / Oostenrijk*, nr. 68345/01, 25 januari 2007; zie met name de punten 26 en 34.

1.2.4. Bescherming van eigendom

Het recht op bescherming van eigendom is vervat in artikel 1 van Protocol nr. 1 bij het EVRM en ook in artikel 17, lid 1, van het Handvest. Een belangrijk aspect van het eigendomrecht is de bescherming van intellectuele eigendom, die uitdrukkelijk wordt genoemd in artikel 17, lid 2, van het Handvest. De rechtsorde van de EU omvat diverse richtlijnen die een doeltreffende bescherming van intellectuele eigendom beogen, en met name van het auteursrecht. Intellectuele eigendom omvat niet alleen literaire en artistieke eigendom, maar ook octrooi-, merken- en aanverwante rechten.

Zoals de jurisprudentie van het HvJ-EU duidelijk heeft gemaakt, moet de bescherming van het grondrecht van eigendom worden afgewogen tegen de bescherming van andere grondrechten, in het bijzonder tegen het recht op gegevensbescherming.[44] Er zijn zaken geweest waarin organisaties die het auteursrecht beschermen hebben geëist dat internetaanbieders de identiteit van gebruikers van platforms waarop bestanden worden gedeeld openbaar zouden maken. Dergelijke platforms maken het voor internetgebruikers vaak mogelijk om gratis muziek te downloaden, ook al berust er op deze werken auteursrecht.

Voorbeeld: De zaak *Promusicae / Telefónica de España*[45] had betrekking op de weigering van een Spaanse internetaanbieder, Telefónica, om Promusicae, een organisatie zonder winstoogmerk van muziekproducenten en uitgevers van muziek- en audiovisuele opnamen, de persoonsgegevens te verstrekken van bepaalde personen aan wie Telefónica internettoegangsdiensten leverde. Promusicae verzocht om bekendmaking van de informatie teneinde civiele procedures te kunnen aanspannen tegen deze personen, die volgens Promusicae gebruikmaakten van een programma voor de uitwisseling van bestanden dat toegang bood tot muzieknummers waarvan de exploitatierechten toebehoorden aan leden van Promusicae.

De Spaanse rechter had de zaak verwezen naar het HvJ-EU met de vraag of deze persoonsgegevens krachtens het communautaire recht, in het kader van een civiele procedure, moesten worden meegedeeld om een doeltreffende bescherming van het auteursrecht te verzekeren. Daarbij verwees

44 EHRM, *Ashby Donald en anderen / Frankrijk*, nr. 36769/08, 10 januari 2013.

45 HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, 29 januari 2008, punten 54 en 60.

de verwijzende rechter naar de Richtlijnen 2000/31/EG, 2001/29/EG en 2004/48/EG, mede gelezen in het licht van de artikel en 17 en 47 van het Handvest. Het HvJ-EU concludeerde dat deze drie richtlijnen, evenals de e-privacyrichtlijn (Richtlijn 2002/58/EG), de lidstaten niet beletten om een verplichting opleggen om in het kader van een civiele procedure persoonsgegevens mee te delen teneinde een doeltreffende bescherming van het auteursrecht te verzekeren.

Het HvJ-EU wees erop dat de zaak derhalve de vraag opwierp hoe de vereisten van de bescherming van verschillende grondrechten met elkaar moesten worden verzoend, namelijk het recht op eerbiediging van het privéleven, het recht op bescherming van eigendom en het recht op een doeltreffende voorziening in rechte.

Het Hof concludeerde dat "[b]ij de omzetting van bovengenoemde richtlijnen (...) de lidstaten niettemin erop [moeten] toezien dat zij zich baseren op een uitlegging daarvan die het mogelijk maakt een juist evenwicht tussen de verschillende door de communautaire rechtsorde beschermde grondrechten te verzekeren. Bij de tenuitvoerlegging van de maatregelen ter omzetting van deze richtlijnen moeten de autoriteiten en de rechterlijke instanties van de lidstaten vervolgens niet alleen hun nationale recht conform deze richtlijnen uitleggen, maar er ook op toezien dat zij zich niet baseren op een uitlegging van deze richtlijnen die in conflict zou komen met deze grondrechten of de andere algemene beginselen van gemeenschapsrecht, zoals het evenredigheidsbeginsel."[46]

46 *Ibid.*, punten 65 en 68; zie ook HvJ-EU, zaak C-360/10, *SABAM / Netlog N.V.*, 16 februari 2012.

2

Gegevensbeschermingsterminologie

EU	Behandelde onderwerpen	RvE
Persoonsgegevens		
Richtlijn gegevensbescherming, artikel 2, onder a) HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR) en Hartmut Eifert / Land Hessen*, 9 november 2010 HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, 29 januari 2008	**Wettelijke definitie**	Verdrag 108, artikel 2, onder a) EHRM, *Bernh Larsen Holding AS en anderen / Noorwegen*, nr. 24117/08, 14 maart 2013
Richtlijn gegevensbescherming, artikel 8, lid 1 HvJ-EU, zaak C-101/01, *Bodil Lindqvist*, 6 november 2003	**Bijzondere categorieën persoonsgegevens (gevoelige gegevens)**	Verdrag 108, artikel 6
Richtlijn gegevensbescherming, artikel 6, lid 1, onder e)	**Geanonimiseerde en gepseudonimiseerde gegevens**	Verdrag 108, artikel 5, onder e) Verdrag 108, memorie van toelichting, artikel 42
Verwerking van gegevens		
Richtlijn gegevensbescherming, artikel 2, onder b) HvJ-EU, zaak C-101/01, *Bodil Lindqvist*, 6 november 2003	**Definities**	Verdrag 108, artikel 2, onder c)

EU	Behandelde onderwerpen	RvE
Gebruikers van gegevens		
Richtlijn gegevensbescherming, artikel 2, onder d)	**Voor de verwerking verantwoordelijke**	Verdrag 108, artikel 2, onder d) Aanbeveling inzake profilering, artikel 1, onder g) *
Richtlijn gegevensbescherming, artikel 2, onder e) HvJ-EU, zaak C-101/01, *Bodil Lindqvist*, 6 november 2003	**Verwerker**	Aanbeveling inzake profilering, artikel 1, onder h)
Richtlijn gegevensbescherming, artikel 2, onder g)	**Ontvanger**	Verdrag 108, Aanvullend Protocol, artikel 2, lid 1
Richtlijn gegevensbescherming, artikel 2, onder f)	**Derde**	
Toestemming		
Richtlijn gegevensbescherming, artikel 2, onder h) HvJ-EU, zaak C-543/09, *Deutsche Telekom AG / Bondsrepubliek Duitsland,* 5 mei 2011	**Definitie en vereisten voor geldige toestemming**	Aanbeveling inzake medische gegevens, artikel 6, en verschillende daaropvolgende aanbevelingen

*Noot: *Raad van Europa, Comité van ministers (2010), Aanbeveling Rec (2010)13 aan de lidstaten inzake de bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens in de context van profilering* **(aanbeveling inzake profilering),** *23 november 2010.*

2.1. Persoonsgegevens

Belangrijkste punten

- Gegevens zijn persoonsgegevens indien ze betrekking hebben op een geïdentificeerde of althans identificeerbare persoon, de betrokkene.
- Een persoon is identificeerbaar indien er zonder onredelijke inspanning aanvullende informatie kan worden verkregen die de identificatie van de betrokkene mogelijk maakt.
- Onder authenticatie wordt verstaan: bewijzen dat een bepaalde persoon een bepaalde identiteit heeft en/of is gemachtigd om bepaalde activiteiten te verrichten.

- Er zijn bijzondere categorieën gegevens, de zogeheten gevoelige gegevens, die worden genoemd in Verdrag 108 en in de richtlijn gegevensbescherming, die een betere bescherming vereisen en daarom onder een speciale wettelijke regeling vallen.
- Gegevens zijn geanonimiseerd als ze niet langer identificatiemiddelen bevatten; ze zijn gepseudonimiseerd als de identificatiemiddelen worden vervangen door kunstmatige identificatiemiddelen (pseudoniemen).
- In tegenstelling tot geanonimiseerde gegevens zijn gepseudonimiseerde gegevens persoonsgegevens.

2.1.1. Belangrijkste aspecten van het begrip persoonsgegevens

Zowel **in het EU-recht** als in het **RvE-recht** wordt het begrip "persoonsgegevens" gedefinieerd als informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon,[47] d.w.z. informatie over een persoon van wie de identiteit ofwel volkomen duidelijk is, ofwel kan worden vastgesteld door aanvullende informatie te verkrijgen.

Als gegevens over een dergelijke persoon worden verwerkt, wordt die persoon "de betrokkene" genoemd.

Een persoon

Het recht op gegevensbescherming is voortgekomen uit het recht op eerbiediging van het privéleven. Het begrip privéleven heeft betrekking op mensen. Natuurlijke personen zijn derhalve de primaire begunstigden van gegevensbescherming. Volgens het advies van de Groep gegevensbescherming artikel 29 beschermt de Europese gegevensbeschermingswetgeving voorts uitsluitend *levende* personen.[48]

De jurisprudentie van het EHRM over artikel 8 van het EVRM laat zien dat het moeilijk kan zijn om privé- en beroepsleven volledig van elkaar te scheiden.[49]

47 Richtlijn gegevensbescherming, artikel 2, onder a); Verdrag 108, artikel 2, onder a).

48 Groep gegevensbescherming artikel 29 (2007), Advies 4/2007 over het begrip persoonsgegeven, WP 136, 20 juni 2007, blz. 22.

49 Zie bijvoorbeeld EHRM, *Rotaru / Roemenië* [GC], nr. 28341/95, 4 mei 2000, punt 43; EHRM, *Niemietz / Duitsland*, nr. 13710/88, 16 december 1992, punt 29.

Voorbeeld: In de zaak *Amann / Zwitserland*[50] hadden autoriteiten een zakelijk telefoontje naar de verzoeker onderschept. Op basis van dat telefoongesprek waren de autoriteiten een onderzoek naar de verzoeker gestart en hadden ze een kaart over de verzoeker ingevuld voor de nationale veiligheidskaartenindex. Hoewel de onderschepping een zakelijk telefoongesprek betrof, oordeelde het EHRM dat de opslag van gegevens over dit gesprek betrekking had op het privéleven van de verzoeker. Het EHRM wees erop dat de term "privéleven" niet restrictief moest worden uitgelegd, met name omdat eerbiediging van het privéleven het recht om relaties met andere mensen aan te gaan en te ontwikkelen omvat. Voorts was er geen principiële reden om de uitsluiting van activiteiten van beroeps- of zakelijke aard van het begrip "privéleven" te rechtvaardigen. Deze brede interpretatie komt overeen met die van Verdrag 108. Voorts oordeelde het EHRM dat de inmenging in de zaak van de verzoeker niet conform de wet was geweest omdat de nationale wetgeving geen specifieke en gedetailleerde bepalingen over het verzamelen, registreren en opslaan van informatie bevatte. Het Hof concludeerde daarom dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Bovendien lijkt het, als aspecten van het beroepsleven ook voor gegevensbescherming in aanmerking komen, twijfelachtig of alleen aan natuurlijke personen bescherming moet worden geboden. Rechten uit hoofde van het EVRM zijn niet alleen gegarandeerd voor natuurlijke personen, maar voor iedereen.

Er bestaat jurisprudentie van het EHRM waarin het Hof een oordeel heeft gegeven over verzoeken van rechtspersonen die schending van hun recht op bescherming tegen het gebruik van hun gegevens krachtens artikel 8 van het EVRM aanvoeren. Het Hof heeft deze kwestie echter onderzocht op grond van het recht op eerbiediging van de woning en de correspondentie in plaats van op grond van het recht op eerbiediging van het privéleven:

Voorbeeld: Het arrest *Bernh Larsen Holding AS en anderen / Noorwegen*[51] had betrekking op een klacht van drie Noorse ondernemingen over een besluit van een belastingautoriteit dat hen verplichtte om de belastinginspecteurs een kopie te verstrekken van alle gegevens op een door alle drie de ondernemingen gebruikte computerserver.

50 EHRM, *Amann / Zwitserland* [GC], nr. 27798/95, 16 februari 2000, punt 65.

51 EHRM, *Bernh Larsen Holding AS en anderen / Noorwegen*, nr. 24117/08, 14 maart 2013. Zie echter ook EHRM, *Liberty en anderen / het Verenigd Koninkrijk*, nr. 58243/00, 1 oktober 2008.

Het EHRM oordeelde dat een dergelijke verplichting voor de verzoekende ondernemingen inmenging in hun rechten op eerbiediging van de "woning" en de "correspondentie" als bedoeld in artikel 8 van het EVRM vormde. Het Hof oordeelde echter ook dat de belastingautoriteiten doeltreffende en toereikende waarborgen tegen misbruik hadden toegepast: de verzoekende ondernemingen waren ruim van tevoren geïnformeerd, waren aanwezig bij de interventie ter plaatse en konden tijdens de interventie opmerkingen maken, en het materiaal zou worden vernietigd zodra de belastingcontrole was voltooid. In dergelijke omstandigheden was een redelijk evenwicht bereikt tussen het recht van de verzoekende ondernemingen op eerbiediging van de "woning" en de "correspondentie" en hun belang om de privacy van personen die voor hen werkten te beschermen, enerzijds, en het algemeen belang van een efficiënte inspectie voor belastingcontroledoeleinden anderzijds. Het Hof concludeerde dat er geen inbreuk op artikel 8 had plaatsgevonden.

Volgens **Verdrag 108** heeft gegevensbescherming in de eerste plaats betrekking op de bescherming van natuurlijke personen; de verdragspartijen kunnen de gegevensbescherming krachtens hun nationale recht niettemin uitbreiden tot rechtspersonen, zoals ondernemingen en verenigingen. De **EU-gegevensbeschermingswetgeving** bestrijkt in algemene zin niet de bescherming van rechtspersonen in verband met de verwerking van gegevens die op hen betrekking hebben. De nationale regelgevingsinstanties zijn vrij om dit gebied te reguleren.[52]

Voorbeeld: In *Volker und Markus Schecke en Hartmut Eifert / Land Hessen*[53] oordeelde het HvJ-EU, met betrekking tot de publicatie van persoonsgegevens van begunstigden van landbouwsteun, dat "rechtspersonen ter zake van een dergelijke vermelding evenwel slechts beroep [kunnen] doen op de door de artikel en 7 en 8 van het Handvest geboden bescherming voor zover uit de officiële naam van de rechtspersoon de identiteit van een of meer natuurlijke personen blijkt. [...D]e eerbiediging van het in de artikel en 7 en 8 van het Handvest erkende recht op persoonlijke levenssfeer bij de verwerking van persoonsgegevens betreft elke informatie aangaande een geïdentificeerde of identificeerbare natuurlijke persoon (...)".[54]

52 Richtlijn gegevensbescherming, overweging 24.

53 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert / Land Hessen*, 9 november 2010, punt 53.

54 *Ibid.*, punt 52.

Identificeerbaarheid van een persoon

Zowel krachtens **het EU-recht** als krachtens **het RvE-recht** bevat informatie gegevens over een persoon indien:

- in deze informatie een natuurlijke persoon wordt geïdentificeerd; of
- een natuurlijke persoon, hoewel niet geïdentificeerd, in deze informatie wordt beschreven op een wijze die het mogelijk maakt om vast te stellen wie de betrokkene is door verder onderzoek te doen.

Deze beide typen informatie worden in de Europese gegevensbeschermingswetgeving op dezelfde wijze beschermd. Het EHRM heeft herhaaldelijk opgemerkt dat het begrip "persoonsgegevens" als bedoeld in het EVRM identiek is aan dit begrip als bedoeld in Verdrag 108, met name wat betreft de voorwaarde dat de informatie betrekking moet hebben op geïdentificeerde of identificeerbare personen.[55]

De wettelijke definities van het begrip "persoonsgegevens" maken verder niet duidelijk wanneer een persoon als geïdentificeerd wordt beschouwd.[56] Het is evident dat voor identificatie elementen nodig zijn die een persoon op zodanige wijze beschrijven dat hij of zij kan worden onderscheiden van alle andere personen en herkenbaar is als individu. Een uitstekend voorbeeld van deze beschrijvende elementen is de naam van een persoon. In uitzonderlijke gevallen kunnen andere identificatiemiddelen hetzelfde effect hebben als een naam. Zo kan voor publieke figuren de functie van de persoon (bv. voorzitter van de Europese Commissie) voldoende zijn om deze persoon te identificeren.

> Voorbeeld: In de zaak *Promusicae*[57] stelde het HvJ-EU dat "niet [wordt] betwist dat de door Promusicae gevorderde mededeling van de naam en het adres van bepaalde gebruikers van [naam van het internetplatform voor het delen van bestanden] impliceert dat persoonsgegevens ter beschikking worden gesteld, dat wil zeggen – volgens de definitie van artikel 2, sub a, van richtlijn 95/46 – informatie betreffende geïdentificeerde of identificeerbare natuurlijke personen

55 EHRM, *Amann / Zwitserland* [GC], nr. 27798/95, 16 februari 2000, punt 65 *et al.*

56 Zie ook EHRM, *Odièvre / Frankrijk* [GC], nr. 42326/98, 13 februari 2003, en EHRM, *Godelli / Italië*, nr. 33783/09, 25 september 2012.

57 HvJ-EU, zaak C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, 29 januari 2008, punt 45.

(...). Deze verstrekking van informatie die volgens Promusicae door Telefónica wordt opgeslagen – wat deze laatste niet betwist – vormt een verwerking van persoonsgegevens in de zin van artikel 2, eerste alinea, van richtlijn 2002/58, gelezen in samenhang met artikel 2, sub b, van richtlijn 95/46".

Omdat veel namen niet uniek zijn, kunnen voor de identificatie van een persoon aanvullende identificatiemiddelen nodig zijn om ervoor te zorgen dat een persoon niet wordt verward met iemand anders. Vaak worden daarvoor de geboortedatum en -plaats gebruikt. Daarnaast zijn in enkele landen gepersonaliseerde nummers ingevoerd om beter onderscheid tussen burgers te kunnen maken. Biometrische gegevens, zoals vingerafdrukken, digitale foto's of irisscans, worden in het technologische tijdperk steeds belangrijker om personen te identificeren.

Voor de toepasbaarheid van de Europese gegevensbeschermingswetgeving is identificatie van de betrokkene op een kwalitatief hoog niveau evenwel niet noodzakelijk; het is voldoende dat de desbetreffende persoon identificeerbaar is. Een persoon wordt identificeerbaar geacht als informatie identificatie-elementen bevat aan de hand waarvan de persoon direct of indirect kan worden geïdentificeerd.[58] Volgens overweging 26 van de richtlijn gegevensbescherming bestaat de maatstaf hierin of alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs kunnen worden ingezet om genoemde persoon te identificeren, beschikbaar zijn voor en zullen worden gebruikt door de voorziene gebruikers van de informatie; hieronder vallen ook derde ontvangers (zie paragraaf 2.3.2).

Voorbeeld: Een lokale autoriteit besluit om gegevens te verzamelen over auto's die te snel rijden in lokale straten. De auto's worden gefotografeerd, waarbij automatisch de tijd en de locatie worden geregistreerd, om de gegevens vervolgens door te geven aan de bevoegde autoriteit, zodat deze boetes kan opleggen aan de snelheidsovertreders. Een betrokkene dient een klacht in en voert daarin aan dat de lokale autoriteit krachtens de gegevensbeschermingswetgeving niet beschikt over een rechtsgrondslag voor deze gegevensverzameling. De lokale autoriteit stelt dat zij geen persoonsgegevens verzamelt. Volgens de lokale autoriteit zijn kentekens van auto's gegevens over anonieme personen. De lokale autoriteit is wettelijk niet bevoegd om het voertuigenregister in te zien om achter de identiteit van de eigenaar of bestuurder van de auto te komen.

58 Richtlijn gegevensbescherming, artikel 2, onder a).

Deze redenering is niet in overeenstemming met overweging 26 van de richtlijn gegevensbescherming. Aangezien het doel van de gegevensbescherming duidelijk is om snelheidsovertreders te identificeren en te beboeten, kan worden voorzien dat een poging tot identificatie zal worden gedaan. Hoewel de lokale autoriteiten niet beschikken over directe identificatiemiddelen, zullen zij de gegevens overdragen aan de bevoegde autoriteit, de politie, die die middelen wel heeft. Overweging 26 omvat uitdrukkelijk een scenario waarin kan worden voorzien dat een latere ontvanger van de gegevens, die niet de onmiddellijke gebruiker is, kan proberen de persoon te identificeren. In het licht van overweging 26 staat het handelen van de lokale autoriteit gelijk aan het verzamelen van gegevens over identificeerbare personen en is er daarom een rechtsgrondslag krachtens de gegevensbeschermingswetgeving nodig.

In het **RvE-recht** wordt het begrip identificeerbaarheid op soortgelijke wijze begrepen. Zo wordt in artikel 1, lid 2, van de Aanbeveling inzake betalingsgegevens[59] bepaald dat een persoon niet "identificeerbaar" wordt geacht als identificatie een onredelijke hoeveelheid tijd, geld of mankracht kost.

Authenticatie

Authenticatie is een procedure die een persoon in staat stelt te bewijzen dat hij of zij een bepaalde identiteit heeft en/of gemachtigd is om bepaalde handelingen te verrichten, zoals een beveiligd gebied betreden of geld van een bankrekening opnemen. Authenticatie kan worden gerealiseerd door het vergelijken van biometrische gegevens, zoals een foto of vingerafdrukken in een paspoort, met de gegevens die de persoon zelf presenteert, bijvoorbeeld bij een immigratiecontrole, of door informatie op te vragen die alleen bekend zou moeten zijn bij de persoon met een bepaalde identiteit of machtiging, zoals een persoonlijk identificatienummer (PIN) of een wachtwoord, of door te vereisen dat de persoon een bepaald "token" presenteert dat exclusief in het bezit is van de persoon met een bepaalde identiteit of machtiging, zoals een speciale chipkaart of de sleutel van een bankkluis. Naast wachtwoorden en chipkaarten, soms in combinatie met PIN's, vormen elektronische handtekeningen een bijzonder geschikt instrument om een persoon in een elektronische communicatieomgeving te identificeren en te authentiseren.

59 RvE, Comité van ministers (1990), Aanbeveling nr. R (90) 19 inzake de bescherming van persoonsgegevens die worden gebruikt voor betalingen en aanverwante activiteiten, 13 september 1990.

Aard van de gegevens

Elk type informatie kan persoonsgegevens omvatten, mits de informatie betrekking heeft op een persoon.

Voorbeeld: Een beoordeling van het functioneren van een werknemer door een leidinggevende, opgeslagen in het personeelsdossier van de werknemer, is een persoonsgegeven over de werknemer, ook al geeft deze beoordeling mogelijk slechts – geheel of gedeeltelijk – de persoonlijke mening van de leidinggevende weer, zoals: "de werknemer is niet toegewijd aan zijn werk", en betreft het geen weergave van harde feiten, zoals: "de werknemer is in de afgelopen zes maanden gedurende vijf weken niet op zijn/haar werk aanwezig geweest".

Het begrip "persoonsgegevens" heeft betrekking op informatie die behoort tot het privéleven van een persoon en op informatie over zijn of haar beroeps- of openbare leven.

In de zaak *Amann*[60] heeft het EHRM het begrip persoonsgegevens zodanig uitgelegd dat het zich niet strikt beperkt tot de persoonlijke levenssfeer van een natuurlijke persoon (zie paragraaf 2.1.1). Deze betekenis van het begrip persoonsgegevens is ook relevant voor de richtlijn gegevensbescherming.

Voorbeeld: In *Volker und Markus Schecke en Hartmut Eifert / Land Hessen*[61] heeft het HvJ-EU bepaald dat het "irrelevant [is] dat de bekendgemaakte gegevens verband houden met beroepsactiviteiten (...). Het Europees Hof voor de Rechten van de Mens heeft in dat verband betreffende de interpretatie van artikel 8 EVRM geoordeeld dat de term 'persoonlijke levenssfeer' niet eng moet worden uitgelegd en dat om geen enkele principiële reden de beroepsactiviteiten (...) van het begrip 'persoonlijke levenssfeer' kunnen worden uitgesloten."

Gegevens hebben ook betrekking op een persoon als de inhoud van de informatie indirect gegevens over die persoon onthult. In bepaalde gevallen, wanneer er een nauw verband bestaat tussen een voorwerp of een gebeurtenis – bv. een mobiele telefoon, een auto, een ongeval – enerzijds, en een persoon – bv. de eigenaar, de

60 EHRM, *Amann / Zwitserland* [GC], nr. 27798/95, 16 februari 2000, punt 65.

61 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert / Land Hessen*, 9 november 2010, punt 59.

gebruiker, het slachtoffer – anderzijds, zou ook informatie over een voorwerp of over een gebeurtenis als een persoonsgegeven moeten worden beschouwd.

Voorbeeld: In *Uzun / Duitsland*[62] waren de verzoeker en een andere man onder surveillance geplaatst via een in de auto van de andere man geplaatst gps-apparaat omdat ze werden verdacht van betrokkenheid bij bomaanslagen. In dit geval oordeelde het EHRM dat de observatie van de verzoeker via gps neerkwam op inmenging in zijn privéleven als beschermd door artikel 8 van het EVRM. De surveillance via gps was echter conform de wet en was ook evenredig aan het rechtmatige doel om verschillende gevallen van poging tot moord te onderzoeken en derhalve noodzakelijk in een democratische samenleving. Het Hof concludeerde dat er geen sprake was geweest van een inbreuk op artikel 8 van het EVRM.

Verschijningsvorm van de gegevens

De vorm waarin de persoonsgegevens worden opgeslagen of gebruikt is niet relevant voor de toepasbaarheid van de gegevensbeschermingswetgeving. Schriftelijke of mondelinge mededelingen kunnen persoonsgegevens bevatten, evenals afbeeldingen,[63] met inbegrip van beeldmateriaal van gesloten televisiecircuits[64] of geluid(en).[65] Elektronisch vastgelegde informatie, evenals informatie op papier, kan persoonsgegevens bevatten; zelfs celmonsters van menselijk weefsel kunnen persoonsgegevens zijn, aangezien ze het DNA van een persoon vastleggen.

2.1.2. Bijzondere categorieën persoonsgegevens

Zowel **in het EU-recht** als **in het RvE-recht** zijn er bijzondere categorieën persoonsgegevens die, gezien hun aard, een risico voor de betrokkene kunnen vormen wanneer ze worden verwerkt en die daarom beter moeten worden beschermd. De verwerking van deze bijzondere categorieën persoonsgegevens ("gevoelige

62 EHRM, *Uzun / Duitsland*, nr. 35623/05, 2 september 2010.

63 EHRM, *Von Hannover / Duitsland*, nr. 59320/00, 24 juni 2004; EHRM, *Sciacca / Italië*, nr. 50774/99, 11 januari 2005.

64 EHRM, *Peck / het Verenigd Koninkrijk*, nr. 44647/98, 28 januari 2003; EHRM, *Köpke / Duitsland*, nr. 420/07, 5 oktober 2010.

65 Richtlijn gegevensbescherming, overwegingen 16 en 17; EHRM, *P.G. en J.H. / het Verenigd Koninkrijk*, nr. 44787/98, 25 september 2001, punten 59 en 60; EHRM, *Wisse / Frankrijk*, nr. 71611/01, 20 december 2005.

gegevens") mag daarom alleen worden toegestaan indien er specifieke waarborgen aanwezig zijn.

Wat betreft de definitie van gevoelige gegevens worden zowel in Verdrag 108 (artikel 6) als in de richtlijn gegevensbescherming (artikel 8) de volgende categorieën genoemd:

- persoonsgegevens waaruit de raciale of etnische afkomst blijkt;
- persoonsgegevens waaruit de politieke, godsdienstige of een andere overtuiging blijkt;
- persoonsgegevens die betrekking hebben op de gezondheid of het seksuele leven.

> Voorbeeld: In de zaak *Bodil Lindqvist*[66] bepaalde het HvJ-EU het volgende: "De vermelding van het feit dat iemand zijn voet heeft bezeerd en met gedeeltelijk ziekteverlof is, is een persoonsgegeven betreffende de gezondheid in de zin van artikel 8, lid 1, van richtlijn 95/46".

In de richtlijn gegevensbescherming wordt voorts "het lidmaatschap van een vakvereniging" genoemd als gevoelig gegeven, omdat deze informatie een belangrijke indicator van politieke overtuiging of kleur is.

In Verdrag 108 worden ook persoonsgegevens over strafrechtelijke veroordelingen als gevoelig aangemerkt.

Artikel 8, lid 7, van de richtlijn gegevensbescherming verplicht de lidstaten om "de voorwaarden vast [te stellen] waaronder een nationaal identificatienummer of enig ander identificatiemiddel van algemene aard voor verwerkingsdoeleinden mag worden gebruikt".

66 HvJ-EU, zaak C-101/01, *Bodil Lindqvist*, 6 november 2003, punt 51.

2.1.3. Geanonimiseerde en gepseudonimiseerde gegevens

Volgens het beginsel van beperkte bewaring van gegevens, dat is vervat in zowel de richtlijn gegevensbescherming als Verdrag 108 (en dat nader zal worden besproken in hoofdstuk 3), mogen gegevens "in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer (...) worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, noodzakelijk is"[67] Dientengevolge moeten gegevens worden geanonimiseerd indien de voor de verwerking verantwoordelijke ze wil opslaan nadat ze niet langer geldig zijn of niet langer dienen voor het doeleinde waarvoor ze oorspronkelijk zijn opgeslagen.

Geanonimiseerde gegevens

Gegevens zijn geanonimiseerd indien alle identificerende elementen zijn verwijderd uit een geheel van persoonsgegevens. De informatie mag geen enkel element meer bevatten dat, door redelijke inspanningen te verrichten, kan dienen om de betrokken perso(o)n(en) opnieuw te identificeren.[68] Wanneer gegevens met succes zijn geanonimiseerd, vormen ze niet langer persoonsgegevens.

Als persoonsgegevens niet langer dienen voor de verwezenlijking van het oorspronkelijke doeleinde waarvoor ze zijn verzameld, maar worden bewaard in identificeerbare vorm voor historische, statistische of wetenschappelijke doeleinden, staan de richtlijn gegevensbescherming en Verdrag 108 dit toe op voorwaarde dat is voorzien in passende waarborgen tegen misbruik.[69]

Gepseudonimiseerde gegevens

Persoonsgegevens bevatten identificatiemiddelen, zoals een naam, geboortedatum, geslacht of adres. Wanneer persoonsgegevens worden gepseudonimiseerd, worden de identificatiemiddelen vervangen door kunstmatige identificatiemiddelen (pseudoniemen). Pseudonimisering wordt bijvoorbeeld bereikt door versleuteling van de identificatiemiddelen in persoonsgegevens.

67 Richtlijn gegevensbescherming, artikel 6, lid 1, onder e), en Verdrag 108, artikel 5, onder e).

68 *Ibid.*, overweging 26.

69 Richtlijn gegevensbescherming, artikel 6, lid 1, onder e), en Verdrag 108, artikel 5, onder e).

Gepseudonimiseerde gegevens worden niet uitdrukkelijk genoemd in de wettelijke definities van zowel Verdrag 108 als de richtlijn gegevensbescherming. In de memorie van toelichting bij Verdrag 108 wordt in artikel 42 echter bepaald dat "[d]e vereiste (...) ten aanzien van de termijnen voor de opslag van gegevens in hun aan een naam gekoppelde vorm [niet] betekent (...) dat gegevens na enige tijd onherroepelijk moeten worden gescheiden van de naam van de persoon waarop ze betrekking hebben, maar alleen dat het niet mogelijk mag zijn om de gegevens en de identificatiemiddelen gemakkelijk aan elkaar te koppelen". Dit effect kan worden bereikt door de gegevens te pseudonimiseren, waarbij identificatiemiddelen vervangen worden door kunstmatige identificatiemiddelen. Één methode van pseudonymisering is het versleutelen van identificatiemiddelen. Voor iedereen die niet in het bezit van de decryptiesleutel is, zijn gepseudonimiseerde gegevens moeilijk identificeerbaar. De connectie met een identiteit bestaat nog wel, in de vorm van het pseudoniem en de decryptiesleutel. Voor personen die in het bezit zijn van de decryptiesleutel is nieuwe identificatie eenvoudig. Met name moet worden voorkomen dat onbevoegde personen decryptiesleutels gebruiken.

Omdat pseudonimisering van gegevens een van de belangrijkste middelen is om gegevensbescherming op grote schaal te verwezenlijken indien het niet mogelijk is om volledig af te zien van het gebruik van persoonsgegevens, moeten de logica en het effect van een dergelijke handeling nader worden toegelicht.

Voorbeeld: De zin "Charles Spencer, geboren op 3 april 1967, is de vader van een gezin met vier kinderen, twee jongens en twee meisjes" kan bijvoorbeeld op de volgende manier worden gepseudonimiseerd:

"C.S. 1967 is de vader van een gezin met vier kinderen, twee jongens en twee meisjes"; of

"324 is de vader van een gezin met vier kinderen, twee jongens en twee meisjes"; of

"YESz320l is de vader van een gezin met vier kinderen, twee jongens en twee meisjes".

Gebruikers die toegang tot deze gepseudonimiseerde gegevens hebben, zullen "Charles Spencer, geboren op 3 april 1967" doorgaans niet kunnen identificeren

uit "324" of "YESz3201". Gepseudonimiseerde gegevens zijn daarom veelal beter beveiligd tegen misbruik.

Het eerste voorbeeld is echter minder veilig. Wanneer de zin "C.S. 1967 is de vader van een gezin met vier kinderen, twee jongens en twee meisjes" wordt gebruikt in het kleine dorp waar Charles Spencer woont, is de heer Spencer mogelijk eenvoudig herkenbaar. De methode die wordt gebruikt voor de pseudonimisering is van invloed op de effectiviteit van de gegevensbescherming.

Persoonsgegevens met versleutelde identificatiemiddelen worden in veel gevallen gebruikt als een middel om de identiteit van personen geheim te houden. Dit is met name nuttig als voor de verwerking verantwoordelijken moeten zorgen dat ze met dezelfde betrokkenen te maken hebben, maar de echte identiteit van de betrokkenen niet nodig hebben of niet nodig zouden moeten hebben. Dit is bijvoorbeeld het geval wanneer een onderzoeker het verloop van een ziekte bestudeert bij patiënten van wie de identiteit alleen bekend is bij het ziekenhuis waar ze worden behandeld en waarvan de onderzoeker de gepseudonimiseerde ziektegeschiedenissen verkrijgt. Pseudonimisering is derhalve een krachtig instrument in het arsenaal van privacyversterkende technologie. Het kan fungeren als een belangrijk element in de toepassing van "privacy by design". Privacy by design houdt in dat gegevensbescherming wordt ingebouwd in de structuur van geavanceerde gegevensverwerkingssystemen.

2.2. Gegevensverwerking

Belangrijkste punten

- De term "verwerking" heeft voornamelijk betrekking op geautomatiseerde verwerking.
- In het EU-recht heeft "verwerking" daarnaast ook betrekking op handmatige verwerking in gestructureerde bestanden van persoonsgegevens.
- Volgens het RvE-recht kan de betekenis van "verwerking" bij nationale wetgeving worden uitgebreid om ook handmatige verwerking te omvatten.

Gegevensbescherming uit hoofde van Verdrag 108 en de richtlijn gegevensbescherming richt zich voornamelijk op geautomatiseerde gegevensverwerking.

In **het RvE-recht** erkent de definitie van geautomatiseerde verwerking echter dat in de tijd tussen geautomatiseerde verwerkingen enkele fasen van handmatig gebruik van persoonsgegevens nodig kunnen zijn. In **het EU-recht** is geautomatiseerde gegevensverwerking gedefinieerd als "elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés".[70]

> Voorbeeld: In *Bodil Lindqvist*[71] oordeelde het HvJ-EU dat:
>
> "het vermelden van verschillende personen op een internetpagina met hun naam of anderszins, bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun liefhebberijen, als een 'geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens' in de zin van artikel 3, lid 1, van richtlijn 95/46 is aan te merken".

Ook bij handmatige gegevensverwerking is gegevensbescherming vereist.

In **het EU-recht** is gegevensbescherming geenszins beperkt tot geautomatiseerde gegevensverwerking. Bijgevolg is gegevensbescherming volgens het EU-recht van toepassing op de verwerking van persoonsgegevens in een handmatig bestand van persoonsgegevens, d.w.z. een daartoe speciaal gestructureerd papieren bestand.[72] De reden voor deze uitbreiding van de gegevensbescherming is dat:

- papieren bestanden zodanig gestructureerd kunnen worden dat informatie snel en gemakkelijk kan worden gevonden; en

- de opslag van persoonsgegevens in gestructureerde papieren bestanden het gemakkelijk maakt om de wettelijke beperkingen op geautomatiseerde gegevensverwerking te omzeilen.[73]

In **het RvE-recht** regelt Verdrag 108 primair gegevensverwerking in geautomatiseerde gegevensbestanden.[74] Het Verdrag voorziet echter ook in de mogelijkheid

70 Verdrag 108, artikel 2, onder c), en de richtlijn gegevensbescherming, artikel 2, onder b), en artikel 3, lid 1.

71 HvJ-EU, zaak C-101/01, *Bodil Lindqvist*, 6 november 2003, punt 27.

72 Richtlijn gegevensbescherming, artikel 3, lid 1.

73 *Ibid*., overweging 27.

74 Verdrag 108, artikel 2, onder b).

dat nationale wetgeving de bescherming uitbreidt naar handmatige verwerking. Veel partijen bij Verdrag 108 hebben van deze mogelijkheid gebruikgemaakt en hiertoe verklaringen gericht tot de secretaris-generaal van de RvE.[75] De uitbreiding van gegevensbescherming op grond van een dergelijke verklaring moet betrekking hebben op alle handmatige verwerkingen en mag niet worden beperkt tot verwerking in manuele bestanden.[76]

Wat betreft de aard van de verwerkingen is het begrip verwerking alomvattend in **zowel het EU-recht als het RvE-recht**: "'verwerking van persoonsgegevens' (...), elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procédés, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens"[77]. De term "verwerking" omvat ook handelingen waarbij de gegevens ophouden een verantwoordelijkheid van een voor de verwerking verantwoordelijke te zijn en onder de verantwoordelijkheid van een andere voor de verwerking verantwoordelijke komen te vallen.

Voorbeeld: Werkgevers verzamelen en verwerken gegevens over hun werknemers, waaronder informatie over hun salarissen. De rechtsgrondslag voor de rechtmatigheid hiervan is het arbeidscontract.

Werkgevers zullen de salarisgegevens van hun werknemers moeten doorgeven aan de belastingautoriteiten. De doorgifte van gegevens zal ook "verwerking" volgens de betekenis van deze term in Verdrag 108 en de richtlijn gegevensbescherming zijn. De rechtsgrondslag voor deze doorgifte is echter niet het arbeidscontract. Er moet een aanvullende rechtsgrondslag zijn voor de verwerkingen die resulteren in de overdracht van salarisgegevens door de werkgever aan de belastingautoriteiten. Deze rechtsgrondslag is over het algemeen vervat in de bepalingen van de nationale belastingwetgeving. Zonder deze bepalingen zou de overdracht van de gegevens een illegale verwerking zijn.

75 Zie de verklaringen als bedoeld in Verdrag 108, artikel 3, lid 2, onder c).

76 Zie de bewoording van Verdrag 108, artikel 3, lid 2.

77 Richtlijn gegevensbescherming, artikel 2, onder b). Zie ook Verdrag 108, artikel 2, onder c).

2.3. De gebruikers van persoonsgegevens

Belangrijkste punten

- Eenieder die besluit om persoonsgegevens van anderen te verwerken, is volgens de gegevensbeschermingswetgeving een "voor de verwerking verantwoordelijke"; wanneer meerdere personen dit besluit samen nemen, kunnen ze "gezamenlijk voor de verwerking verantwoordelijken" zijn.
- Een "verwerker" is een juridisch afzonderlijke entiteit die ten behoeve van de voor de verwerking verantwoordelijke persoonsgegevens verwerkt.
- Een verwerker wordt een voor de verwerking verantwoordelijke als hij of zij gegevens voor zijn of haar eigen doeleinden gebruikt en daarbij niet in opdracht van een voor de verwerking verantwoordelijke handelt.
- Iedereen die gegevens van een verwerker ontvangt is een "ontvanger".
- Een "derde" is een natuurlijke of rechtspersoon die niet in opdracht van de voor de verwerking verantwoordelijke handelt (en niet de betrokkene is).
- Een "ontvangende derde" is een persoon of entiteit die juridisch losstaat van de voor de verwerking verantwoordelijke, maar persoonsgegevens van de voor de verwerking verantwoordelijke ontvangt.

2.3.1. Voor de verwerking verantwoordelijken en verwerkers

De status van voor de verwerking verantwoordelijke of verwerker heeft als belangrijkste consequentie dat de betrokken persoon of entiteit wettelijk verantwoordelijk is voor de naleving van de van toepassing zijnde verplichtingen uit hoofde van de gegevensbeschermingswetgeving. Alleen wie krachtens de toepasselijke wetgeving verantwoordelijk kan worden gesteld, kan derhalve deze posities innemen. In de private sector is dit meestal een natuurlijke of een rechtspersoon; in de publieke sector is dit doorgaans een autoriteit. Andere entiteiten, zoals organen of instellingen zonder rechtspersoonlijkheid, kunnen alleen voor de verwerking verantwoordelijken of verwerkers zijn als bijzondere wettelijke bepalingen daarin voorzien.

Voorbeeld: Wanneer de marketingafdeling van Zonneschijn B.V. van plan is gegevens te verwerken in het kader van een marktonderzoek, is Zonneschijn B.V. de voor de verwerking verantwoordelijke voor deze verwerking.

De marketingafdeling kan niet de voor de verwerking verantwoordelijke zijn, omdat ze geen rechtspersoonlijkheid heeft.

In groepen van ondernemingen worden de moedermaatschappij en elke verbonden onderneming, als afzonderlijke rechtspersonen, beschouwd als voor de verwerking verantwoordelijken of verwerkers. Als gevolg van deze juridisch losstaande status is voor de overdracht van gegevens tussen de leden van een groep van ondernemingen een bijzondere rechtsgrondslag nodig. Er bestaat als zodanig geen voorrecht dat het toestaat om persoonsgegevens tussen de afzonderlijke rechtspersonen binnen de groep uit te wisselen.

In dit verband moet de rol van particulieren worden vermeld. **In het EU-recht** vallen particulieren die gegevens over anderen verwerken in het kader van een zuiver persoonlijke of huishoudelijke activiteit niet onder de voorschriften van de richtlijn gegevensbescherming; ze worden niet geacht voor de verwerking verantwoordelijken te zijn.[78]

In de jurisprudentie is echter bepaald dat gegevensbeschermingswetgeving desondanks van toepassing is wanneer een particulier tijdens het gebruik van internet gegevens over anderen publiceert.

Voorbeeld: In de zaak *Bodil Lindqvist*[79] oordeelde het HvJ-EU dat:

"het vermelden van verschillende personen op een internetpagina met hun naam of anderszins (...), als een 'geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens' in de zin van artikel 3, lid 1, van richtlijn 95/46 is aan te merken".[80]

Deze persoonsgegevens vallen niet onder zuiver persoonlijke of huishoudelijke activiteiten, die buiten het toepassingsgebied van de richtlijn gegevensbescherming vallen, aangezien deze uitzondering "derhalve aldus [moet] worden uitgelegd, dat zij uitsluitend betrekking heeft op activiteiten die tot het persoonlijke of gezinsleven van particulieren behoren, hetgeen klaarblijkelijk niet het geval is met de verwerking van persoonsgegevens die bestaat in hun openbaarmaking

78 Richtlijn gegevensbescherming, overweging 12 en artikel 3, lid 2, laatste streepje.

79 HvJ-EU, zaak C-101/01, *Bodil Lindqvist*, 6 november 2003.

80 *Ibid.*, punt 27.

op internet waardoor die gegevens voor een onbepaald aantal personen toegankelijk worden gemaakt."[81]

Voor de verwerking verantwoordelijke

In **het EU-recht** is een voor de verwerking verantwoordelijke gedefinieerd als iemand die "alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt".[82] In een besluit van een voor de verwerking verantwoordelijke wordt vastgelegd waarom en hoe de gegevens zullen worden verwerkt. In **het RvE-recht** wordt in de definitie van "voor de verwerking verantwoordelijke" bovendien vermeld dat een voor de verwerking verantwoordelijke beslist welke categorieën persoonsgegevens dienen te worden opgeslagen.[83]

De definitie van "voor de verwerking verantwoordelijke" van Verdrag 108 omvat nog een ander aspect van verantwoordelijkheid voor de verwerking dat aandacht verdient. In deze definitie wordt verwezen naar de bevoegdheid volgens het nationale recht om bepaalde gegevens voor een bepaald doel te verwerken. Wanneer echter een vermeende illegale verwerking plaatsvindt en de voor de verwerking verantwoordelijke moet worden gevonden, zal de persoon of de entiteit, zoals een onderneming of een autoriteit, die heeft beslist dat de gegevens moesten worden verwerkt, ongeacht of deze daar wettelijk toe bevoegd was of niet,[84] geacht worden de voor de verwerking verantwoordelijke te zijn. Een verzoek om het uitwissen van gegevens moet dan ook altijd worden gericht tot de "feitelijke" voor de verwerking verantwoordelijke.

Gezamenlijke verantwoordelijkheid voor de verwerking

De definitie van "voor de verwerking verantwoordelijke" in de richtlijn gegevensbescherming voorziet erin dat ook meerdere, juridisch van elkaar gescheiden entiteiten samen of gezamenlijk verantwoordelijk voor de verwerking kunnen zijn. Dat betekent dat ze samen beslissen om gegevens te verwerken voor een gedeeld doel.[85] Dit is echter alleen wettelijk mogelijk wanneer een bijzondere rechtsgrondslag voorziet in de gezamenlijke verwerking voor een gemeenschappelijk doel.

81 *Ibid*., punt 47.

82 Richtlijn gegevensbescherming, artikel 2, onder d).

83 Verdrag 108, artikel 2, onder d).

84 Zie ook de Groep gegevensbescherming artikel 29 (2010), *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010, blz. 15.

85 Richtlijn gegevensbescherming, artikel 2, onder d).

Voorbeeld: Een door verschillende kredietinstellingen beheerde databank over wanbetalende klanten is een gebruikelijk voorbeeld van gezamenlijke verantwoordelijkheid voor de verwerking. Wanneer iemand een kredietlijn aanvraagt bij een bank die een van de gezamenlijk voor de verwerking verantwoordelijken is, controleert de bank de databank om een geïnformeerd besluit te kunnen nemen over de kredietwaardigheid van de aanvrager.

In de wetgeving wordt niet uitdrukkelijk bepaald of het voor het bestaan van gezamenlijke verantwoordelijkheid noodzakelijk is dat het gedeelde doeleinde voor elk van de voor de verwerking verantwoordelijken hetzelfde is dan wel of het voldoende is dat hun doeleinden elkaar slechts gedeeltelijk overlappen. Hierover is echter nog geen toepasselijke jurisprudentie beschikbaar op Europees niveau, en ook is er geen duidelijkheid over de consequenties ten aanzien van aansprakelijkheid. De Groep gegevensbescherming artikel 29 pleit voor een bredere interpretatie van het begrip "gezamenlijke verantwoordelijkheid" om enige flexibiliteit in te bouwen in verband met de toenemende complexiteit van de huidige gegevensverwerkingsrealiteit.[86] Een zaak rond de Society for Worldwide Interbank Financial Telecommunication (SWIFT) is illustratief voor het standpunt van de werkgroep.

Voorbeeld: In de zogenoemde SWIFT-zaak hadden Europese bankinstellingen SWIFT ingehuurd, oorspronkelijk als verwerker, om de doorgifte van gegevens in het kader van banktransacties te verzorgen. SWIFT droeg deze gegevens over banktransacties, die waren opgeslagen in servers in de Verenigde Staten, over aan het Amerikaanse ministerie van Financiën zonder dat de Europese bankinstellingen die SWIFT hadden gecontracteerd daar expliciet opdracht toe hadden gegeven. De Groep gegevensbescherming artikel 29 kwam na het beoordelen van de rechtmatigheid van deze situatie tot de conclusie dat de Europese bankinstellingen die SWIFT hadden ingehuurd, evenals SWIFT zelf, moesten worden gezien als gezamenlijk voor de verwerking verantwoordelijken die tegenover Europese klanten verantwoordelijk waren voor de doorgifte van hun gegevens aan de Amerikaanse autoriteiten.[87] SWIFT had, door te besluiten de gegevens over te dragen, – onterecht – de rol van voor de verwerking verantwoordelijke op zich genomen; de bankinstellingen waren duidelijk

86 Zie Groep gegevensbescherming artikel 29 (2010), *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010, blz. 19.

87 Groep gegevensbescherming artikel 29 (2006), *Advies 10/2006 over de verwerking van persoonsgegevens door de Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Brussel, 22 november 2006.

tekortgeschoten in de naleving van hun verplichting om toezicht op de verwerker te houden en konden daarom niet volledig worden ontslagen van hun verantwoordelijkheid als voor de verwerking verantwoordelijken. Deze situatie resulteerde in gezamenlijke verantwoordelijkheid voor de verwerking.

Verwerker

Een verwerker wordt in **het EU-recht** gedefinieerd als iemand die persoonsgegevens verwerkt ten behoeve van de voor de verwerking verantwoordelijke.[88] De werkzaamheden die aan een verwerker worden toevertrouwd kunnen beperkt blijven tot een zeer specifieke taak of context of kunnen van vrij algemene of van alomvattende aard zijn.

In **het RvE-recht** is de betekenis van een verwerker hetzelfde als in het EU-recht.

Verwerkers zullen, benevens gegevens verwerken voor anderen, zelf ook voor de verwerking verantwoordelijken zijn in verband met de verwerkingen die ze uitvoeren voor hun eigen doeleinden, bv. voor de administratie van de eigen werknemers, verkopen en facturen.

Voorbeeld: Een onderneming is gespecialiseerd in gegevensverwerking in het kader van de administratie van HR-gegevens voor andere ondernemingen. In deze functie is de onderneming een verwerker.

Wanneer de onderneming echter gegevens over haar eigen werknemers verwerkt, is ze de voor de verwerking verantwoordelijke met het oog op het vervullen van de verplichtingen die ze als werkgever heeft.

De verhouding tussen de voor de verwerking verantwoordelijke en de verwerker

Zoals we hebben gezien, is de "voor de verwerking verantwoordelijke" gedefinieerd als degene die de doeleinden van de verwerking en de wijze van verwerking bepaalt.

88 Richtlijn gegevensbescherming, artikel 2, onder e).

Voorbeeld: De directeur van Zonneschijn B.V. besluit dat Maanlicht B.V., een specialist in marktanalyse, een marktanalyse van de klantgegevens van Zonneschijn B.V. moet uitvoeren. Hoewel de taak om de wijze van verwerking te bepalen dus wordt gedelegeerd aan Maanlicht B.V., blijft Zonneschijn B.V. de voor de verwerking verantwoordelijke en is Maanlicht B.V. slechts een verwerker, aangezien, volgens het contract, Maanlicht B.V. de klantgegevens van Zonneschijn B.V. alleen mag gebruiken voor de doeleinden die Zonneschijn B.V. heeft vastgesteld.

Als de bevoegdheid om de wijze van verwerking te bepalen wordt gedelegeerd aan een verwerker, moet de voor de verwerking verantwoordelijke zich niettemin kunnen bemoeien met de beslissingen van de verwerker met betrekking tot de wijze van verwerking. De eindverantwoordelijkheid ligt nog steeds bij de voor de verwerking verantwoordelijke, die toezicht moet houden op de verwerkers om ervoor te zorgen dat hun beslissingen voldoen aan de gegevensbeschermingswetgeving. Een contract dat de voor de verwerking verantwoordelijke verbiedt om zich te bemoeien met de beslissingen van de verwerker zou daarom waarschijnlijk worden geacht te resulteren in gezamenlijke verantwoordelijkheid, waarbij beide partijen de wettelijke verantwoordelijkheid van een voor de verwerking verantwoordelijke delen.

Voorts zal een verwerker, indien deze de beperkingen aan het gebruik van de gegevens als voorgeschreven door de voor de verwerking verantwoordelijke niet respecteert, een voor de verwerking verantwoordelijke moeten worden, althans voor zover het de inbreuk op de instructies van de voor de verwerking verantwoordelijke betreft. Dit zal de verwerker naar alle waarschijnlijkheid tot een voor de verwerking verantwoordelijke maken die onrechtmatig handelt. Op zijn beurt zal de oorspronkelijke voor de verwerking verantwoordelijke moeten uitleggen hoe het mogelijk was dat de verwerker zijn of haar mandaat te buiten kon gaan. De Groep gegevensbescherming artikel 29 is geneigd om in dergelijke gevallen gezamenlijke verantwoordelijkheid te veronderstellen, aangezien dit resulteert in de beste bescherming van de belangen van de betrokkenen.[89] Een belangrijke consequentie van gezamenlijke verantwoordelijkheid zou hoofdelijke aansprakelijkheid voor schade moeten zijn, waardoor de betrokkenen ruimere mogelijkheden hebben om verhaal te halen.

89 Groep gegevensbescherming artikel 29 (2010), *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010, blz. 25; en Groep gegevensbescherming artikel 29 (2006), Advies 10/2006 over de verwerking van persoonsgegevens door de Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128, Brussel, 22 november 2006.

Ook kunnen er problemen ontstaan met de verdeling van de verantwoordelijkheid wanneer de voor de verwerking verantwoordelijke een kleine onderneming is en de verwerker een grote onderneming die over de macht beschikt om de voorwaarden van de diensten te dicteren. In dergelijke omstandigheden stelt de Groep gegevensbescherming artikel 29 echter dat de normen voor de verantwoordelijkheid voor de gegevensverwerking niet mogen worden versoepeld vanwege economische onevenwichtigheden en dat de uitleg van het begrip "voor de verwerking verantwoordelijke" moet worden gehandhaafd.[90]

Ten behoeve van de duidelijkheid en de transparantie moeten de details van de verhouding tussen een voor de verwerking verantwoordelijke en een verwerker worden vastgelegd in een schriftelijke overeenkomst.[91] Het ontbreken van een dergelijke overeenkomst vormt een inbreuk op de verplichting van de voor de verwerking verantwoordelijke om schriftelijke documentatie van de wederzijdse verplichtingen te verstrekken en zou tot het opleggen van sancties kunnen leiden.[92]

Verwerkers zullen mogelijk bepaalde taken willen delegeren aan aanvullende subverwerkers. Dit is wettelijk toegestaan en zal afhankelijk zijn van de details van de contractuele bepalingen tussen de voor de verwerking verantwoordelijke en de verwerker, bijvoorbeeld of de machtiging van de voor de verwerking verantwoordelijke in elk afzonderlijk geval noodzakelijk is dan wel dat alleen informeren volstaat.

In **het RvE-recht** is de interpretatie van de begrippen verwerker en voor de verwerking verantwoordelijke, zoals hierboven uiteengezet, volledig van toepassing, zoals blijkt uit de aanbevelingen die op basis van Verdrag 108 zijn ontwikkeld.[93]

2.3.2. Ontvangers en derden

Het verschil tussen deze categorieën van personen of entiteiten, die zijn ingevoerd bij de richtlijn gegevensbescherming, is voornamelijk gelegen in hun verhouding tot de verwerker en dientengevolge in hun bevoegdheid om toegang te verkrijgen tot gegevens die berusten bij de voor de verwerking verantwoordelijke.

90 Zie Groep gegevensbescherming artikel 29 (2010), *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010, blz. 30.

91 Richtlijn gegevensbescherming, artikel 17, leden 3 en 4.

92 Zie Groep gegevensbescherming artikel 29 (2010), *Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"*, WP 169, Brussel, 16 februari 2010, blz. 31.

93 Zie bijvoorbeeld de Aanbeveling inzake profilering, artikel 1.

Een "derde" is iemand die juridisch niet dezelfde is als de voor de verwerking verantwoordelijke. Voor de overdracht van gegevens aan een derde zal daarom altijd een specifieke rechtsgrondslag nodig zijn. Volgens artikel 2, onder f), van de richtlijn gegevensbescherming is een derde "de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam, niet zijnde de betrokkene, noch de voor de verwerking verantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de voor de verwerking verantwoordelijke of de verwerker gemachtigd zijn om de gegevens te verwerken". Dit betekent dat personen die werkzaam zijn voor een organisatie die juridisch niet dezelfde is als de voor de verwerker verantwoordelijke, ook wanneer deze deel uitmaakt van hetzelfde concern of dezelfde houdstermaatschappij, "derden" zullen zijn (of tot een derde zullen behoren). Anderzijds zijn kantoren van banken die de rekeningen van klanten verwerken onder rechtstreeks gezag van hun hoofdkantoor, geen "derden".[94]

"Ontvanger" is een bredere term dan "derde". Volgens artikel 2, onder g), van de richtlijn gegevensbescherming betekent ontvanger "de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander lichaam aan wie, respectievelijk waaraan de gegevens worden meegedeeld, ongeacht of het al dan niet een derde betreft". Deze ontvanger kan ofwel een persoon buiten de voor de verwerking verantwoordelijke of de verwerker zijn – dit zou dan een derde zijn – of iemand binnen de voor de verwerking verantwoordelijke of de verwerker, zoals een werknemer of een andere afdeling van dezelfde onderneming of autoriteit.

Het onderscheid tussen ontvangers en derden is alleen van belang vanwege de voorwaarden voor rechtmatige doorgifte van gegevens. De werknemers van een voor de verwerking verantwoordelijke of verwerker kunnen zonder verdere wettelijke vereisten ontvangers van persoonsgegevens zijn indien ze betrokken zijn bij verwerkingen van de voor de verwerking verantwoordelijke of de verwerker. Anderzijds is een derde, die juridisch niet dezelfde is als de voor de verwerking verantwoordelijke of de verwerker, niet bevoegd om door de voor de verwerking verantwoordelijke verwerkte gegevens te gebruiken, tenzij op basis van een specifieke rechtsgrondslag in een specifiek geval. "Derde ontvangers" van gegevens zullen derhalve altijd een rechtsgrondslag nodig hebben om rechtmatig persoonsgegevens te kunnen ontvangen.

94 Zie Groep gegevensbescherming artikel 29 (2010), Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker", WP 169, Brussel, 16 februari 2010, blz. 35.

Voorbeeld: Een werknemer van een verwerker die persoonsgegevens gebruikt binnen de taakopdracht die hem of haar door de werkgever is toevertrouwd, is een ontvanger van gegevens, maar geen derde, aangezien hij of zij de gegevens gebruikt namens en in opdracht van de verwerker.

Indien dezelfde werknemer echter besluit de gegevens waartoe hij of zij als werknemer van de verwerker toegang heeft te gebruiken voor zijn of haar eigen doeleinden en ze aan een andere onderneming verkoopt, is de werknemer opgetreden als derde. Hij of zij volgt niet langer de orders van de verwerker (de werkgever). Als derde heeft de werknemer een rechtsgrondslag nodig om de gegevens te kunnen verwerven en verkopen. In dit voorbeeld beschikt de werknemer zeker niet over een dergelijke rechtsgrondslag, zodat deze handelingen illegaal zijn.

2.4. Toestemming

Belangrijkste punten

- Toestemming als rechtsgrondslag voor de verwerking van persoonsgegevens moet vrij, geïnformeerd en specifiek zijn.
- De toestemming moet ondubbelzinnig zijn gegeven. De toestemming kan ofwel expliciet worden gegeven, ofwel impliciet op een wijze die geen ruimte voor twijfel laat over het feit dat de betrokkene ermee instemt dat zijn of haar gegevens worden verwerkt.
- De verwerking van gevoelige gegevens op basis van toestemming vereist expliciete toestemming.
- De toestemming kan te allen tijde worden ingetrokken.

Toestemming betekent "elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem/haar betreffende persoonsgegevens worden verwerkt".[95] Dit is in veel gevallen de rechtsgrondslag voor rechtmatige gegevensverwerking (zie paragraaf 4.1).

95 Richtlijn gegevensbescherming, artikel 2, onder h).

2.4.1. De elementen van geldige toestemming

In **het EU-recht** worden drie elementen genoemd die vervuld moeten zijn om een toestemming geldig te laten zijn, die ten doel hebben om te garanderen dat betrokkenen heel bewust hebben ingestemd met het gebruik van hun gegevens.

- de betrokkene mag niet onder druk zijn gezet om toestemming te geven;
- de betrokkene moet naar behoren zijn geïnformeerd over het doel en de gevolgen van de toestemming;
- de reikwijdte van de toestemming moet in redelijke mate concreet zijn.

Alleen als aan al deze eisen is voldaan, zal de toestemming geldig zijn in de zin van de gegevensbeschermingswetgeving.

Verdrag 108 bevat geen definitie van toestemming; dit wordt overgelaten aan het nationale recht. De elementen van geldige toestemming zijn in **het RvE-recht** echter verder ontwikkeld in de aanbevelingen die op basis van Verdrag 108 zijn geformuleerd en komen overeen met de hierboven genoemde.[96] De vereisten voor het bestaan van toestemming zijn dezelfde als die welke van toepassing zijn op een geldige intentieverklaring in het Europese civiele recht.

Aanvullende eisen voor geldige toestemming in het civiele recht, zoals rechtshandelingsbekwaamheid, zijn uiteraard ook van toepassing in het kader van gegevensbescherming, aangezien deze eisen fundamentele juridische voorafgaande voorwaarden zijn. Ongeldige toestemming van personen die niet handelingsbekwaam zijn zal resulteren in het ontbreken van een rechtsgrondslag voor de verwerking van gegevens over deze personen.

De toestemming kan uitdrukkelijk[97] of niet-uitdrukkelijk worden gegeven. Uitdrukkelijke toestemming laat geen ruimte voor twijfel over de intenties van de betrokkene en kan ofwel mondeling, ofwel schriftelijk worden gegeven. Elke toestemming moet op ondubbelzinnige wijze worden gegeven.[98] Dit betekent dat er geen redelijke twijfel mag bestaan of de betrokkene zijn of haar instemming met de verwerking van zijn of haar gegevens wilde meedelen of niet. Het afleiden van toestemming uit

96 Zie bijvoorbeeld Verdrag 108, Aanbeveling betreffende statistische gegevens, punt 6.

97 Richtlijn gegevensbescherming, artikel 8, lid 2.

98 *Ibid.*, artikel 7, onder a), en artikel 26, lid 1.

loutere inactiviteit kan bijvoorbeeld niet voor het bestaan van ondubbelzinnige toestemming zorgen. Wanneer de verwerkte gegevens gevoelig zijn, is uitdrukkelijke toestemming verplicht en moet deze ondubbelzinnig zijn.

Vrije toestemming

Vrije toestemming kan alleen rechtsgeldig zijn "als de betrokkene een werkelijke keuze heeft en er geen sprake is van bedrog, intimidatie of dwang en de betrokkene ook niet het risico van aanzienlijke negatieve gevolgen loopt wanneer hij niet toestemt".[99]

Voorbeeld: Op veel luchthavens moeten passagiers door zogeheten "lichaamsscanners" om de boardingruimte te kunnen betreden.[100] Aangezien tijdens het scannen passagiersgegevens worden verwerkt, moet de verwerking voldoen aan een van de rechtsgrondslagen van artikel 7 van de richtlijn gegevensbescherming (zie paragraaf 4.1.1). Het passeren van lichaamsscanners wordt soms aan passagiers gepresenteerd als een optie, waarbij wordt geïmpliceerd dat hun toestemming de verwerking zou kunnen rechtvaardigen. Passagiers zouden echter kunnen vrezen dat een weigering om door lichaamsscanners te gaan hen verdacht zal doen lijken of tot extra controles zal leiden, zoals fouillering. Veel passagiers stemmen ermee in om te worden gescand omdat ze daarmee mogelijke problemen uit de weg gaan en vertragingen vermijden. Deze toestemming is vermoedelijk niet voldoende vrij.

Een deugdelijke rechtsgrond kan alleen worden gevonden in een rechtshandeling van een wetgever, op basis van artikel 7, onder e), van de richtlijn gegevensbescherming, die resulteert in een verplichting voor passagiers om mee te werken vanwege het hogere algemene belang. Dergelijke wetgeving kan nog steeds voorzien in een keuze tussen scannen en fouilleren, maar alleen als onderdeel van aanvullende grenscontrolemaatregelen die in specifieke

99 Zie ook Groep gegevensbescherming artikel 29 (2011), *Advies 15/2011 over de definitie van "toestemming"*, WP 187, Brussel, 13 juli 2011, blz. 12.

100 Dit voorbeeld is genomen uit *Ibid.*, blz. 15.

omstandigheden noodzakelijk zijn. Dit is wat de Europese Commissie in 2011 heeft voorgesteld in twee verordeningen inzake beveiligingsscanners.[101]

Het bestaan van vrije toestemming zou ook kunnen worden bedreigd in situaties van ondergeschiktheid wanneer er een significante onevenwichtige economische of andere machtsverhouding bestaat tussen de voor de verwerking verantwoordelijke die toestemming verkrijgt en de betrokkene die toestemming verleent.[102]

Voorbeeld: Een groot bedrijf wil een gids samenstellen met de namen van alle werknemers, hun functie in het bedrijf en hun zakelijke adressen, met als enig doel het verbeteren van de interne bedrijfscommunicatie. Het hoofd personeelszaken stelt voor ook een foto van elke werknemer in de gids op te nemen om het bijvoorbeeld makkelijker te maken collega's bij vergaderingen te herkennen. Werknemersvertegenwoordigers verlangen dat dit uitsluitend gebeurt met toestemming van de werknemers zelf.

In een dergelijke situatie kan de toestemming van de werknemer worden beschouwd als de rechtsgrondslag voor de verwerking van de foto's in de gids, omdat het duidelijk is dat het publiceren van een foto in de gids op zich geen nadelige gevolgen heeft en het bovendien geloofwaardig is dat de werknemer geen nadelige gevolgen door toedoen van de werkgever zal ondervinden als hij of zij niet instemt met publicatie van zijn of haar foto in de gids.

Dit betekent echter niet dat toestemming nooit rechtsgeldig kan zijn in omstandigheden waarin het niet verlenen van toestemming negatieve gevolgen kan hebben. Als bijvoorbeeld het niet verlenen van toestemming voor het verkrijgen van een klantenkaart van een supermarkt er uitsluitend toe leidt dat de betrokkene geen kortingen op de prijs van bepaalde artikel en krijgt, is toestemming nog steeds een

101 Verordening (EU) nr. 1141/2011 van de Commissie van 10 november 2011 tot wijziging van Verordening (EG) nr. 272/2009 ter aanvulling van de gemeenschappelijke basisnormen voor de beveiliging van de burgerluchtvaart, wat betreft het gebruik van beveiligingsscanners op EU-luchthavens, PB L 293 van 11.11.2011, blz. 22, en Uitvoeringsverordening (EU) nr. 1147/2011 van de Commissie van 11 november 2011 houdende vaststelling van gedetailleerde maatregelen voor de toepassing van de gemeenschappelijke basisnormen op het gebied van de beveiliging van de luchtvaart, wat betreft het gebruik van beveiligingsscanners op EU-luchthavens, PB L 294 van 12.11.2011, blz. 7.

102 Zie ook Groep gegevensbescherming artikel 29 (2001), *Advies 8/2001 over de verwerking van persoonsgegevens in het kader van de arbeidsverhouding*, WP 48, Brussel, 13 september 2001, en Groep gegevensbescherming artikel 29 (2005), *Werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995*, WP 114, Brussel, 25 november 2005.

geldige rechtsgrondslag voor de verwerking van persoonsgegevens van de klanten die er wel mee hebben ingestemd om een klantenkaart te ontvangen. Er is geen sprake van een situatie van ondergeschiktheid tussen de onderneming en de klant, en de gevolgen van het niet verlenen van toestemming zijn niet ernstig genoeg voor de betrokkene om af te doen aan het bestaan van vrije keuze.

Anderzijds geldt dat wanneer voldoende belangrijke goederen of diensten enkel en alleen kunnen worden verkregen als bepaalde persoonsgegevens aan derden worden overgedragen, de toestemming van de betrokkene voor de overdracht van zijn of haar gegevens over het algemeen niet als een vrije keuze kan worden beschouwd en deze toestemming dus niet rechtsgeldig is overeenkomstig de gegevensbeschermingswetgeving.

Voorbeeld: Door passagiers aan een luchtvaartmaatschappij verleende toestemming om zogeheten "passenger name records" (PNR), d.w.z. gegevens over hun identiteit, eetgewoonten en gezondheidsproblemen, aan de immigratieautoriteiten van een specifiek derde land door te geven, kan niet worden beschouwd als geldige toestemming krachtens de gegevensbeschermingswetgeving, aangezien de passagiers geen keuze hebben als ze het desbetreffende land willen bezoeken. Voor de rechtmatige overdracht van deze gegevens is een andere rechtsgrondslag dan toestemming vereist: zeer waarschijnlijk een specifieke wet.

Geïnformeerde toestemming

De betrokkene moet over voldoende informatie beschikken alvorens zijn of haar besluit te nemen. Of de verstrekte informatie al dan niet voldoende is, kan alleen per geval worden beoordeeld. Voor geïnformeerde toestemming zal doorgaans een precieze en eenvoudig te begrijpen beschrijving van het onderwerp van de toestemming en van de gevolgen van het al dan niet verlenen van toestemming nodig zijn. De taal die in de verstrekte informatie wordt gebruikt moet zijn aangepast aan de verwachte ontvangers van de informatie.

Ook moet de informatie gemakkelijk beschikbaar zijn voor de betrokkene. De toegankelijkheid en zichtbaarheid van de informatie zijn belangrijke elementen. In een online-omgeving kan gelaagde informatie een goede oplossing zijn, omdat in dat geval behalve een beknopte versie van de informatie ook een uitgebreidere versie ter beschikking van de betrokkene staat.

Specifieke toestemming

Om geldig te zijn, moet toestemming ook specifiek zijn. Dit gaat hand in hand met de kwaliteit van de over het oogmerk van de toestemming verstrekte informatie. In dit verband zijn de redelijke verwachtingen van een gemiddelde betrokkene relevant. De betrokkene moet opnieuw om toestemming worden gevraagd indien verwerkingsactiviteiten worden toegevoegd of gewijzigd op een manier die redelijkerwijs niet kon worden voorzien toen de oorspronkelijke toestemming werd verleend.

Voorbeeld: In de zaak *Deutsche Telekom AG*[103] behandelde het HvJ-EU de vraag of een telecomaanbieder die persoonsgegevens van abonnees op grond van artikel 12 van richtlijn betreffende privacy en elektronische communicatie[104] moest overdragen, opnieuw toestemming van de betrokkenen nodig had, gelet op het feit dat de ontvangers bij de oorspronkelijke toestemmingsverlening niet waren genoemd.

Het HvJ-EU oordeelde dat volgens dit artikel hernieuwde toestemming om de gegevens over te dragen niet noodzakelijk was omdat de betrokkenen op grond van deze bepaling de mogelijkheid hadden om alleen toestemming te geven voor het doeleinde van de verwerking, te weten de publicatie van hun gegevens, en niet konden kiezen tussen verschillende gidsen waarin deze gegevens mogelijk zouden worden gepubliceerd.

Zoals het Hof onderstreepte, "volgt uit een contextuele en systematische uitlegging van artikel 12 van de richtlijn betreffende privacy en elektronische communicatie dat de in artikel 12, lid 2, bedoelde toestemming betrekking heeft op het doel van de publicatie van de persoonsgegevens in een openbare telefoongids, en niet op de identiteit van een telefoongidsaanbieder in het bijzonder."[105] Bovendien "is [het] de publicatie zelf van persoonsgegevens in een telefoongids die een bijzondere doelstelling heeft, die schadelijk kan blijken te zijn voor een abonnee"[106] en niet wie de auteur van deze publicatie is.

103 HvJ-EU, zaak C-543/09, *Deutsche Telekom AG / Bondsrepubliek Duitsland*, 5 mei 2011; zie met name de punten 53 en 54.

104 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (*richtlijn betreffende privacy en elektronische communicatie*), PB L 201 van 31.7.2002, blz. 37.

105 HvJ-EU, zaak C-543/09, *Deutsche Telekom AG / Bondsrepubliek Duitsland*, 5 mei 2011; zie met name punt 61.

106 *Ibid.*, zie met name punt 62.

2.4.2. Het recht om toestemming te allen tijde in te trekken

In de richtlijn gegevensbescherming wordt geen melding gemaakt van een algemeen recht om toestemming te allen tijd in te trekken. Het wordt echter algemeen aangenomen dat een dergelijk recht bestaat en dat het voor de betrokkene mogelijk moet zijn om dit recht naar eigen goeddunken uit te oefenen. Er mag geen verplichting bestaan om redenen te geven voor een intrekking en er mag geen risico bestaan op negatieve gevolgen anders dan de beëindiging van de voordelen die mogelijk voortvloeiden uit het eerder overeengekomen gebruik van de gegevens.

Voorbeeld: Een klant stemt erin toe om reclamemateriaal te ontvangen op een adres dat hij of zij opgeeft aan de voor de verwerking verantwoordelijke. Mocht de klant deze toestemming weer intrekken, dan moet de voor de verwerking verantwoordelijke onmiddellijk stoppen met het verzenden van het reclamemateriaal. Daar mogen geen sancties op staan, zoals boetes of vergoedingen.

Als de klant een korting van 5 % op de kosten van een hotelkamer ontving in ruil voor de toestemming voor het gebruik van zijn of haar gegevens voor reclamedoeleinden, mag de intrekking van de toestemming om reclamemateriaal te ontvangen op een later moment niet tot gevolg hebben dat de klant de ontvangen kortingen moet terugbetalen.

3

De belangrijkste beginselen van de Europese gegevensbeschermingswetgeving

EU	Behandelde onderwerpen	RvE
Richtlijn gegevensbescherming, artikel 6, lid 1, onder a) en b) HvJ-EU, zaak C-524/06, *Huber / Bondsrepubliek Duitsland*, 16 december 2008 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert / Land Hessen*, 9 november 2010	**Het beginsel van rechtmatige verwerking**	Verdrag 108, artikel 5, onder a) en b) EHRM, *Rotaru / Roemenië* [GC], nr. 28341/95, 4 mei 2000 EHRM, *Taylor-Sabori / Verenigd Koninkrijk*, nr. 47114/99, 22 oktober 2002 EHRM, *Peck / Verenigd Koninkrijk*, nr. 44647/98, 28 januari 2003 EHRM, *Khelili / Zwitserland*, nr. 16188/07, 18 oktober 2011 EHRM, *Leander / Zweden*, nr. 9248/81, 26 maart 1987
Richtlijn gegevensbescherming, artikel 6, lid 1, onder b)	**Het beginsel van doelbepaling en -binding**	Verdrag 108, artikel 5, onder b)
	Beginselen inzake de kwaliteit van de gegevens:	
Richtlijn gegevensbescherming, artikel 6, lid 1, onder c)	**Relevantie van de gegevens**	Verdrag 108, artikel 5, onder c)
Richtlijn gegevensbescherming, artikel 6, lid 1, onder d)	**Nauwkeurigheid van de gegevens**	Verdrag 108, artikel 5, onder d)

EU	Behandelde onderwerpen	RvE
Richtlijn gegevensbescherming, artikel 6, lid 1, onder e)	**Beperkte bewaring van gegevens**	Verdrag 108, artikel 5, onder e)
Richtlijn gegevensbescherming, artikel 6, lid 1, onder e)	**Uitzondering voor wetenschappelijke en statistische doeleinden**	Verdrag 108, artikel 9, lid 3
Richtlijn gegevensbescherming, artikel 6, lid 1, onder a)	**Het beginsel van eerlijke verwerking**	Verdrag 108, artikel 5, onder a) EHRM, *Haralambie / Roemenië*, nr. 21737/03, 27 oktober 2009 EHRM, *K.H. en anderen / Slowakije*, nr. 32881/04, 6 november 2009
Richtlijn gegevensbescherming, artikel 6, lid 2	**Het verantwoordingsbeginsel**	

De in artikel 5 van Verdrag 108 vervatte beginselen vormen de essentie van de Europese gegevensbeschermingswetgeving. Dezelfde beginselen zijn vastgelegd in artikel 6 van de richtlijn gegevensbescherming, als het uitgangspunt voor meer gedetailleerde bepalingen in de daaropvolgende artikel en van de richtlijn. Alle latere gegevensbeschermingswetgeving op RvE- of EU-niveau moet voldoen aan deze beginselen en deze beginselen moet in aanmerking worden genomen bij de interpretatie van deze wetgeving. Op nationaal niveau kunnen uitzonderingen op en beperkingen van deze fundamentele beginselen worden vastgesteld;[107] deze uitzonderingen en beperkingen moeten bij wet zijn gesteld, een rechtmatig doel dienen en noodzakelijk zijn in een democratische samenleving. Alle drie deze voorwaarden moeten zijn vervuld.

107 Verdrag 108, artikel 9, lid 2, en richtlijn gegevensbescherming, artikel 13.

3.1. Het beginsel van rechtmatige verwerking

Belangrijkste punten

- Om het beginsel van rechtmatige verwerking te begrijpen, moeten de voorwaarden voor de rechtmatige beperking van het recht op gegevensbescherming worden bezien in het licht van artikel 52, lid 1, van het Handvest van de grondrechten en de eisen van gerechtvaardigde inmenging van artikel 8, lid 2, van het EVRM.
- Bijgevolg is de verwerking van persoonsgegevens alleen rechtmatig indien deze:
  - overeenkomstig de wet plaatsvindt; en
  - een rechtmatig doel dient; en
  - noodzakelijk is in een democratische samenleving om het rechtmatige doel te verwezenlijken.

In **de gegevensbeschermingswetgeving van de EU en de RvE** is het beginsel van rechtmatige verwerking het eerste beginsel dat wordt genoemd; het beginsel wordt in artikel 5 van Verdrag 108 en artikel 6 van de richtlijn gegevensbescherming in vrijwel identieke termen omschreven.

Geen van deze bepalingen bevat een definitie van "rechtmatige verwerking". Om deze wettelijke term te begrijpen moet worden gekeken naar het begrip "gerechtvaardigde inmenging" als bedoeld in het EVRM en als uitgelegd in de jurisprudentie van het EHRM, en naar de voorwaarden voor wettelijke beperkingen in artikel 52 van het Handvest.

3.1.1. De vereisten voor gerechtvaardigde inmenging als bedoeld in het EVRM

De verwerking van persoonsgegevens kan een inmenging in het recht op eerbiediging van het privéleven van de betrokkene vormen. Het recht op eerbiediging van het privéleven is echter geen absoluut recht, maar moet worden afgewogen tegen en worden verzoend met andere rechtmatige belangen, hetzij van andere personen (particuliere belangen), hetzij van de samenleving als geheel (algemene belangen). De omstandigheden waarin inmenging door de staat is gerechtvaardigd zijn de volgende:

In overeenstemming met de wet

Volgens de jurisprudentie van het EHRM is inmenging in overeenstemming met de wet indien deze is gebaseerd op een nationale wettelijke bepaling die bepaalde eigenschappen moet hebben. De wet "moet toegankelijk zijn voor de betrokkene en qua gevolgen voorzienbaar zijn".[108] Een voorschrift is voorzienbaar "indien het voldoende nauwkeurig" is om iedere persoon – zo nodig met deskundig advies – in staat te stellen "zijn gedrag daarop af te stemmen".[109] "De vereiste mate van nauwkeurigheid van de wet in dit verband zal afhankelijk zijn van het specifieke onderwerp."[110]

Voorbeeld: In *Rotaru / Roemenië*[111] stelde het EHRM een inbreuk op artikel 8 van het EVRM vast omdat de Roemeense wet de vergaring, registratie en archivering in geheime dossiers van informatie die van belang was voor de nationale veiligheid toestond zonder dat er beperkingen waren gesteld aan de uitoefening van deze discretionaire bevoegdheden van de autoriteiten. Zo werd in de nationale wet geen definitie gegeven van het type informatie dat mocht worden verwerkt, de categorieën van personen tegen wie surveillancemaatregelen konden worden genomen, de omstandigheden waarin dergelijke maatregelen konden worden genomen en de te volgen procedure. Vanwege deze tekortkomingen concludeerde het Hof dat het nationale recht niet voldeed aan de eisen van voorzienbaarheid als bedoeld in artikel 8 van het EVRM en dat het artikel was geschonden.

Voorbeeld: In *Taylor-Sabori / Verenigd Koninkrijk*[112] was de verzoeker het doelwit van surveillance door de politie. Door gebruik te maken van een "kloon" van

108 EHRM, *Amann / Zwitserland* [GC], nr. 27798/95, 16 februari 2000, punt 50; zie ook EHRM, *Kopp / Zwitserland*, nr. 23224/94, 25 maart 1998, punt 55 en EHRM, *Iordachi en anderen / Moldavië*, nr. 25198/02, 10 februari 2009, punt 50.

109 EHRM, *Amann / Zwitserland* [GC], nr. 27798/95, 16 februari 2000, punt 56; zie ook EHRM, *Malone / Verenigd Koninkrijk*, nr. 8691/79, 26 april 1985, punt 66, en EHRM, *Silver en anderen / Verenigd Koninkrijk*, nrs. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 en 7113/75, 25 maart 1983, punt 88.

110 EHRM, *The Sunday Times / Verenigd Koninkrijk*, nr. 6538/74, 26 april 1979, punt 49; zie ook EHRM, *Silver en anderen / Verenigd Koninkrijk*, nrs. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 en 7113/75, 25 maart 1983, punt 88.

111 EHRM, *Rotaru / Roemenië* [GC], nr. 28341/95, 4 april 2000, punt 57; zie ook EHRM, *Association for European Integration and Human Rights en Ekimdzhiev / Bulgarije*, nr. 62540/00, 28 juni 2007, EHRM, *Shimovolos / Rusland*, nr. 30194/09, 21 juni 2011, en EHRM, *Vetter / Frankrijk*, nr. 59842/00, 31 mei 2005.

112 EHRM, *Taylor-Sabori / Verenigd Koninkrijk*, nr. 47114/99, 22 oktober 2002.

de pieper van de verzoeker had de politie aan hem verzonden berichten weten te onderscheppen. Vervolgens werd de verzoeker aangehouden en samenzwering met het oogmerk om een gecontroleerde drug te leveren ten laste gelegd. De zaak van de openbaar aanklager was deels gebaseerd op de transcripties van de verstuurde berichten die de politie had gemaakt. Ten tijde van de rechtszaak tegen de verzoeker bevatte het recht van het Verenigd Koninkrijk echter geen bepaling inzake de onderschepping van via een particulier telecommunicatiesysteem verzonden berichten. De inmenging in zijn rechten was daarom niet "in overeenstemming met de wet" geweest. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Een rechtmatig doel dienen

Het rechtmatige doel kan ofwel een van de genoemde algemene belangen zijn, ofwel de rechten en vrijheden van anderen.

Voorbeeld: In *Peck / Verenigd Koninkrijk*[113] had de verzoeker geprobeerd zelfmoord te plegen door op straat zijn polsen door te snijden, zich er niet van bewust dat een bewakingscamera hem tijden de poging had gefilmd. Nadat de politie, die op de bewakingscamera meekeek, hem had gered, droeg de politieautoriteit het beeldmateriaal over aan de media, die het materiaal publiceerden zonder het gezicht van de verzoeker onherkenbaar te maken. Het EHRM oordeelde dat er geen toepasselijke of voldoende redenen waren voor de directe bekendmaking van het beeldmateriaal door de autoriteiten aan het publiek zonder eerst toestemming van de verzoeker te hebben verkregen of zijn identiteit te verhullen. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Noodzakelijk in een democratische samenleving

Het EHRM heeft bepaald dat "het begrip noodzakelijkheid (...) erop [duidt] dat de inmenging haar grond moet vinden in een dwingende maatschappelijke behoefte en in het bijzonder evenredig moet zijn aan het nagestreefde wettige doel".[114]

113 EHRM, *Peck / Verenigd Koninkrijk*, nr. 44647/98, 28 januari 2003, in het bijzonder punt 85.

114 EHRM, *Leander / Zweden*, nr. 9248/81, 11 juli 1985, punt 58.

Voorbeeld: In *Khelili / Zwitserland*[115] had de politie tijdens een controle bij de verzoekster visitekaartjes aangetroffen met de volgende tekst: "Aardige, mooie vrouw, achterin de dertig, wil een man leren kennen om soms mee uit te gaan en iets te drinken. Tel.: (...)". De verzoekster voerde aan dat de politie na deze ontdekking haar naam in de politieregisters had ingevoerd als prostituee, welk beroep zij consistent ontkende uit te oefenen. De verzoekster verzocht dat het woord "prostituee" werd verwijderd uit de geautomatiseerde registers van de politie. Het EHRM erkende in beginsel dat het bewaren van de persoonsgegevens van een natuurlijke persoon, op grond van het vermoeden dat hij of zij mogelijk opnieuw een strafbaar feit zou gaan plegen, in bepaalde omstandigheden evenredig zou kunnen zijn. In het geval van verzoekster leek het vermoeden van illegale prostitutie echter te vaag en te algemeen en werd dit vermoeden niet ondersteund door concrete feiten, aangezien zij nooit was veroordeeld voor illegale prostitutie, en was er derhalve geen "dwingende maatschappelijke behoefte" in de zin van artikel 8 van het EVRM. Het Hof was van mening dat het aan de autoriteiten was om de juistheid van de opgeslagen gegevens van verzoekster te bewijzen en oordeelde, ook gezien de ernst van de inmenging in de rechten van verzoekster, dat jarenlange bewaring van het woord "prostituee" in de politieregisters niet noodzakelijk was in een democratische samenleving. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Voorbeeld: In *Leander / Zweden*[116] oordeelde het EHRM dat het in het geheim controleren van personen die solliciteren naar een functie die van belang is voor de nationale veiligheid op zichzelf niet in strijd was met de eis dat dit noodzakelijk moest zijn in een democratische samenleving. De bijzondere waarborgen in het nationale recht die de belangen van de betrokkene moesten beschermen – zoals door het nationale parlement of de minister van justitie uitgevoerde controles – leidden tot de conclusie van het EHRM dat het Zweedse systeem om personeel te controleren voldeed aan de eisen van artikel 8, lid 2, van het EVRM. Gelet op de ruime beoordelingsmarge die hem ter beschikking stond, had de Zweedse staat het recht om in de zaak van de verzoekster het nationale belang te laten prevaleren boven de individuele belangen. Het Hof concludeerde dat artikel 8 van het EVRM niet was geschonden.

115 EHRM, *Khelili / Zwitserland*, nr. 16188/07, 18 oktober 2011.

116 EHRM, *Leander / Zweden*, nr. 9248/81, 11 juli 1985, punten 59 en 67.

3.1.2. De voorwaarden voor rechtmatige beperkingen volgens het Handvest

De structuur en de bewoording van het Handvest wijken af van die van het EVRM. In het Handvest wordt niet gesproken van inmenging in gegarandeerde rechten, maar wel bevat het een bepaling inzake beperking(en) op de uitoefening van de in het Handvest erkende rechten en vrijheden.

Volgens artikel 52, lid 1, zijn beperkingen op de uitoefening van de in het Handvest erkende rechten en dientengevolge op het recht op gegevensbescherming, zoals de verwerking van persoonsgegevens, alleen toegestaan indien deze:

- bij wet zijn gesteld; en
- het wezen van het recht op gegevensbescherming eerbiedigen; en
- met inachtneming van het evenredigheidbeginsel 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.

Voorbeeld: In *Volker und Markus Schecke*[117] concludeerde het HvJ-EU dat de Raad en de Commissie, door het opleggen van een verplichting om persoonsgegevens van iedere natuurlijke persoon die de begunstigde was van steun uit [bepaalde landbouwfondsen] te publiceren, zonder dat daarbij een onderscheid wordt gemaakt op basis van relevante criteria, zoals de tijdvakken waarin zij die steun hadden ontvangen, de frequentie, het type en de omvang van de steunverlening, de door het evenredigheidsbeginsel gestelde grenzen hadden overschreden.

117 HvJ-EU, gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert / Land Hessen*, 9 november 2010, punten 89 en 86.

> Om die reden achtte het HvJ-EU het noodzakelijk om bepaalde bepalingen van Verordening (EG) nr. 1290/2005 van de Raad, en Verordening (EG) nr. 259/2008 in haar geheel, nietig te verklaren.[118]

Ondanks de afwijkende bewoording vertonen de voorwaarden voor rechtmatige verwerking in artikel 52, lid 1, van het Handvest sterke gelijkenis met die van artikel 8, lid 2, van het EVRM. De in artikel 52, lid 1, van het Handvest genoemde voorwaarden moeten zelfs worden gezien als overeenstemmend met die van artikel 8, lid 2, van het EVRM, aangezien in de eerste zin van artikel 52, lid 3, van het Handvest wordt bepaald dat "[v]oor zover dit Handvest rechten bevat die corresponderen met rechten welke zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, (...) de inhoud en reikwijdte ervan dezelfde [zijn] als die welke er door genoemd verdrag aan worden toegekend".

De laatste zin van artikel 52, lid 3, bepaalt echter het volgende: "Deze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt". In het kader van een vergelijking tussen artikel 8, lid 2, van het EVRM en de eerste zin van artikel 52, lid 3, van het Handvest kan dit alleen betekenen dat de voorwaarden voor gerechtvaardigde inmenging overeenkomstig artikel 8, lid 2, van het EVRM de minimumvereisten voor de rechtmatige beperking van het recht op gegevensbescherming overeenkomstig het Handvest zijn. Bijgevolg vereist een rechtmatige verwerking van persoonsgegevens krachtens het EU-recht dat ten minste de voorwaarden van artikel 8, lid 2, van het EVRM moeten zijn vervuld; het EU-recht zou echter aanvullende vereisten kunnen omvatten voor specifieke gevallen.

De overeenstemming van het beginsel van rechtmatige verwerking krachtens het EU-recht met de desbetreffende bepalingen van het EVRM wordt verder bevorderd door artikel 6, lid 3, van het VEU, dat bepaalt dat "[d]e grondrechten, zoals zij worden gewaarborgd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (...) als algemene beginselen deel uit [maken] van het recht van de Unie".

118 Verordening (EG) nr. 1290/2005 van de Raad van 21 juni 2005 betreffende de financiering van het gemeenschappelijk landbouwbeleid, PB L 209 van 11.8.2005, blz. 1, en Verordening (EG) nr. 259/2008 van de Commissie van 18 maart 2008 tot vaststelling van uitvoeringsbepalingen van Verordening (EG) nr. 1290/2005 van de Raad met betrekking tot de bekendmaking van informatie over de begunstigden van financiële middelen uit het Europees Landbouwgarantiefonds (ELGF) en het Europees Landbouwfonds voor Plattelandsontwikkeling (ELFPO), PB L 76 van 19.3.2008, blz. 28.

3.2. Het beginsel van doelbepaling en -binding

Belangrijkste punten

- Het doeleinde van de verwerking van gegevens moet zichtbaar zijn omschreven voordat de verwerking van start gaat.
- Volgens het EU-recht moet het doeleinde van de verwerking expliciet worden gedefinieerd; in het RvE-recht wordt dit overgelaten aan het nationale recht.
- Verwerking voor onbepaalde doeleinden is niet in overeenstemming met de gegevensbeschermingswetgeving.
- Voor verder gebruik voor andere doeleinden is een aanvullende rechtsgrond nodig als het nieuwe doeleinde van de verwerking niet verenigbaar is met het oorspronkelijke doeleinde.
- Overdracht van gegevens aan derden is een nieuw doeleinde waarvoor een aanvullende rechtsgrondslag nodig is.

In essentie houdt het beginsel van doelbepaling en -binding in dat de rechtmatigheid van de verwerking van persoonsgegevens afhankelijk zal zijn van het doeleinde van de verwerking.[119] Het doeleinde moet zijn gespecificeerd en de voor de verwerking verantwoordelijke moet dit doeleinde duidelijk hebben gemaakt voordat de gegevensverwerking van start gaat.[120] In **het EU-recht** moet dit gebeuren in een verklaring, of met andere woorden een kennisgeving, aan de desbetreffende toezichthoudende autoriteit, of ten minste in interne documentatie die de voor de verwerking verantwoordelijke beschikbaar moet stellen aan de toezichthoudende autoriteit voor inspectie en die voor de betrokkene toegankelijk moet zijn.

De verwerking van persoonsgegevens voor onbepaalde doeleinden en/of onbeperkte doeleinden, is onrechtmatig.

Elk nieuw doeleinde van de verwerking van gegevens moet zijn eigen specifieke rechtsgrondslag hebben en mag niet worden gebaseerd op het feit dat de gegevens oorspronkelijk waren verworven of verwerkt voor een ander rechtmatig doeleinde. Op haar beurt is elke rechtmatige verwerking beperkt tot het oorspronkelijk gespecificeerde doeleinde en zal voor een nieuw doeleinde van de verwerking een afzonderlijke, nieuwe rechtsgrondslag nodig zijn. Met name zal zorgvuldig moeten

119 Verdrag 108, artikel 5, onder b), en richtlijn gegevensbescherming, artikel 6, lid 1, onder b).

120 Zie ook Groep gegevensbescherming artikel 29 (2013), *Advies 03/2013 over doelbinding*, WP 203, Brussel, 2 april 2013.

worden overwogen of gegevens mogen worden meegedeeld aan derden, aangezien dit doorgaans een nieuw doeleinde zal vormen en derhalve een nieuwe rechtsgrondslag vereist die niet dezelfde is als de rechtsgrondslag voor het verzamelen van de gegevens.

Voorbeeld: Een luchtvaartmaatschappij verzamelt in het kader van het maken van boekingen gegevens van haar passagiers om de vlucht naar behoren te laten verlopen. De luchtvaartmaatschappij zal gegevens nodig hebben over: de stoelnummers van de passagiers, specifieke fysieke beperkingen, bijvoorbeeld of iemand een rolstoel nodig heeft, en specifieke voedingswensen, zoals koosjer of halal voedsel. Als luchtvaartmaatschappijen worden gevraagd om deze gegevens, die onderdeel zijn van de PNR, over te dragen aan de immigratieautoriteiten van de luchthaven waar het vliegtuig landt, zullen deze gegevens vervolgens worden gebruikt voor immigratie- en controledoeleinden, die afwijken van het doeleinde waarvoor de gegevens oorspronkelijk waren verzameld. Voor de overdracht van deze gegevens aan een immigratieautoriteit is daarom een nieuwe en afzonderlijke rechtsgrondslag nodig.

Bij het omschrijven van het toepassingsgebied en de grenzen van een specifiek doeleinde wordt in zowel Verdrag 108 als de richtlijn gegevensbescherming toevlucht genomen tot het begrip "verenigbaar": het gebruik van gegevens voor verenigbare doeleinden is toegestaan op basis van de oorspronkelijke rechtsgrond. Het begrip "verenigbaar" wordt echter niet gedefinieerd en staat open voor interpretatie per afzonderlijk geval.

Voorbeeld: De verkoop van klantgegevens van Zonneschijn B.V., die het bedrijf heeft verworven in het kader van zijn klantenbeheer, aan een in direct marketing gespecialiseerd bedrijf, Maanlicht B.V., dat deze gegevens wil gebruiken in marketingcampagnes van derde ondernemingen, is een nieuw doeleinde dat onverenigbaar is met het klantenbeheer, het oorspronkelijk doeleinde van Zonneschijn B.V. voor het verzamelen van de klantgegevens. De verkoop van de gegevens aan Maanlicht B.V. vereist derhalve een eigen, afzonderlijke rechtsgrondslag.

Het gebruik door Zonneschijn B.V. van haar klantgegevens voor marketingdoeleinden, d.w.z. het verzenden van reclameboodschappen over haar eigen producten aan haar eigen klanten, wordt daarentegen algemeen aanvaard als een verenigbaar doeleinde.

In de richtlijn gegevensbescherming wordt uitdrukkelijk bepaald dat de "[v]erdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden (...) niet als onverenigbaar [wordt] beschouwd, mits de lidstaten passende garanties bieden".[121]

Voorbeeld: Zonneschijn B.V. heeft gegevens over haar klanten verzameld en opgeslagen. Verder gebruik van deze gegevens door Zonneschijn B.V. voor de statistische analyse van het koopgedrag van haar klanten is toegestaan, aangezien dit een statistisch en derhalve verenigbaar doeleinde is. Een aanvullende rechtsgrondslag, zoals toestemming van de betrokkenen, is niet nodig.

Als dezelfde gegevens zouden worden doorgegeven aan een derde, Sterrenhemel B.V., voor uitsluitend statistische doeleinden, zou deze doorgifte zijn toegestaan zonder aanvullende rechtsgrondslag, maar alleen op voorwaarde dat passende waarborgen zijn ingevoerd, zoals het onherkenbaar maken van de identiteit van de betrokkene, omdat identiteiten over het algemeen niet nodig zijn voor statistische doeleinden.

3.3. Beginselen inzake de kwaliteit van de gegevens

Belangrijkste punten

- De beginselen inzake de kwaliteit van de gegevens moeten door de voor de verwerking verantwoordelijke worden toegepast in alle verwerkingen.
- Het beginsel van beperkte bewaring van gegevens maakt het noodzakelijk om gegevens uit te wissen zodra ze niet langer noodzakelijk zijn voor de doeleinden waarvoor ze zijn verzameld.
- Vrijstellingen van het beginsel van beperkte bewaring moeten bij wet zijn gesteld en vergezeld gaan van bijzondere waarborgen voor de bescherming van betrokkenen.

121 Een voorbeeld van dergelijke nationale bepalingen is de Oostenrijkse gegevensbeschermingswet (*Datenschutzgesetz*), Bundesgesetzblatt I nr. 165/1999, lid 46.

3.3.1. Het beginsel van relevantie van de gegevens

Alleen die gegevens worden verwerkt die "toereikend, ter zake dienend en niet bovenmatig (...) zijn, uitgaande van de doeleinden waarvoor zij worden verzameld of waarvoor zij vervolgens worden verwerkt".[122] De categorieën gegevens die worden gekozen voor verwerking moeten noodzakelijk zijn om het verklaarde algemene doel van de verwerkingen te verwezenlijken, en een voor de verwerking verantwoordelijke moet de verzameling van gegevens strikt beperken tot de informatie die direct relevant is voor het specifieke doel dat met de verwerking wordt nagestreefd.

In de hedendaagse samenleving is aan het beginsel van relevantie van de gegevens nog een extra overweging verbonden: door speciale privacyverbeterende technologieën toe te passen kan het gebruik van persoonsgegevens soms helemaal worden vermeden, of worden beperkt tot alleen gepseudonimiseerde gegevens, waardoor privacyvriendelijke oplossingen mogelijk worden. Dit is met name passend in uitgebreidere verwerkingssystemen.

Voorbeeld: Een gemeentebestuur biedt regelmatige gebruikers van het openbaarvervoerssysteem van de gemeente tegen een bepaalde vergoeding een chipkaart aan. De naam van de gebruiker wordt vermeld op het oppervlak van de kaart en ook in elektronische vorm in de chip. Steeds wanneer gebruik wordt gemaakt van een bus of een tram, moet de chipkaart voor het in het voertuig geïnstalleerde afleesapparaat worden gehouden. De gegevens die het apparaat afleest worden elektronisch gecontroleerd in een databank met de namen van de personen die de reiskaart hebben aangeschaft.

Dit systeem voldoet niet optimaal aan het beginsel van relevantie van de gegevens: of iemand gebruik mag maken van vervoersmiddelen kan worden gecontroleerd zonder de persoonsgegevens op de chip van de kaart te vergelijken met een databank. Daarvoor zou het bijvoorbeeld volstaan om een in de chip van de kaart geïntegreerde speciale elektronische code te laten aflezen door het afleesapparaat, waardoor zou worden bevestigd of de kaart geldig is of niet. In een dergelijk systeem zou niet worden vastgelegd wie welk vervoersmiddel gebruikt op welk tijdstip. Er zouden geen persoonsgegevens worden verzameld, wat de optimale oplossing is in de zin van het beginsel van

122 Verdrag 108, artikel 5, onder c), en richtlijn gegevensbescherming, artikel 6, lid 1, onder c).

relevantie, omdat dit beginsel resulteert in de verplichting om de gegevensverzameling te minimaliseren.

3.3.2. Het beginsel van nauwkeurigheid van de gegevens

Een voor de verwerking verantwoordelijke bij wie persoonlijke informatie berust mag die informatie niet gebruiken zonder stappen te ondernemen die er met redelijke zekerheid voor zorgen dat de gegevens nauwkeurig en actueel zijn.

De verplichting om voor de nauwkeurigheid van de gegevens te zorgen moet worden gezien in de context van het doel van de gegevensverwerking.

Voorbeeld: Een bedrijf dat meubels verkoopt heeft de identiteiten en de adressen van klanten verzameld om hen een rekening te kunnen sturen. Zes maanden later wil hetzelfde bedrijf een marketingcampagne beginnen en daarvoor contact opnemen met voormalige klanten. Om deze voormalige klanten te kunnen bereiken, wil het bedrijf inzage in het nationale register van burgerlijke stand, dat waarschijnlijk geactualiseerde adresgegevens bevat omdat burgers wettelijk verplicht zijn om het register in kennis te stellen van hun feitelijke adres. De toegang tot de gegevens in dit register is beperkt tot personen en entiteiten die een gerechtvaardigde reden kunnen opgeven.

In deze situatie kan het bedrijf, om te onderbouwen dat het het recht heeft om nieuwe adresgegevens van al zijn voormalige klanten uit het nationale register te verzamelen, niet als argument aanvoeren dat de gegevens nauwkeurig en actueel moeten zijn. De gegevens waren verzameld om facturen te kunnen sturen; voor dit doel is het adres op het moment van de verkoop relevant. Er is geen rechtsgrondslag voor het verzamelen van nieuwe adresgegevens, aangezien marketing geen belang is dat voorrang heeft op het recht op gegevensbescherming en derhalve geen rechtvaardiging vormt voor het verkrijgen van toegang tot de gegevens in het register.

Ook kunnen er gevallen zijn waarin het actualiseren van opgeslagen gegevens wettelijk is verboden omdat het doel van de opslag van de gegevens in essentie was om gebeurtenissen te documenteren.

Voorbeeld: Een protocol voor een medische handeling mag niet worden gewijzigd, of anders gezegd 'geactualiseerd', ook niet als in het protocol genoemde bevindingen later verkeerd blijken te zijn. In dergelijke omstandigheden mogen uitsluitend aanvullingen op de opmerkingen in het protocol worden toegevoegd, zolang ze duidelijk worden gemarkeerd als in een later stadium toegevoegde bijdragen.

Anderzijds zijn er situaties waarin het regelmatig controleren van de nauwkeurigheid van de gegevens, met inbegrip van het actualiseren ervan, een absolute noodzaak is vanwege de potentiële schade die kan worden veroorzaakt voor de betrokkene als de gegevens onnauwkeurig zouden zijn.

Voorbeeld: Als iemand een contract wil sluiten met een bancaire instelling, zal de bank doorgaans de kredietwaardigheid van de toekomstige klant controleren. Voor dit doel zijn speciale databanken beschikbaar met gegevens over de kredietgeschiedenis van particuliere personen. Indien een dergelijke databank onjuiste of verouderde gegevens over een persoon bevat, kan deze persoon met ernstige problemen worden geconfronteerd. Voor de verwerking verantwoordelijken van dergelijke databanken moeten daarom bijzondere inspanningen verrichten om het beginsel van nauwkeurigheid te volgen.

Voorts mogen gegevens die geen betrekking hebben op feiten, maar op verdenkingen, zoals in strafrechtelijke onderzoeken, worden verzameld en opgeslagen zolang de voor de verwerking verantwoordelijke een rechtsgrondslag heeft voor de verzameling van deze gegevens en de vorming van de verdenking voldoende kan worden gerechtvaardigd.

3.3.3. Het beginsel van beperkte bewaring van gegevens

Artikel 6, lid 1, onder e), van de richtlijn gegevensbescherming, en ook, op vergelijkbare wijze, artikel 5, onder e), van Verdrag 108, verplicht de lidstaten om ervoor te zorgen dat persoonsgegevens "in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer mogen worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, noodzakelijk is". De gegevens moeten daarom worden verwijderd wanneer de doeleinden zijn verwezenlijkt.

In zaak *S. en Marper* concludeerde het EHRM dat de kernbeginselen van de relevante instrumenten van de Raad van Europa en de wet en praktijken van de andere overeenkomstsluitende partijen vereisen dat de bewaring van gegevens evenredig is met het doeleinde van de gegevensverzameling en moet worden beperkt in de tijd, in het bijzonder in de politiesector.[123]

De tijdsbeperking voor de opslag van persoonsgegevens is echter alleen van toepassing op gegevens die worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren. De rechtmatige opslag van gegevens die niet langer noodzakelijk zijn zou derhalve kunnen worden bereikt door anonimisering van de gegevens.

De bewaring van gegevens voor toekomstige wetenschappelijke, historische of statistische doeleinden is uitdrukkelijk uitgezonderd van het beginsel van beperkte bewaring van gegevens als vervat in de richtlijn gegevensbescherming.[124] Een dergelijk(e) gecontinueerd(e) opslag en gebruik van persoonsgegevens moet evenwel vergezeld gaan van in het nationaal recht opgenomen bijzondere waarborgen.

3.4. Het beginsel van eerlijke verwerking

Belangrijkste punten

- Eerlijke verwerking houdt in dat de verwerking transparant is, met name voor betrokkenen.
- Voor de verwerking verantwoordelijken moeten betrokkenen, voordat ze hun gegevens verwerken, ten minste het doeleinde van de verwerking en de identiteit en het adres van de voor de verwerking verantwoordelijke meedelen.
- Tenzij dit specifiek wordt toegestaan door de wet, mag er geen geheime of heimelijke verwerking van persoonsgegevens plaatsvinden.
- Betrokkenen hebben altijd het recht om hun gegevens in te zien wanneer deze worden verwerkt.

123 EHRM, *S. en Marper / Verenigd Koninkrijk*, nrs. 30562/04 en 30566/04, 4 december 2008; zie ook, bijvoorbeeld, EHRM, *M.M. / Verenigd Koninkrijk*, nr. 24029/07, 13 november 2012.

124 Richtlijn gegevensbescherming, artikel 6, lid 1, onder e).

Het beginsel van eerlijke verwerking reguleert voornamelijk de verhouding tussen de voor de verwerking verantwoordelijke en de betrokkene.

3.4.1. Transparantie

Dit beginsel legt de voor de verwerking verantwoordelijke een verplichting op om betrokkenen op de hoogte te houden van de wijze waarop hun gegevens worden gebruikt.

> Voorbeeld: In de zaak *Haralambie / Roemenië*[125] had de verzoeker verzocht om inzage in het dossier dat de geheime dienst over hem had opgeslagen, maar was zijn verzoek pas na vijf jaar ingewilligd. Het EHRM herhaalde dat natuurlijke personen die het voorwerp waren van persoonlijke dossiers die door overheidsautoriteiten werden bewaard een vitaal belang hadden bij het hebben van toegang tot die dossiers. De autoriteiten hadden de plicht om te voorzien in een effectieve procedure voor het verkrijgen van toegang tot deze informatie. Het EHRM stelde dat noch de kwantiteit van de overgedragen dossiers, noch de tekortkomingen in het archiveringssysteem een vertraging van vijf jaar bij het inwilligen van het verzoek van verzoeker om zijn dossiers te kunnen inzien, rechtvaardigden. De autoriteiten hadden verzoeker geen effectieve en toegankelijke procedure ter beschikking gesteld om hem in staat te stellen binnen een redelijke termijn inzage in zijn persoonlijke dossier te krijgen. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Verwerkingen moeten aan de betrokkenen worden uitgelegd op een gemakkelijk toegankelijke manier die ervoor zorgt dat ze begrijpen wat er met hun gegevens gebeurt. Ook heeft een betrokkene het recht om op verzoek door de voor de verwerking verantwoordelijke te worden meegedeeld of zijn of haar gegevens worden verwerkt, en zo ja, welke gegevens worden verwerkt.

3.4.2. Vertrouwen opbouwen

Voor de verwerking verantwoordelijken moeten, ten behoeve van de betrokkenen en ten behoeve van het algemene publiek, documenteren dat ze gegevens op een rechtmatige en transparante wijze verwerken. Verwerkingen mogen niet in het geheim worden uitgevoerd en mogen geen onvoorzienbare negatieve gevolgen hebben. Voor de verwerking verantwoordelijken moeten ervoor zorgen dat klanten

125 EHRM, *Haralambie / Roemenië*, nr. 21737/03, 27 oktober 2009.

of burgers worden geïnformeerd over het gebruik van hun persoonsgegevens. Voorts moeten voor de verwerking verantwoordelijken, voor zover mogelijk, op een zodanige wijze handelen dat ze prompt tegemoetkomen aan de wensen van de betrokkene, vooral wanneer zijn of haar toestemming de rechtsgrondslag voor de gegevensverwerking vormt.

Voorbeeld: In de zaak *K.H. en anderen / Slowakije*[126] waren de verzoeksters acht vrouwen van Roma-afkomst die in twee ziekenhuizen in het oosten van Slowakije waren behandeld tijdens hun zwangerschap en de bevalling. Naderhand kon geen van de vrouwen meer zwanger worden, ondanks herhaalde pogingen daartoe. De nationale rechtbanken hadden verordend dat de ziekenhuizen de verzoeksters en hun vertegenwoordigers inzage in de medische dossiers moesten bieden en daarbij de mogelijkheid kregen om handgeschreven aantekeningen te maken, maar hadden hun verzoek om fotokopieën te maken verworpen met het argument dat potentieel misbruik moest worden voorkomen. De positieve verplichtingen van de staat uit hoofde van artikel 8 van het EVRM omvatte noodzakelijkerwijs een verplichting om kopieën van de dossiers over de betrokkene beschikbaar te stellen. Het was aan de staat om de regelingen voor het kopiëren van persoonlijke dossiers te bepalen of, indien passend, om zwaarwegende redenen aan te voeren om dit niet toe te staan. In het geval van de verzoeksters hadden de nationale rechtbanken het verbod op het maken van kopieën van medische dossiers voornamelijk gerechtvaardigd op grond van de noodzaak om de desbetreffende informatie te beschermen tegen misbruik. Het EHRM kon echter niet zien hoe de verzoeksters, die in elk geval inzage hadden gekregen in hun volledige medische dossiers, misbruik zouden kunnen maken van informatie over henzelf. Bovendien kon het risico van een dergelijk misbruik op andere wijze worden voorkomen dan door de verzoeksters kopieën van de dossiers te ontzeggen, bijvoorbeeld door het aantal personen dat recht op toegang tot de dossiers had te beperken. De staat had verzuimd om het bestaan van voldoende zwaarwegende redenen voor het weigeren aan de verzoeksters van effectieve toegang tot informatie over hun gezondheid aan te tonen. Het Hof concludeerde dat er een inbreuk op artikel 8 had plaatsgevonden.

126 EHRM, *K.H. en anderen / Slowakije*, nr. 32881/04, 6 november 2009.

Met betrekking tot internetdiensten moeten de eigenschappen van de gegevensverwerkingssystemen het voor betrokkenen mogelijk maken om daadwerkelijk te begrijpen wat er met hun gegevens gebeurt.

Eerlijke verwerking betekent ook dat voor de verwerking verantwoordelijken bereid moeten zijn om verder te gaan dan de wettelijke minimumeisen voor de dienst aan de betrokkene indien de rechtmatige belangen van de betrokkene dat noodzakelijk maken.

3.5. Het verantwoordingsbeginsel

Belangrijkste punten

- Het verantwoordingsbeginsel vereist dat voor de verwerking verantwoordelijken actieve maatregelen ten uitvoer leggen om de bescherming van persoonsgegevens in hun verwerkingen te bevorderen en te waarborgen.
- Voor de verwerking verantwoordelijken zijn ervoor verantwoordelijk dat hun verwerkingen voldoen aan de gegevensbeschermingswetgeving.
- Voor de verwerking verantwoordelijken moeten te allen tijde aan de betrokkenen, het algemene publiek en de toezichthoudende autoriteiten kunnen aantonen dat de gegevensbeschermingsbepalingen worden nageleefd.

De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) heeft in 2013 privacyrichtsnoeren vastgesteld waarin wordt bepaald dat voor de verwerking verantwoordelijken een belangrijke rol hebben bij het in de praktijk laten werken van gegevensbescherming. In de richtsnoeren is een verantwoordingsbeginsel ontwikkeld in de zin dat "een voor de verwerking verantwoordelijke verantwoording moet afleggen over de naleving van maatregelen die uitvoering geven aan de hierboven omschreven [materiële] beginselen".[127]

Terwijl in Verdrag 108 niet wordt verwezen naar de verantwoordingsplicht van voor de verwerking verantwoordelijken en dit onderwerp grotendeels aan de nationale wetgeving wordt overgelaten, bepaalt artikel 6, lid 2, van de richtlijn gegevensbescherming dat de voor de verwerking verantwoordelijke de plicht heeft om voor de

127 OESO (2013), Guidelines on governing the Protection of Privacy and transborder flows of personal data, artikel 14.

naleving van de in lid 1 genoemde beginselen inzake de kwaliteit van gegevens te zorgen.

Voorbeeld: Een voorbeeld van wetgeving waarin het verantwoordingsbeginsel wordt onderstreept is de wijziging[128] van de e-privacyrichtlijn (Richtlijn 2002/58/EG) van 2009. Volgens artikel 4 in zijn gewijzigde vorm legt de richtlijn een verplichting op om een beveiligingsbeleid toe te passen, namelijk om ervoor te zorgen dat er "een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens". Wat betreft de beveiligingsbepalingen van deze richtlijn heeft de wetgever dus besloten dat er een expliciete eis moest worden ingevoerd om een beveiligingsbeleid te hebben en uit te voeren.

Volgens het advies van de Groep gegevensbescherming artikel 29[129] is de essentie van verantwoording de verplichting van de voor de verwerking verantwoordelijke om:

- maatregelen te nemen die – onder normale omstandigheden – waarborgen dat de gegevensbeschermingsregels worden nageleefd in de context van verwerkingen; en

- over documenten te beschikken die aan de betrokkenen en aan de toezichthoudende autoriteiten aantonen welke maatregelen zijn genomen om naleving van de gegevensbeschermingsregels te verwezenlijken.

Het verantwoordingsbeginsel vereist derhalve van voor de verwerking verantwoordelijken dat ze actief laten zien dat ze deze regels naleven en daar niet mee wachten tot ze door betrokkenen of toezichthoudende autoriteiten op tekortkomingen worden gewezen.

128 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, PB L 337 van 18.12.2009, blz. 11.

129 Groep gegevensbescherming artikel 29, *Advies 3/2010 over het verantwoordingsbeginsel*, WP 173, Brussel, 13 juli 2010.

4

De regels van de Europese gegevensbeschermingswetgeving

EU	Behandelde onderwerpen	RvE
Regels voor de rechtmatige verwerking van niet-gevoelige gegevens		
Richtlijn gegevensbescherming, artikel 7, onder a)	**Toestemming**	Aanbeveling inzake profilering, artikel 3.4, onder b), en artikel 3.6
Richtlijn gegevensbescherming, artikel 7, onder b)	**(Pre-)contractuele relatie**	Aanbeveling inzake profilering, artikel 3.4, onder b)
Richtlijn gegevensbescherming, artikel 7, onder c)	**Wettelijke plichten van de voor de verwerking verantwoordelijke**	Aanbeveling inzake profilering, artikel 3.4, onder a)
Richtlijn gegevensbescherming, artikel 7, onder d)	**Vitale belangen van de betrokkene**	Aanbeveling inzake profilering, artikel 3.4, onder b)
Richtlijn gegevensbescherming, artikel 7, onder e), en artikel 8, lid 4 HvJ-EU, zaak C-524/06, *Huber / Bondsrepubliek Duitsland*, 16 december 2008	**Algemeen belang en uitoefening van officiële autoriteit**	Aanbeveling inzake profilering, artikel 3.4, onder b)
Richtlijn gegevensbescherming, artikel 7, onder f), en artikel 8, leden 2 en 3 HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24 november 2011	**Rechtmatige belangen van anderen**	Aanbeveling inzake profilering, artikel 3.4, onder b)

EU	Behandelde onderwerpen	RvE
Regels voor de rechtmatige verwerking van gevoelige gegevens		
Richtlijn gegevensbescherming, artikel 8, lid 1	Algemeen verbod op verwerking	Verdrag 108, artikel 6
Richtlijn gegevensbescherming, artikel 8, leden 2 t/m 4	Uitzonderingen op het algemene verbod	Verdrag 108, artikel 6
Richtlijn gegevensbescherming, artikel 8, lid 5	Verwerking van gegevens over (strafrechtelijke) veroordelingen	Verdrag 108, artikel 6
Richtlijn gegevensbescherming, artikel 8, lid 7	Verwerking van identificatienummers	
Regels voor beveiligde verwerking		
Richtlijn gegevensbescherming, artikel 17	Verplichting om voor beveiligde verwerking te zorgen	Verdrag 108, artikel 7 EHRM, *I. / Finland*, nr. 20511/03, 17 juli 2008
E-privacyrichtlijn, artikel 4, lid 2	Kennisgevingen van inbreuken	
Richtlijn gegevensbescherming, artikel 16	Verplichting tot vertrouwelijkheid	
Regels voor de transparantie van de verwerking		
	Transparantie in het algemeen	Verdrag 108, artikel 8, onder a)
Richtlijn gegevensbescherming, artikel en 10 en lid 11	Informatie	Verdrag 108, artikel 8, onder a)
Richtlijn gegevensbescherming, artikel en 10 en lid 11	Uitzonderingen op de informatieverplichting	Verdrag 108, artikel 9
Richtlijn gegevensbescherming, artikel en 18 en 19	Kennisgeving	Aanbeveling inzake profilering, artikel 9.2, onder a)
Regels voor het bevorderen van de naleving		
Richtlijn gegevensbescherming, artikel 20	Voorafgaande controle	
Richtlijn gegevensbescherming, artikel 18, lid 2	Gegevensbeschermingsfunctionarissen	Aanbeveling inzake profilering, artikel 8.3
Richtlijn gegevensbescherming, artikel 27	Gedragscodes	

Beginselen zijn noodzakelijkerwijs van algemene aard. De toepassing ervan op concrete situaties laat een zekere ruimte voor interpretatie en voor de keuze van de middelen. In **het RVE-recht** wordt het aan de partijen bij Verdrag 108 overgelaten om deze ruimte voor interpretatie in hun nationale wetgeving in te vullen. In **het EU-recht** is de situatie anders: Bij de invoering van gegevensbescherming in de interne markt werd het noodzakelijk geacht om reeds op EU-niveau meer gedetailleerde regels vast te stellen om het niveau van gegevensbescherming in de nationale wetgevingen van de lidstaten te harmoniseren. In de richtlijn gegevensbescherming is, op basis van de in artikel 6 beschreven beginselen, een laag van gedetailleerde regels vastgelegd die in het nationale recht nauwgezet ten uitvoer moeten worden gelegd. De volgende opmerkingen over gedetailleerde gegevensbeschermingsregels op Europees niveau hebben dan ook voornamelijk betrekking op het EU-recht.

4.1. Regels voor de rechtmatigheid van de verwerking

Belangrijkste punten

- Persoonsgegevens kunnen rechtmatig worden verwerkt indien:
  - de verwerking is gebaseerd op toestemming van de betrokkene; of
  - vitale belangen van betrokkenen de verwerking van hun gegevens vereisen; of
  - rechtmatige belangen van anderen de reden voor de verwerking zijn, maar alleen zolang het belang van bescherming van de grondrechten van de betrokkenen niet prevaleert.
- Voor de rechtmatige verwerking van gevoelige persoonsgegevens gelden speciale, strengere regels.

De richtlijn gegevensbescherming bevat twee verschillende stelsels van regels voor de rechtmatige verwerking van gegevens: één voor niet-gevoelige gegevens, in artikel 7, en één voor gevoelige gegevens, in artikel 8.

4.1.1. Rechtmatige verwerking van niet-gevoelige gegevens

Hoofdstuk II van Richtlijn 95/46/EG, getiteld "Algemene voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens", bepaalt dat, behoudens de uitzonderingen die artikel 13 toestaat, alle verwerkingen van persoonsgegevens in de eerste plaats moeten voldoen aan de beginselen inzake de kwaliteit van de gegevens als beschreven in artikel 6 van de richtlijn gegevensbescherming, en in de tweede plaats aan ten minste één van de in artikel 7 genoemde criteria voor de rechtmatigheid van gegevensverwerkingen.[130] Dit hoofdstuk beschrijft de gronden voor de rechtmatige verwerking van niet-gevoelige persoonsgegevens.

Toestemming

In **het RvE-recht** wordt toestemming niet genoemd in artikel 8 van het EVRM of in Verdrag 108. Wel wordt dit begrip gebruikt in de jurisprudentie van het EHRM en in diverse aanbevelingen van de RvE. In **het EU-recht** is toestemming als grondslag voor een rechtmatige gegevensverwerking stevig verankerd in artikel 7, onder a), van de richtlijn gegevensbescherming en wordt het ook uitdrukkelijk genoemd in artikel 8 van het Handvest.

Contractuele relatie

Een andere rechtsgrondslag voor de rechtmatige verwerking van persoonsgegevens in **het EU-recht**, die is vastgelegd in artikel 7, onder b), van de richtlijn gegevensbescherming, is dat "de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene". Deze bepaling is ook van toepassing op precontractuele relaties. Een voorbeeld: een partij is van plan een contract te sluiten, maar heeft dat nog niet gedaan, mogelijk omdat er nog enkele controles moeten worden uitgevoerd. Als een partij met het oog hierop gegevens moet verwerken, is deze verwerking rechtmatig zolang de verwerking nodig is "voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene".

130 HvJ-EU, gevoegde zaken C-465/00, C-138/01 en C-139/01 *Österreichischer Rundfunk en anderen*, 20 mei 2003, punt 65; HvJ-EU, C-524/06, *Huber / Bondsrepubliek Duitsland*, 16 december 2008, punt 48; HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24 november 2011, punt 26.

In **het RvE-recht** wordt "de bescherming van de rechten en vrijheden van anderen" genoemd in artikel 8, lid 2, van het EVRM als een reden voor rechtmatige inmenging in het recht op gegevensbescherming.

Wettelijke plichten van de voor de verwerking verantwoordelijke

In **het EU-recht** wordt vervolgens expliciet een ander criterium genoemd voor het rechtmatig maken van gegevensverwerkingen, namelijk dat "de verwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de voor de verwerking verantwoordelijke onderworpen is" (artikel 7, onder c), van de richtlijn gegevensbescherming). Deze bepaling heeft betrekking op voor de verwerking verantwoordelijken in de private sector; de wettelijke verplichting van voor de verwerking verantwoordelijken in de publieke sector valt onder artikel 7, onder e), van de richtlijn gegevensbescherming. Er zijn veel gevallen waarin voor de verwerking verantwoordelijken in de private sector wettelijk verplicht zijn om gegevens over anderen te verwerken; zo hebben artsen en ziekenhuizen de wettelijke plicht om gegevens over de behandeling van hun patiënten gedurende een aantal jaren te bewaren, moeten werkgevers gegevens over hun werknemers verwerken in verband met de sociale zekerheid en belastingen en moeten ondernemingen gegevens over hun klanten verwerken om belastingredenen.

In het kader van de verplichte overdracht van passagiersgegevens door luchtvaartmaatschappijen aan buitenlandse immigratiecontroleautoriteiten rees de vraag of een wettelijk verplichting uit hoofde van *buitenlandse* wetgeving al dan niet een rechtmatige grondslag krachtens het EU-recht zou kunnen vormen om gegevens te verwerken (deze kwestie wordt nader besproken in paragraaf 6.2).

In **het RvE-recht** dienen de wettelijke verplichtingen van de voor de verwerking verantwoordelijke als grondslag voor de rechtmatige verwerking van gegevens. Zoals reeds eerder is opgemerkt, vormen de wettelijke verplichtingen van een voor de verwerking verantwoordelijke in de private sector maar één specifiek geval van rechtmatige belangen van anderen als bedoeld in artikel 8, lid 2, van het EVRM. Het bovenstaande voorbeeld is derhalve ook relevant voor het RvE-recht.

Vitale belangen van de betrokkene

In **het EU-recht** bepaalt artikel 7, onder d), van de **richtlijn gegevensbescherming** dat de verwerking van persoonsgegevens rechtmatig is als "de verwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene". Deze vitale

belangen, die nauw verband houden met het overleven van de betrokkene, zouden bijvoorbeeld de grondslag kunnen vormen voor het rechtmatig gebruik van gezondheidsgegevens over vermiste personen.

In **het RvE-recht** worden vitale belangen van de betrokkene niet genoemd in artikel 8 van het EVRM als reden voor rechtmatige inmenging in het recht op gegevensbescherming. In enkele aanbevelingen van de RvE, die Verdrag 108 op specifieke gebieden aanvullen, worden de vitale belangen van betrokkene echter uitdrukkelijk genoemd als grondslag voor een rechtmatige verwerking.[131] Vitale belangen van de betrokkene worden duidelijk geacht geïmpliceerd te zijn in de redenen die gegevensverwerking rechtvaardigen: de bescherming van grondrechten mag nooit de vitale belangen van de beschermde persoon in gevaar brengen.

Algemeen belang en uitoefening van officiële autoriteit

Gezien de vele mogelijke manieren om het openbaar bestuur te organiseren, bepaalt artikel 7, onder e), van de **richtlijn gegevensbescherming** dat persoonsgegevens rechtmatig mogen worden verwerkt indien "de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de voor de verwerking verantwoordelijke of de derde aan wie de gegevens worden verstrekt, is opgedragen (...)".[132]

Voorbeeld: In *Huber / Bondsrepubliek Duitsland*[133] had de heer Huber, een in Duitsland wonende onderdaan van Oostenrijk, het Federale Bureau voor immigratie en vluchtelingen verzocht gegevens over hem te verwijderen uit het centrale register van buitenlandse onderdanen (*Ausländerzentralregister* – hierna "het AZR"). Dit register, dat persoonsgegevens bevat van niet-Duitse EU-burgers die langer dan drie maanden in Duitsland verblijven, wordt gebruikt voor statistische doeleinden en door wetshandhavings- en gerechtelijke autoriteiten met het oog op het onderzoeken en vervolgen van criminele activiteiten of activiteiten die een bedreiging voor de openbare veiligheid vormen. De doorverwijzende rechtbank vroeg of de verwerking van persoonsgegevens in een register als het betreffende centrale register, waartoe ook andere overheidsautoriteiten toegang hebben, verenigbaar was met het EU-recht, aangezien er niet een dergelijk register bestond voor Duitse onderdanen.

131 Aanbeveling inzake profilering, artikel 3.4, onder b).

132 Zie ook de richtlijn gegevensbescherming, overweging 32.

133 HvJ-EU, zaak C-524/06, *Huber / Bondsrepubliek Duitsland*, 16 december 2008.

Het HvJ-EU oordeelde eerstens dat volgens artikel 7, onder e), van de richtlijn gegevensbescherming persoonsgegevens alleen rechtmatig mogen worden verwerkt indien dit nodig is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag.

Volgens het Hof "kan het begrip noodzakelijkheid zoals dit naar voren komt uit artikel 7, sub e, van richtlijn 95/46 (...) niet een inhoud hebben die verschilt van lidstaat tot lidstaat. Het gaat bijgevolg om een autonoom begrip van het gemeenschapsrecht, dat moet worden uitgelegd op een wijze die volledig beantwoordt aan het doel van de richtlijn zoals omschreven in artikel 1, lid 1".[134]

Het Hof merkte op dat het recht op vrij verkeer van een burger van de Unie op het grondgebied van een lidstaat waarvan hij of zij geen onderdaan is, niet onvoorwaardelijk is, maar kan worden gebonden aan beperkingen en voorwaarden die in het Verdrag en de maatregelen ter uitvoering daarvan zijn vastgesteld. Als het voor een lidstaat dus in principe rechtmatig is om een register als het AZR te gebruiken ter ondersteuning van de autoriteiten die verantwoordelijk zijn voor de toepassing van de wetgeving inzake het recht op verblijf, mag een dergelijk register geen andere informatie bevatten dan die welke noodzakelijk is om dat specifieke doel te verwezenlijken. Het Hof concludeerde dat het bedoelde systeem voor de verwerking van persoonsgegevens voldoet aan het EU-recht als het uitsluitend de gegevens bevat die noodzakelijk zijn voor de uitvoering van de desbetreffende wetgeving en als de centrale aard ervan de toepassing van de wetgeving doeltreffender maakt. De nationale rechtbank moest zich ervan vergewissen of deze voorwaarden in dit specifieke geval waren vervuld. Indien dit niet het geval was, kon de opslag en verwerking van persoonsgegevens in een register als het AZR op geen enkele grond worden geacht noodzakelijk te zijn in de zin van artikel 7, onder e), van Richtlijn 95/46/EG.[135]

Tot slot, met betrekking tot het gebruik van de gegevens die in het register waren opgenomen voor criminaliteitsbestrijdingsdoeleinden, oordeelde het Hof dat deze doelstelling "noodzakelijkerwijs gericht [is] op de vervolging van gepleegde misdrijven en delicten, ongeacht de nationaliteit van de daders". Het betreffende register bevat geen persoonsgegevens over onderdanen van de betrokken lidstaat, en dit verschil in behandeling vormt een geval van discriminatie als verboden bij artikel 18 van het VWEU. Bijgevolg staat deze bepaling,

134 *Ibid.*, punt 52.

135 *Ibid.*, punten 54, 58, 59 en 66-68.

als uitgelegd door het Hof, "in de weg (...) aan de invoering door een lidstaat van een systeem van verwerking van persoonsgegevens speciaal voor burgers van de Unie die niet de nationaliteit van die lidstaat bezitten, met als doel de bestrijding van de criminaliteit."[136]

Het gebruik van persoonsgegevens door autoriteiten die in de publieke arena werkzaam zijn is tevens onderworpen aan artikel 8 van het **EVRM**.

Door de voor de verwerker verantwoordelijke of een derde nagestreefde rechtmatige belangen

De betrokkene is niet de enige met rechtmatige belangen. Artikel 7, onder f), van de **richtlijn gegevensbescherming** bepaalt dat persoonsgegevens rechtmatig mogen worden verwerkt indien "de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt, mits het belang of de fundamentele rechten en vrijheden van de betrokkene die aanspraak maakt op bescherming (...) niet prevaleren".

In het volgende arrest heeft het HvJ-EU zich uitdrukkelijk uitgesproken over artikel 7, onder f), van de richtlijn:

Voorbeeld: In *ASNEF en FECEMD*[137] verduidelijkte het HvJ-EU dat in het nationale recht geen aanvullende voorwaarden mogen worden gesteld aan de voorwaarden die worden genoemd in artikel 7, onder f), van de richtlijn. Dit had betrekking op een situatie waarin de Spaanse gegevensbeschermingswetgeving een bepaling bevatte die andere private partijen alleen de mogelijkheid bood om een rechtmatig belang bij de verwerking van persoonsgegevens aan te voeren als de informatie reeds in openbare bronnen was opgenomen.

Het Hof merkte in de eerste plaats op dat het doel van Richtlijn 95/46/EG is om ervoor te zorgen dat het niveau van de bescherming van de rechten en vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens gelijk is in alle lidstaten. Ook mag het beter op elkaar afstemmen van

136 *Ibid.*, punten 78 en 81.

137 HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) en Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10 / Administración del Estado*, 24 november 2011.

de nationale wetgeving die op dit gebied van toepassing is niet leiden tot een vermindering van de geboden bescherming. De nationale wetgeving moet juist gericht zijn op een hoog beschermingsniveau in de Unie.[138] Bijgevolg oordeelde het HvJ-EU als volgt: "Derhalve vloeit uit het doel om in alle lidstaten een gelijkwaardige bescherming te bieden voort, dat artikel 7 van richtlijn 95/46 een uitputtende lijst bevat van gevallen waarin een verwerking van persoonsgegevens als rechtmatig kan worden aangemerkt". Bovendien mogen "de lidstaten aan artikel 7 van richtlijn 95/46 geen nieuwe beginselen betreffende de toelaatbaarheid van de verwerking van persoonsgegevens (...) toevoegen, noch bijkomende vereisten (...) vaststellen die de reikwijdte van een van de zes in dat artikel vervatte beginselen zouden wijzigen."[139] Het Hof gaf toe dat "[w]at de door artikel 7, sub f, van richtlijn 95/46 vereiste afweging betreft, (...) er rekening mee [kan] worden gehouden dat de ernst van de aantasting door die verwerking van de grondrechten van de betrokkene kan verschillen naargelang van de vraag of de desbetreffende gegevens reeds in voor het publiek toegankelijke bronnen zijn opgenomen".

Daarentegen "verzet artikel 7, sub f, van die richtlijn zich er (...) tegen dat een lidstaat voor bepaalde categorieën persoonsgegevens categorisch en generiek de mogelijkheid van verwerking uitsluit, zonder ruimte te bieden voor een afweging van de betrokken tegengestelde rechten en belangen in een concreet geval."

In het licht van deze overwegingen concludeerde het Hof dat "artikel 7, sub f, van richtlijn 95/46 in die zin moet worden uitgelegd dat het zich verzet tegen een nationale wettelijke regeling die, bij ontbreken van toestemming van de betrokkene, de mogelijkheid tot verwerking van diens persoonsgegevens, die noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de voor die verwerking verantwoordelijke of van de derde(n) aan wie de gegevens zullen worden meegedeeld, niet alleen afhankelijk stelt van de voorwaarde dat de fundamentele rechten en vrijheden van de betrokkene niet worden geschonden, maar ook van het vereiste dat de gegevens in voor het publiek toegankelijke bronnen zijn opgenomen, en aldus elke verwerking van

138 *Ibid.*, punt 28. Zie de richtlijn gegevensbescherming, overwegingen 8 en 10.

139 HvJ-EU, gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24 november 2011, punten 30 en 32.

gegevens die niet in dergelijke voor het publiek toegankelijke bronnen zijn opgenomen, categorisch en algemeen uitsluit".[140]

Vergelijkbare formuleringen zijn te vinden in **aanbevelingen van de RvE**. De Aanbeveling inzake profilering erkent de verwerking van persoonsgegevens voor profileringsdoeleinden als rechtmatig indien deze verwerking noodzakelijk is in verband met de rechtmatige belangen van anderen, "uitgezonderd indien de fundamentele rechten en vrijheden van de betrokkenen prevaleren".[141]

4.1.2. Rechtmatige verwerking van gevoelige gegevens

Het RvE-recht laat het aan het nationale recht over om passende bescherming voor het gebruik van gevoelige gegevens vast te stellen, terwijl **het EU-recht**, in artikel 8 van de richtlijn gegevensbescherming, gedetailleerde voorschriften bevat voor de verwerking van categorieën gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakvereniging of informatie over de gezondheid of het seksuele leven blijkt. De verwerking van gevoelige gegevens is in beginsel verboden.[142] Er is echter een uitputtende lijst van uitzonderingen op dit verbod, die is te vinden in artikel 8, leden 2 en 3, van de richtlijn. Deze uitzonderingen zijn gerelateerd aan uitdrukkelijke toestemming van de betrokkene, vitale belangen van de betrokkene, rechtmatige belangen van anderen en algemene belangen.

Anders dan bij de verwerking van niet-gevoelige gegevens wordt een contractuele relatie met de betrokkene niet gezien als een algemene grondslag voor de rechtmatige verwerking van gevoelige gegevens. Als gevoelige gegevens worden verwerkt in het kader van een contract met de betrokkene, vereist het gebruik van deze gegevens derhalve de afzonderlijke, uitdrukkelijke toestemming van de betrokkene, naast instemming met het sluiten van het contract. Een uitdrukkelijk verzoek van de betrokkene om goederen of diensten die noodzakelijkerwijs de bekendmaking van gevoelige gegevens met zich meebrengen, moet echter even goed als uitdrukkelijke toestemming worden opgevat.

140 *Ibid.*, punten 40, 44, 48 en 49.

141 Aanbeveling inzake profilering, artikel 3.4, onder b).

142 Richtlijn gegevensbescherming, artikel 8, lid 1.

Voorbeeld: Als een luchtvaartpassagier bij het boeken van een vlucht de luchtvaartmaatschappij verzoekt om een rolstoel en koosjere voeding, mag de luchtvaartmaatschappij deze gegevens gebruiken, ook al heeft de passagier geen extra toestemmingsclausule getekend die inhoudt dat hij of zij instemt met het gebruik van zijn of haar gegevens waaruit informatie over zijn of haar gezondheid en godsdienstige overtuiging blijkt.

Uitdrukkelijke toestemming van de betrokkene

De eerste voorwaarde voor de rechtmatige verwerking van gegevens, ongeacht of het niet-gevoelige of gevoelige gegevens betreft, is toestemming van de betrokkene. Ingeval van gevoelige gegevens moet deze toestemming uitdrukkelijk zijn. De nationale wetgeving kan er echter in voorzien dat toestemming voor het gebruik van gevoelige gegevens als rechtsgrondslag onvoldoende is om de verwerking ervan toe te staan,[143] bijvoorbeeld wanneer, in uitzonderlijke gevallen, de verwerking ongebruikelijke risico's voor de betrokkene met zich meebrengt.

In één bijzonder geval wordt zelfs impliciete toestemming erkend als rechtsgrond voor de verwerking van gevoelige gegevens. Artikel 8, lid 2, onder e), van de richtlijn bepaalt dat verwerking niet is verboden als deze betrekking heeft op gegevens die duidelijk door de betrokkene openbaar zijn gemaakt. Deze bepaling gaat duidelijk uit van de veronderstelling dat de handeling van de betrokkene om zijn of haar gegevens openbaar te maken moet worden uitgelegd als impliciete toestemming van de betrokkene voor het gebruik van deze gegevens.

Vitale belangen van de betrokkene

Evenals niet-gevoelige gegevens mogen ook gevoelige gegevens worden verwerkt vanwege de vitale belangen van de betrokkene.[144]

Om de verwerking van gevoelige gegevens op deze grond rechtmatig te laten zijn, moet het onmogelijk zijn om de betrokkene te vragen een beslissing te nemen omdat, bijvoorbeeld, de betrokkene niet bij bewustzijn is, afwezig is of niet kan worden bereikt.

143 *Ibid.,* artikel 8, lid 2, onder a).

144 *Ibid.,* artikel 8, lid 2, onder c).

Rechtmatige belangen van anderen

Zoals dat voor niet-gevoelige gegevens geldt, kunnen de rechtmatige belangen van anderen ook dienen als grondslag voor de verwerking van gevoelige gegevens. Voor gevoelige gegevens, en volgens artikel 8, lid 2, van de richtlijn gegevensbescherming, is dit echter alleen van toepassing op de volgende gevallen:

- wanneer dit noodzakelijk is ter verdediging van de vitale belangen van een andere persoon[145] indien deze lichamelijk of juridisch niet in staat is van zijn instemming te getuigen;

- wanneer gevoelige gegevens relevant zijn op het gebied van het arbeidsrecht, zoals gezondheidsgegevens, bijvoorbeeld in de context van een bijzonder gevaarlijke werkplek, of gegevens over godsdienstige overtuiging, bijvoorbeeld in de context van vakanties;[146]

- wanneer een stichting, een vereniging of enige andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is gegevens over haar leden, sponsoren of andere belanghebbende partijen verwerkt (dergelijke gegevens zijn gevoelig omdat er godsdienstige of levensbeschouwelijke overtuigingen of politieke opvattingen van de betrokken personen uit kunnen blijken);[147]

- wanneer gevoelige gegevens worden gebruikt in het kader van een gerechtelijke procedure bij een rechtbank of administratieve autoriteit voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.[148]

- Bovendien bepaalt artikel 8, lid 3, van de richtlijn gegevensbescherming dat wanneer gezondheidsgegevens worden gebruikt voor medisch onderzoek en behandelingen door gezondheidswerkers, het beheer van deze diensten ook onder deze uitzondering valt. Als bijzondere waarborg worden personen alleen als "gezondheidswerker" erkend als ze onderworpen zijn aan een specifiek beroepsgeheim of de verplichting om de gegevens vertrouwelijk te behandelen.

145 *Ibid.*

146 *Ibid.,* artikel 8, lid 2, onder b).

147 *Ibid.,* artikel 8, lid 2, onder d).

148 *Ibid.,* artikel 8, lid 2, onder e).

Algemeen belang

Voorts kunnen de lidstaten volgens artikel 8, lid 4, van de richtlijn gegevensbescherming verdere doeleinden invoeren waarvoor gevoelige gegevens kunnen worden verwerkt, zolang:

- de verwerking van gegevens gebeurt om redenen van zwaarwegend algemeen belang; en
- deze doeleinden bij nationale wet of bij een besluit van de toezichthoudende autoriteit zijn vastgesteld; en
- de nationale wet of het besluit van de toezichthoudende autoriteit de noodzakelijke waarborgen biedt om de belangen van de betrokkenen voldoende te beschermen.[149]

Een prominent voorbeeld zijn elektronische patiëntendossiers, waarvan de invoering in veel lidstaten wordt overwogen. Dit systeem staat toe dat gezondheidsgegevens, die zijn verzameld tijdens de behandeling van een patiënt, op grote schaal, meestal op landelijk niveau, beschikbaar worden gesteld aan andere behandelaars van deze patiënt.

De Groep gegevensbescherming artikel 29 heeft geconcludeerd dat de invoering van dit soort systemen niet is toegestaan op grond van de bestaande wettelijke voorschriften voor de verwerking van gegevens over patiënten, in het bijzonder artikel 8, lid 3, van de richtlijn gegevensbescherming. Aangenomen dat het bestaan van dergelijke systemen met elektronische patiëntendossiers een zwaarwegend algemeen belang vormt, zou de invoering ervan kunnen worden gebaseerd op artikel 8, lid 4, van de richtlijn, dat een expliciete rechtsgrondslag voor de invoering vereist die ook de noodzakelijk waarborgen biedt om ervoor te zorgen dat het systeem op veilige wijze wordt beheerd.[150]

149 *Ibid.,* artikel 8, lid 4.

150 Groep gegevensbescherming artikel 29 (2007), Werkdocument inzake de verwerking van persoonsgegevens betreffende gezondheid in elektronische medische dossiers, WP 131, Brussel, 15 februari 2007.

4.2. Regels voor de beveiliging van de verwerking

Belangrijkste punten

- De regels voor de beveiliging van de verwerking brengen een verplichting voor de voor de verwerking verantwoordelijke en de verwerker met zich mee om passende technische en organisatorische maatregelen te nemen om onbevoegde inmenging in verwerkingen te voorkomen.
- Het benodigde niveau van de gegevensbeveiliging wordt bepaald door:
  - de veiligheidskenmerken die beschikbaar zijn in de markt voor specifieke typen verwerkingen; en
  - de kosten; en
  - de gevoeligheid van de verwerkte gegevens.
- De veilige verwerking van gegevens wordt verder gewaarborgd door de algemene plicht voor iedereen, voor de verwerking verantwoordelijken en verwerkers, om ervoor te zorgen dat de gegevens vertrouwelijk blijven.

De verplichting van voor de verwerking verantwoordelijken en verwerkers om maatregelen te nemen die een toereikende gegevensbeveiliging waarborgen is daarom opgenomen in zowel de **gegevensbeschermingswetgeving van de RvE** als de **gegevensbeschermingswetgeving van de EU**.

4.2.1. Elementen van gegevensbeveiliging

De relevante bepaling van **het EU-recht** luidt als volgt:

> *"De lidstaten bepalen dat de voor de verwerking verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer dient te 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."*[151]

151 Richtlijn gegevensbescherming, artikel 17, lid 1.

Het **RvE-recht** bevat een vergelijkbare bepaling:

> *"Er dienen passende beveiligingsmaatregelen te worden getroffen om persoonsgegevens opgeslagen in geautomatiseerde bestanden te beschermen tegen toevallige of ongeoorloofde vernietiging, toevallig verlies en ongeoorloofde toegang, wijziging of verspreiding."*[152]

Vaak zijn er ook sectorale, nationale en internationale normen ontwikkeld om een veilige verwerking van gegevens mogelijk te maken. Het Europees privacyzegel (EuroPriSe) bijvoorbeeld is een eTEN (trans-Europese telecommunicatienetwerken)-project van de EU, waarin de mogelijkheden zijn onderzocht om producten, met name software, te certificeren als in overeenstemming met de Europese gegevensbeschermingswetgeving. Het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (ENISA) is opgezet om het vermogen van de EU, de EU-lidstaten en het bedrijfsleven om problemen met netwerk- en informatiebeveiliging op te lossen te vergroten.[153] ENISA publiceert regelmatig analyses van actuele beveiligingsbedreigingen en adviseert over de aanpak ervan.

Gegevensbeveiliging wordt niet alleen bereikt door de juiste uitrusting – hardware en software – te hebben. Daarvoor zijn ook passende interne organisatorische voorschriften nodig. Deze interne voorschriften zouden idealiter de volgende punten moeten bestrijken:

- de regelmatige verstrekking van informatie aan alle werknemers over gegevensbeveiligingsregels en hun verplichtingen uit hoofde van de gegevensbeschermingswetgeving, met name hun verplichting om gegevens vertrouwelijk te behandelen;

- een duidelijke verdeling van verantwoordelijkheden en een duidelijke omschrijving van bevoegdheden op het gebied van gegevensverwerking, met name met betrekking tot besluiten om persoonsgegevens te verwerken en gegevens over te dragen aan derden;

- het uitsluitend gebruiken van persoonsgegevens overeenkomstig de instructies van de bevoegde persoon of algemeen vastgestelde voorschriften;

152 Verdrag 108, artikel 7.

153 Verordening (EG) nr. 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging, PB L 77 van 13.3.2004, blz. 1.

- bescherming van de toegang tot locaties en tot hard- en software van de voor de verwerking verantwoordelijke en de verwerker, met inbegrip van controles op toegangsmachtigingen;

- de waarborg dat machtigingen voor de toegang tot persoonsgegevens worden toegewezen door bevoegd personeel en passende documentatie vereisen;

- geautomatiseerde protocollen voor de toegang tot persoonsgegevens met behulp van elektronische middelen en regelmatige controles van deze protocollen door een interne toezichthoudende eenheid;

- een zorgvuldige documentatie van andere vormen van overdracht dan via geautomatiseerde toegang tot gegevens om te kunnen aantonen dat er geen illegale gegevensoverdrachten plaatsvinden.

Ook het aanbieden van adequate opleidingen en onderwijs op het gebied van gegevensbeveiliging aan personeelsleden is een belangrijk element van een doeltreffende gegevensbeveiliging. Daarnaast moeten er verificatieprocedures zijn ingesteld om ervoor te zorgen dat passende maatregelen niet alleen op papier bestaan, maar in de praktijk worden toegepast en naar behoren werken (zoals interne en externe audits).

Maatregelen die het beveiligingsniveau van een voor de verwerking verantwoordelijke of verwerker kunnen verbeteren zijn bijvoorbeeld de aanstelling van een gegevensbeschermingsfunctionaris, de opleiding van werknemers op het gebied van gegevensbeveiliging, regelmatige audits, penetratietesten en kwaliteitszegels.

Voorbeeld: In *I. / Finland*,[154] was de verzoekster niet in staat gebleken te bewijzen dat andere werknemers van het ziekenhuis waar ze werkte illegaal inzage in haar medisch dossier hadden gehad. Deze vermeende schending van haar recht op gegevensbescherming was om die reden door de nationale rechtbanken verworpen. Het EHRM concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM omdat het registratiesysteem voor de inzage in medische dossiers dat het ziekenhuis toepaste "zodanig was dat het niet mogelijk was om met terugwerkende kracht duidelijkheid te verkrijgen over het gebruik van patiëntendossiers, aangezien daarin slechts de vijf meest recente raadplegingen werden vermeld en deze informatie werd verwijderd nadat het dossier

154 EHRM, *I. / Finland*, nr. 20511/03, 17 juli 2008.

weer in de archieven was opgeslagen". Voor het Hof was het doorslaggevend dat het registratiesysteem van het ziekenhuis duidelijk niet in overeenstemming was met de wettelijke eisen van het nationale recht, een feit waar de nationale rechtbanken te weinig gewicht aan hadden toegekend.

Kennisgevingen van inbreuken

In de gegevensbeschermingswetgeving van diverse Europese landen is een nieuw instrument voor het aanpakken van inbreuken op de gegevensbeschermingswetgeving ingevoerd: de verplichting van aanbieders van elektronische communicatiediensten om inbreuken te melden aan de vermoedelijke slachtoffers en aan de toezichthoudende autoriteiten. Voor telecommunicatieaanbieders is dit verplicht krachtens het EU-recht.[155] Het doel van het melden van inbreuken op de gegevensbeschermingswetgeving aan de betrokkene is om schade te voorkomen: het melden van inbreuken en de mogelijke gevolgen daarvan minimaliseert het risico op negatieve gevolgen voor de betrokkenen. Ingeval van ernstige nalatigheid kan de aanbieders van de diensten ook een boete worden opgelegd.

Er zullen tevoren interne procedures voor het effectieve beheer en de melding van inbreuken moeten worden opgezet, aangezien de termijn voor de verplichting om de betrokkene en/of de toezichthoudende autoriteit van een inbreuk in kennis te stellen, overeenkomstig de nationale wetgeving, doorgaans vrij kort is.

4.2.2. Vertrouwelijkheid

In het EU-recht wordt de veilige verwerking van gegevens verder gewaarborgd door de algemene plicht voor iedereen, voor de verwerking verantwoordelijken en verwerkers, om ervoor te zorgen dat gegevens vertrouwelijk blijven.

Voorbeeld: Een medewerkster van een verzekeringsmaatschappij ontvangt op haar werkplek een telefoontje van iemand die zegt een klant te zijn en informatie over zijn verzekeringspolis opvraagt.

155 Zie Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (*richtlijn betreffende privacy en elektronische communicatie*), PB L 201 van 31.7.2002, blz. 37, artikel 4, lid 3, als gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming PB L 337 van 18.12.2009, blz. 11.

De plicht om de gegevens van klanten vertrouwelijk te behandelen vereist dat de medewerkster ten minste minimumbeveiligingsmaatregelen toepast alvorens persoonsgegevens mee te delen. Dit zou bijvoorbeeld kunnen door aan te bieden om de klant terug te bellen op het telefoonnummer dat wordt vermeld in het dossier van de klant.

Artikel 16 van de richtlijn gegevensbescherming heeft uitsluitend betrekking op vertrouwelijkheid in de verhouding tussen de voor de verwerking verantwoordelijke en de verwerker. Of voor de verwerking verantwoordelijken gegevens al dan niet vertrouwelijk moeten behandelen, in de zin dat ze deze niet aan derden mogen meedelen, wordt geregeld in de artikel en 7 en 8 van de richtlijn.

De verplichting om persoonsgegevens vertrouwelijk te behandelen strekt zich niet uit tot situaties waarin gegevens ter kennis van iemand komen in zijn of haar hoedanigheid als particuliere persoon en niet als werknemer van een voor de verwerking verantwoordelijke of verwerker. In dat geval is artikel 16 van de richtlijn gegevensbescherming niet van toepassing, omdat het gebruik van persoonsgegevens door particuliere personen in feite volledig is uitgezonderd van het toepassingsgebied van de richtlijn indien dit gebruik binnen de grenzen van de zogeheten uitzondering voor huishoudens valt.[156] De uitzondering voor huishoudens is het gebruik van persoonsgegevens "door een natuurlijk persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden".[157] Sinds de beslissing van het HvJ-EU in het arrest *Bodil Lindqvist*[158] moet deze uitzondering echter eng worden uitgelegd, met name ten aanzien van de mededeling van gegevens. Met name zal de uitzondering voor huishoudens zich niet uitstrekken tot de mededeling van persoonsgegevens aan een onbeperkt aantal ontvangers op internet (voor nadere details van deze zaak, zie de paragrafen 2.1.2, 2.2, 2.3.1 en 6.1).

In het RvE-recht is de verplichting om gegevens vertrouwelijk te behandelen inherent aan het begrip "beveiliging van gegevens" in artikel 7 van Verdrag 108, dat betrekking heeft op gegevensbeveiliging.

Voor verwerkers betekent vertrouwelijkheid dat ze persoonsgegevens die hun door de voor de verwerking verantwoordelijke zijn toevertrouwd alleen mogen gebruiken in overeenstemming met diens instructies. Voor de werknemers van een voor

156 Richtlijn gegevensbescherming, artikel 3, lid 2, tweede streepje.

157 *Ibid*.

158 HvJ-EU, zaak C-101/01, *Bodil Lindqvist*, 6 november 2003.

de verwerking verantwoordelijke of een verwerker betekent vertrouwelijkheid dat ze persoonsgegevens alleen mogen gebruiken in overeenstemming met de instructies van hun bevoegde leidinggevenden.

De verplichting om gegevens vertrouwelijk te behandelen moet worden opgenomen in elke overeenkomst tussen voor de verwerking verantwoordelijken en verwerkers. Voorts zullen voor de verwerking verantwoordelijken en verwerkers specifieke maatregelen moeten nemen om voor hun werknemers een wettelijke plicht om gegevens vertrouwelijk te behandelen in te stellen, hetgeen normaliter wordt bereikt door de opneming van vertrouwelijkheidsclausules in het arbeidscontract.

Inbreuk op de beroepsplicht om gegevens vertrouwelijk te behandelen is in veel EU-lidstaten en andere partijen bij Verdrag 108 strafbaar gesteld.

4.3. Regels voor de transparantie van de verwerking

Belangrijkste punten

- Voordat een voor de verwerking verantwoordelijke begint met het verwerken van persoonsgegevens, moet hij, op zijn minst, de betrokkenen de identiteit van de voor de verwerking verantwoordelijke en het doel van de verwerking meedelen, tenzij de betrokkenen reeds over deze informatie beschikken.
- Als de gegevens worden verzameld bij derden is de verplichting om informatie te verstrekken niet van toepassing indien:
  - de gegevensverwerking wettelijk is toegestaan; of
  - de verstrekking van informatie onmogelijk blijkt of onevenredige inspanningen vereist.
- Voorts moet de voor de verwerking verantwoordelijke, voordat hij begint met het verwerken van persoonsgegevens:
  - de toezichthoudende autoriteit in kennis stellen van de voorgenomen verwerking(en); of
  - de verwerking(en) intern laten documenteren door een onafhankelijke gegevensbeschermingsfunctionaris indien het nationale recht in een dergelijke procedure voorziet.

Het beginsel van eerlijke verwerking vereist dat de verwerking transparant verloopt. In **het RvE-recht** is hiertoe vastgelegd dat eenieder in staat dient te worden gesteld om kennis te nemen van het bestaan van een bestand van persoonsgegevens, het doel daarvan en de identiteit van de voor de verwerking verantwoordelijke.[159] Hoe dit moet worden verwezenlijkt, wordt overgelaten aan het nationale recht. **Het EU-recht** is specifieker en waarborgt de transparantie voor de betrokkene door middel van een verplichting van de voor de verwerking verantwoordelijke om de betrokkene te informeren, en voor het algemene publiek door middel van kennisgevingen.

Volgens beide rechtsstelsels kunnen er in het nationale recht uitzonderingen op en beperkingen van de transparantieverplichtingen van de voor de verwerking verantwoordelijke worden vastgesteld indien een dergelijke uitzondering of beperking een noodzakelijke maatregel vormt om een bepaald algemeen belang of de bescherming van de betrokkene of van de rechten en vrijheden van anderen te vrijwaren, zolang dit noodzakelijk is in een democratische samenleving.[160] Zulke uitzonderingen kunnen bijvoorbeeld nodig zijn in het kader van een strafrechtelijk onderzoek, maar kunnen ook gerechtvaardigd zijn in andere omstandigheden.

4.3.1. Informatie

Zowel volgens het RvE-recht als het EU-recht zijn voor de verwerking verantwoordelijken verplicht om de betrokkene van tevoren in kennis te stellen van de voorgenomen verwerking.[161] Deze verplichting is niet afhankelijk van een verzoek van de betrokkene, maar moet proactief worden nagekomen door de voor de verwerking verantwoordelijke, ongeacht of de betrokkene belangstelling toont voor de informatie of niet.

Inhoud van de informatie

De informatie moet het doel van de verwerking en de identiteit en de contactgegevens van de voor de verwerking verantwoordelijke omvatten.[162] De richtlijn gegevensbescherming vereist dat verdere informatie wordt verstrekt indien dit "met inachtneming van de specifieke omstandigheden waaronder de verdere informa-

159 Verdrag 108, artikel 8, onder a).

160 *Ibid.*, artikel 9, lid 2, en richtlijn gegevensbescherming, artikel 13, lid 1.

161 Verdrag 108, artikel 8, onder a), en richtlijn gegevensbescherming, artikelen 10 en 11.

162 Verdrag 108, artikel 8, onder a), en richtlijn gegevensbescherming, artikel 10, leden a) en b).

tie verkregen wordt, nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen". In de artikel en 10 en 11 van de richtlijn worden, onder meer, de categorieën gegevens die worden verwerkt en de ontvangers van deze gegevens beschreven, evenals het bestaan van het recht op toegang tot de gegevens en het recht om de gegevens te rectificeren. Wanneer gegevens worden verzameld bij de betrokkene, moet de informatie duidelijk maken of men al dan niet verplicht is om te antwoorden en wat de eventuele gevolgen van niet-beantwoording zijn.[163]

Vanuit het oogpunt van **het RvE-recht** kan de verstrekking van deze informatie worden beschouwd als een goede praktijk volgens het beginsel van eerlijke gegevensverwerking en is deze informatieverstrekking in zoverre ook onderdeel van het RvE-recht.

Het beginsel van eerlijke verwerking vereist dat de informatie voor de betrokkenen gemakkelijk te begrijpen is. Het taalgebruik moet passend zijn voor de geadresseerde(n). Het niveau van het taalgebruik en het type taalgebruik zullen anders moeten zijn naar gelang het beoogde publiek bestaat uit bijvoorbeeld volwassenen of kinderen of uit het algemene publiek of deskundige academici.

Sommige betrokkenen zullen alleen summier willen worden geïnformeerd over het hoe en waarom van de verwerking van hun persoonsgegevens, terwijl anderen een gedetailleerde uitleg zullen willen ontvangen. Op de vraag welk gewicht moet worden toegekend aan dit aspect van eerlijke informatie, is ingegaan in een advies van de Groep gegevensbescherming artikel 29, waarin het idee van de zogeheten "getrapte kennisgevingen" naar voren is gebracht.[164] Een getrapte opmaak van kennisgevingen zou betrokkenen in staat stellen om zelf de mate van gedetailleerdheid van de informatie zoals ze die tot zich nemen te bepalen.

Moment van de informatieverstrekking

De richtlijn gegevensbescherming bevat licht van elkaar afwijkende bepalingen omtrent het moment waarop de informatie moet worden verstrekt, afhankelijk van de vraag of de gegevens zijn verzameld bij de betrokkene (artikel 10) of bij een derde (artikel 11). Wanneer gegevens worden verzameld bij de betrokkene, moet de informatie uiterlijk op het moment van de gegevensverzameling worden

163 Richtlijn gegevensbescherming, artikel 10, onder c).

164 Groep gegevensbescherming artikel 29 (2004), Advies 10/2004 over meer geharmoniseerde bepalingen inzake informatieverstrekking, WP 100, Brussel, 25 november 2004.

verstrekt. Wanneer gegevens worden verzameld bij derden, moet de informatie uiterlijk worden verstrekt op het moment dat de voor de verwerking verantwoordelijke de gegevens registreert, of voordat de gegevens voor het eerst aan een derde worden meegedeeld.

Uitzonderingen op de informatieverplichting

In het EU-recht bestaat er een algemene uitzondering op de verplichting om de betrokkene te informeren als de betrokkene reeds over de informatie beschikt.[165] Dit heeft betrekking op situaties waarin de betrokkene, overeenkomstig de omstandigheden van het geval, zich reeds bewust is van het feit dat zijn of haar gegevens door een bepaalde voor de verwerking verantwoordelijke zullen worden verwerkt voor een bepaald doel.

Artikel 11 van de richtlijn gegevensbescherming, dat betrekking heeft op de verplichting om de betrokkene te informeren indien de gegevens niet bij hem of haar zijn verkregen, bepaalt ook dat deze verplichting niet bestaat, met name ingeval van gegevensverwerking voor statistische doeleinden of voor historisch of wetenschappelijk onderzoek, wanneer:

- de verstrekking van informatie onmogelijk blijkt; of
- onevenredig veel moeite kost; of
- de registratie of verstrekking bij wet is voorgeschreven.[166]

Alleen artikel 11, lid 2, van de richtlijn gegevensbescherming bepaalt dat betrokkenen niet hoeven te worden geïnformeerd over verwerkingen als deze bij wet zijn voorgeschreven. Gegeven de algemene veronderstelling in het recht dat de wet bekend is bij wie eronder vallen, zou kunnen worden beargumenteerd dat wanneer gegevens worden verzameld bij een betrokkene op grond van artikel 10 van de richtlijn, de betrokkene reeds over de informatie beschikt. Maar aangezien deze kennis van de wet slechts een aanname is, vereist het beginsel van eerlijke verwerking op grond van artikel 10 dat de betrokkene ook wordt geïnformeerd als de verwerking bij wet is voorgeschreven, met name omdat het informeren van de

165 Richtlijn gegevensbescherming, artikel 10 en artikel 11, lid 1.

166 *Ibid.*, overweging 40 en artikel 11, lid 2.

betrokkene geen bijzonder moeilijke taak is wanneer de informatie rechtstreeks bij de betrokkene wordt verzameld.

Wat betreft **het RvE-recht** voorziet Verdrag 108 uitdrukkelijk in uitzonderingen op zijn artikel 8. De in de artikel en 10 en 11 van de richtlijn gegevensbescherming genoemde uitzonderingen kunnen worden gezien als voorbeelden van goede praktijken met betrekking tot de uitzonderingen als bedoeld in artikel 9 van Verdrag 108.

Verschillende manieren om informatie te verstrekken

De ideale manier om informatie te verstrekken zou zijn om elke afzonderlijke betrokkene mondeling of schriftelijk te benaderen. Als de gegevens worden verzameld bij de betrokkene, moet de informatieverstrekking gelijktijdig met het verzamelen van de gegevens plaatsvinden. Maar met name wanneer gegevens worden verzameld bij derden kan de informatie ook, gezien de evidente praktische moeilijkheid om alle betrokkenen persoonlijk te bereiken, worden verstrekt door middel van een passende openbare mededeling.

Een van de meest efficiënte manieren om informatie te verstrekken is om passende informatiebepalingen te publiceren op de homepage van de voor de verwerking verantwoordelijke, zoals een privacyverklaring. Een significant deel van de bevolking maakt evenwel geen gebruik van internet, en in het informatiebeleid van een onderneming of een overheidsautoriteit zou hiermee rekening moeten worden gehouden.

4.3.2. Kennisgeving

Het nationale recht kan voor de verwerking verantwoordelijken ertoe verplichten om de bevoegde toezichthoudende autoriteit in kennis te stellen van hun verwerkingsactiviteiten, zodat deze kunnen worden gepubliceerd. Als alternatief kan het nationale recht bepalen dat voor de verwerking verantwoordelijken een gegevensbeschermingsfunctionaris kunnen aanstellen die belast is met het bijhouden van een register van alle door de voor de verwerking verantwoordelijke verrichte verwerkingen.[167] Dit interne register moet op verzoek beschikbaar worden gesteld aan leden van het publiek.

167 *Ibid.,* artikel 18, lid 2, tweede streepje.

Voorbeeld: In een kennisgeving, evenals in de documentatie die door een interne functionaris voor gegevensbescherming wordt verzorgd, moeten de belangrijkste kenmerken van de desbetreffende verwerking worden beschreven. Dit zal informatie omvatten over de voor de verwerking verantwoordelijke, het doel van de verwerking, de rechtsgrondslag van de verwerking, de categorieën gegevens die worden verwerkt en de vermoedelijke ontvangende derden, en of er grensoverschrijdend gegevensverkeer wordt beoogd, en zo ja welk.

De publicatie van kennisgevingen door de toezichthoudende autoriteit moet geschieden in de vorm van een speciaal register. Om de doelstelling ervan te verwezenlijken zou de toegang tot dit register eenvoudig en kosteloos moeten zijn. Hetzelfde is van toepassing op de documentatie die door de gegevensverwerkingsfunctionaris van de voor de verwerking verantwoordelijke wordt bijgehouden.

De uitzonderingen op de verplichting om de bevoegde toezichthoudende autoriteit te informeren of een interne gegevensbeschermingsfunctionaris aan te wijzen die in het nationale recht kunnen worden vastgesteld voor verwerkingen waaraan waarschijnlijk geen specifiek risico voor betrokkenen zal zijn verbonden, worden genoemd in artikel 18, lid 2, van de richtlijn gegevensbescherming.[168]

4.4. Regels voor het bevorderen van de naleving

Belangrijkste punten

- In de richtlijn gegevensbescherming worden, in het kader van de verdere ontwikkeling van het verantwoordingsbeginsel, verschillende instrumenten voor het bevorderen van de naleving genoemd:
  - voorafgaande controle van beoogde verwerkingen door de nationale toezichthoudende autoriteit;
  - gegevensbeschermingsfunctionarissen die de voor de verwerking verantwoordelijke voorzien van speciale deskundigheid op het gebied van gegevensbescherming;

168 *Ibid.,* artikel 18, lid 2, eerste streepje.

  - gedragscodes waarin de bestaande gegevensbeschermingsregels die van toepassing zijn in een bepaald domein van de samenleving, zoals het bedrijfsleven, worden gespecificeerd.

- In het RvE-recht worden vergelijkbare instrumenten voorgesteld om de naleving van de Aanbeveling inzake profilering van de RvE te bevorderen.

4.4.1. Voorafgaande controle

Volgens artikel 20 van de richtlijn gegevensverwerking moet de toezichthoudende autoriteit verwerkingen controleren die mogelijk specifieke risico's voor de persoonlijke rechten en vrijheden van de betrokkenen inhouden – als gevolg van hetzij het doel, hetzij de omstandigheden van de verwerking – voordat de verwerking van start gaat. Het nationale recht moet bepalen welke verwerkingen in aanmerking komen voor voorafgaande controle. Deze controle kan erin resulteren dat verwerkingen worden verboden of dat bepaalde kenmerken van het voorgestelde ontwerp van de verwerkingen moeten worden gewijzigd. Met artikel 20 van de richtlijn wordt beoogd te waarborgen dat onnodig risicovolle verwerkingen niet eens van start gaan, omdat de toezichthoudende autoriteit bevoegd is om dergelijke verwerkingen te verbieden. De voorafgaande voorwaarde voor een doeltreffende werking van dit mechanisme is dat de toezichthoudende autoriteit van tevoren in kennis wordt gesteld. Om ervoor te zorgen dat voor de verwerking verantwoordelijken hun kennisgevingsverplichting nakomen, zullen toezichthoudende autoriteiten over de bevoegdheid moeten beschikken om dwangmaatregelen op te leggen, zoals boetes.

Voorbeeld: Als een onderneming verwerkingen uitvoert die volgens het nationale recht zijn onderworpen aan voorafgaande controle, moet deze onderneming documenten over de geplande verwerkingen aan de toezichthoudende autoriteit overleggen. De onderneming mag niet met de verwerking beginnen voordat ze van de toezichthoudende autoriteit groen licht heeft gekregen.

In enkele lidstaten bepaalt het nationale recht dat verwerkingen van start mogen gaan als de toezichthoudende autoriteit niet binnen een bepaalde termijn heeft gereageerd, bijvoorbeeld drie maanden.

4.4.2. Gegevensbeschermingsfunctionarissen

De richtlijn gegevensverwerking biedt de mogelijkheid dat in het nationale recht wordt bepaald dat voor de verwerking verantwoordelijken een werknemer kunnen aanwijzen die als gegevensbeschermingsfunctionaris optreedt.[169] Het doel van het aanstellen van een dergelijke functionaris is om de kans te minimaliseren dat de rechten en vrijheden van de betrokkenen door de verwerkingen negatief worden beïnvloed.[170]

> Voorbeeld: In Duitsland zijn private ondernemingen volgens afdeling 4f, subafdeling 1, van de Duitse federale gegevensbeschermingswet (*Bundesdatenschutzgesetz*) verplicht om een interne gegevensbeschermingsfunctionaris te benoemen als ze permanent tien of meer werknemers in dienst hebben die zich bezighouden met de geautomatiseerde verwerking van persoonsgegevens.

Het vermogen om dit doel te verwezenlijken vereist een bepaalde mate van onafhankelijkheid voor de positie van de functionaris binnen de organisatie van de voor de verwerking verantwoordelijke, zoals uitdrukkelijk wordt bepaald door de richtlijn. Om deze functionaris effectief te laten functioneren, zullen ook krachtige werknemersrechten, die bescherming bieden tegen eventualiteiten als ongerechtvaardigd ontslag, noodzakelijk zijn.

De RvE heeft, teneinde de naleving van nationale gegevensbeschermingswetgeving te bevorderen, het concept van een interne gegevensbeschermingsfunctionaris overgenomen in enkele aanbevelingen.[171]

4.4.3. Gedragscodes

Om de naleving te bevorderen kunnen het bedrijfsleven en andere sectoren gedetailleerde regels voor hun specifieke verwerkingen opstellen door beste praktijken vast te leggen in een gedragscode. De deskundigheid van de leden van de sector zal bevorderlijk zijn voor het vinden van oplossingen die praktisch zijn en daarom eerder zullen worden gevolgd. Dientengevolge worden de lidstaten – evenals de Europese Commissie – aangespoord om gedragscodes op te stellen die moeten bijdragen tot een goede toepassing van de ter uitvoering van deze richtlijn door de lidstaten

169 *Ibid.,* artikel 18, lid 2, tweede streepje.

170 *Ibid.*

171 Zie bijvoorbeeld de Aanbeveling inzake profilering, artikel 8.3.

vastgestelde nationale bepalingen, rekening houdend met de specifieke kenmerken van de verschillende sectoren.[172]

Om ervoor te zorgen dat de gedragscodes in overeenstemming zijn met de ter uitvoering van de richtlijn door de lidstaten vastgestelde nationale bepalingen, moeten de lidstaten een procedure voor de evaluatie van de codes instellen. Bij deze procedure zouden normaliter de nationale autoriteit, beroepsverenigingen en andere vertegenwoordigingsorganen van andere categorieën voor de verwerking verantwoordelijken moeten worden betrokken.[173]

De ontwerpen van communautaire codes, alsmede wijzigingen of verlengingen van bestaande communautaire codes, kunnen ter beoordeling worden voorgelegd aan de Groep gegevensbescherming artikel 29. Na goedkeuring door deze werkgroep kan de Europese Commissie zorg dragen voor een passende bekendmaking van de codes.[174]

Voorbeeld: De Federatie van Europese direct- en interactieve-marketingverenigingen (FEDMA) heeft een Europese gedragscode voor het gebruik van persoonsgegevens in het kader van direct marketing ontwikkeld. De code is met succes voorgelegd aan de Groep gegevensbescherming artikel 29. In 2010 is een bijlage over elektronische marketingboodschappen toegevoegd aan de code.[175]

172 Zie de richtlijn gegevensbescherming, artikel 27, lid 1.

173 *Ibid.,* artikel 27, lid 2.

174 *Ibid.,* artikel 27, lid 3.

175 Groep gegevensbescherming artikel 29 (2010), *Advies 4/2010 over de Europese gedragscode van FEDMA voor het gebruik van persoonsgegevens in het kader van direct marketing*, WP 174, Brussel, 13 juli 2010.

5

De rechten van betrokkenen en de handhaving van deze rechten

EU	Behandelde onderwerpen	RvE
Recht op toegang		
Richtlijn gegevensbescherming, artikel 12 HvJ-EU, zaak C-553/07, *College van burgemeester en wethouders van Rotterdam / M.E.E. Rijkeboer*, 7 mei 2009	**Recht op toegang tot eigen persoonsgegevens**	Verdrag 108, artikel 8, onder b)
	Recht op rectificatie, uitwissing (verwijdering) of afscherming	Verdrag 108, artikel 8, onder c) EHRM, *Cemalettin Canli / Turkije*, nr. 22427/04, 18 november 2008 EHRM, *Segerstedt-Wiberg en anderen / Zweden*, nr. 62332/00, 6 juni 2006 EHRM, *Ciubotaru / Moldavië*, nr. 27138/04, 27 april 2010
Recht van verzet		
Richtlijn gegevensbescherming, artikel 14, lid 1, onder a)	**Recht van verzet op grond van de bijzondere situatie van de betrokkene**	Aanbeveling inzake profilering, artikel 5.3
Richtlijn gegevensbescherming, artikel 14, lid 1, onder b)	**Recht van verzet tegen verder gebruik van gegevens met het oog op direct marketing**	Aanbeveling inzake direct marketing, artikel 4.1

EU	Behandelde onderwerpen	RvE
Richtlijn gegevensbescherming, artikel 15	Recht van verzet tegen geautomatiseerde besluiten	Aanbeveling inzake profilering, artikel 5.5
Onafhankelijk toezicht		
Handvest, artikel 8, lid 3 Richtlijn gegevensbescherming, artikel 28 Verordening gegevensbescherming EU-instellingen, hoofdstuk V HvJ-EU, zaak C-518/07, *Europese Commissie / Bondsrepubliek Duitsland,* 9 maart 2010 HvJ-EU, zaak C-614/10, *Europese Commissie / Republiek Oostenrijk*, 16 oktober 2012 HvJ-EU, zaak C-288/12, *Europese Commissie / Hongarije*, 8 april 2014	Nationale toezichthoudende autoriteiten	Verdrag 108, Aanvullend Protocol, artikel 1
Rechtsmiddelen en sancties		
Richtlijn gegevensbescherming, artikel 12	Verzoek aan de voor de verwerking verantwoordelijke	Verdrag 108, artikel 8, onder b)
Richtlijn gegevensbescherming, artikel 28, lid 4 Verordening gegevensbescherming EU-instellingen, artikel 32, lid 2	Bij een toezichthoudende autoriteit ingediende verzoeken	Verdrag 108, Aanvullend Protocol, artikel 1, lid 2, onder b)
Handvest, artikel 47	Rechtbanken (algemeen)	EVRM, artikel 13
Richtlijn gegevensbescherming, artikel 28, lid 3	Nationale rechtbanken	Verdrag 108, Aanvullend Protocol, artikel 1, lid 4
VWEU, artikel 263, lid 4 Verordening gegevensbescherming EU-instellingen, artikel 32, lid 1 VWEU, artikel 267	HvJ-EU	
	EHRM	EVRM, artikel 34
Rechtsmiddelen en sancties		
Handvest, artikel 47 Richtlijn gegevensbescherming, artikel en 22 en 23 HvJ-EU, zaak C-14/83, *Sabine von Colson en Elisabeth Kamann / Land Nordrhein-Westfalen*, 10 april 1984	Voor inbreuken op nationale gegevensbescher-mingswetgeving	EVRM, artikel 13 (alleen voor lidstaten van de RvE) Verdrag 108, artikel 10 EHRM, *K.U. / Finland*, nr. 2872/02, 2 maart 2008

EU	Behandelde onderwerpen	RvE
HvJ-EU, C-152/84, *M.H. Marshall / Southampton and South-West Hampshire Area Health Authority*, 26 februari 1986		EHRM, *Biriuk / Litouwen*, nr. 23373/03, 25 november 2008
Verordening gegevensbescherming EU-instellingen, artikel en 34 en 49 HvJ-EU, C-28/08 P, *Europese Commissie / The Bavarian Lager Co. Ltd*, 29 juni 2010	Voor inbreuken op EU-wetgeving door EU-instellingen en -organen	

De effectiviteit van wettelijke voorschriften in het algemeen en rechten van betrokkenen in het bijzonder is in aanzienlijke mate afhankelijk van het bestaan van passende mechanismen om ze te handhaven. In de Europese gegevensbeschermingswetgeving moet de betrokkene door het nationale recht in staat worden gesteld om zijn of haar gegevens te beschermen. Ook moeten bij het nationale recht onafhankelijke toezichthoudende autoriteiten worden ingesteld om de betrokkenen te helpen bij het uitoefenen van hun rechten en om toezicht te houden op de verwerking van persoonsgegevens. Voorts vereist het recht op een doeltreffende voorziening in rechte, als gegarandeerd door het EVRM en het Handvest, dat aan iedere persoon rechtsmiddelen ter beschikking staan.

5.1. De rechten van betrokkenen

Belangrijkste punten

- Eenieder heeft krachtens het nationale recht het recht om elke voor de verwerking verantwoordelijke te vragen of deze zijn of haar gegevens verwerkt.
- Betrokkenen hebben krachtens het nationale recht het recht om:
  - toegang te krijgen tot hun eigen gegevens bij elke voor de verwerking verantwoordelijke die hun gegevens verwerkt;
  - hun gegevens te laten rectificeren (uitwissen of afschermen, naar gelang het geval) door de voor de verwerking verantwoordelijke die hun gegevens verwerkt als de gegevens onjuist zijn;
  - hun gegevens te laten verwijderen of afschermen, naar gelang van het geval, door de voor de verwerking verantwoordelijke die hun gegevens verwerkt als deze de gegevens illegaal verwerkt.

- Voorts hebben betrokkenen het recht om bij voor de verwerking verantwoordelijken bezwaar te maken tegen:
  - geautomatiseerde besluiten (die worden genomen door persoonsgegevens uitsluitend met elektronische middelen te verwerken);
  - de verwerking van hun gegevens als deze verwerking leidt tot onevenredige resultaten;
  - het gebruik van hun gegevens voor direct-marketingdoeleinden.

5.1.1. Recht op toegang

In **het EU-recht** bevat artikel 12 van de richtlijn gegevensbescherming de elementen van het recht op toegang van de betrokkene, waaronder het recht om van de voor de verwerking verantwoordelijke uitsluitsel te verkrijgen "omtrent het al dan niet bestaan van verwerkingen van hem betreffende gegevens, alsmede ten minste informatie over de doeleinden van deze verwerkingen, de categorieën gegevens waarop deze verwerkingen betrekking hebben en de ontvangers of categorieën ontvangers aan wie de gegevens worden verstrekt", evenals "naar gelang van het geval, de rectificatie, de uitwissing of de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van deze richtlijn, met name op grond van het onvolledige of onjuiste karakter van de gegevens".

In het RvE-recht bestaan deze zelfde rechten en moeten deze worden gewaarborgd door het nationaal recht (artikel 8 van Verdrag 108). In verschillende aanbevelingen van de RvE wordt de term "toegang" gebruikt en worden de verschillende aspecten van het recht op toegang beschreven en voorgesteld voor tenuitvoerlegging in het nationaal recht op dezelfde wijze als uiteengezet in de paragraaf hierboven.

Volgens artikel 9 van Verdrag 108 en artikel 13 van de richtlijn gegevensbescherming kan de verplichting van voor de verwerking verantwoordelijken om in te gaan op een verzoek om toegang van een betrokkene worden beperkt op grond van het feit dat wettelijke belangen van anderen prevaleren. Prevalerende wettelijke belangen kunnen algemene belangen als de nationale veiligheid, de openbare veiligheid en de vervolging van strafbare feiten omvatten, evenals particuliere belangen die zwaarwegender zijn dan het belang van gegevensbescherming. Uitzonderingen of beperkingen moeten noodzakelijk zijn in een democratische samenleving en moeten evenredig zijn aan het nagestreefde doel. In zeer uitzonderlijke omstandigheden, bijvoorbeeld vanwege medische indicaties, kan de bescherming van de betrokkene op zichzelf een beperking van de transparantie vereisen; daarbij gaat het met name om beperking van het recht op toegang van elke betrokkene.

Wanneer gegevens uitsluitend worden verwerkt met het oog op wetenschappelijk onderzoek of voor statistische doeleinden, staat de richtlijn gegevensbescherming toe dat toegangsrechten bij nationaal recht worden beperkt; in dat geval moeten evenwel passende juridische waarborgen zijn ingesteld. In het bijzonder moet ervoor worden gezorgd dat er in het kader van deze verwerkingen geen maatregelen of besluiten over specifieke personen worden genomen en dat "er duidelijk geen gevaar bestaat dat inbreuk wordt gepleegd op de persoonlijke levenssfeer van de betrokkene".[176] Vergelijkbare bepalingen zijn te vinden in artikel 9, lid 3, van Verdrag 108.

Recht op toegang tot eigen persoonsgegevens

In het RvE-recht wordt het recht op toegang tot de eigen persoonsgegevens uitdrukkelijk erkend bij artikel 8 van Verdrag 108. Het EHRM heeft herhaaldelijk geoordeeld dat er een recht op toegang tot informatie over de eigen persoonsgegevens die berusten bij of worden gebruikt door anderen bestaat en dat dit recht voortvloeit uit de noodzaak om de persoonlijke levenssfeer te eerbiedigen.[177] In de zaak *Leander*[178] concludeerde het EHRM echter dat het recht op toegang tot door overheidsautoriteiten opgeslagen persoonsgegevens in bepaalde omstandigheden kan worden beperkt.

In het EU-recht wordt het recht op toegang tot de eigen persoonsgegevens uitdrukkelijk erkend in artikel 12 van de richtlijn gegevensbescherming en, als grondrecht, in artikel 8, lid 2, van het Handvest.

Artikel 12, onder a), van de richtlijn bepaalt dat lidstaten elke betrokkene het recht op toegang tot hun persoonsgegevens en op informatie moeten waarborgen. In het bijzonder heeft elke betrokkene het recht om van de voor de verwerking verantwoordelijke uitsluitsel te krijgen omtrent het al dan niet bestaan van verwerkingen van hem of haar betreffende gegevens, alsmede ten minste informatie over:

- de doeleinden van de verwerkingen;
- de categorieën gegevens waarop de verwerkingen betrekking hebben;

176 Richtlijn gegevensbescherming, artikel 13, lid 2.

177 EHRM, *Gaskin / het Verenigd Koninkrijk*, nr. 10454/83, 7 juli 1989; EHRM, *Odièvre / Frankrijk* [GC], nr. 42326/98, 13 februari 2003; EHRM, *K.H. en anderen / Slowakije*, nr. 32881/04, 28 april 2009; EHRM, *Godelli / Italië*, nr. 33783/09, 25 september 2012.

178 EHRM, *Leander / Zweden*, nr. 9248/81, 11 juli 1985.

- de gegevens die worden verwerkt;
- de ontvangers of categorieën ontvangers aan wie de gegevens worden verstrekt;
- de beschikbare informatie over de oorsprong van de gegevens die worden verwerkt;
- in geval van geautomatiseerde besluiten, de logica die ten grondslag ligt aan de automatische verwerkingen.

In het nationaal recht kunnen bepalingen worden toegevoegd over de informatie die door de voor de verantwoordelijk moet worden verstrekt, zoals de rechtsgrondslag van de gegevensverwerkingen.

Voorbeeld: Door inzage te krijgen in de eigen persoonsgegevens kan iemand bepalen of de gegevens al dan niet correct zijn. Het is daarom onontbeerlijk dat de betrokkene wordt geïnformeerd over de categorieën gegevens die worden verwerkt, evenals over de inhoud van de gegevens. Derhalve is het onvoldoende dat een voor de verwerking verantwoordelijke de betrokkene simpelweg meedeelt dat zijn of haar naam, adres, geboortedatum en interessegebied worden verwerkt. De voor de verwerking verantwoordelijke moet de betrokkene ook meedelen dat "de naam: N.N., een adres: Schwarzenbergplatz 11, 1040 Wenen, Oostenrijk, de geboortedatum: 10.10.1974, en het interessegebied van de betrokkene (zoals opgegeven door de betrokkene): klassieke muziek" worden verwerkt. Dit laatste element bevat tevens informatie over de gegevensbron.

De mededeling aan de betrokkene van de gegevens die worden verwerkt en van de beschikbare informatie over de bron ervan moet in begrijpelijke vorm worden gedaan, wat inhoudt dat de voor de verwerking verantwoordelijke de betrokkene mogelijk meer gedetailleerd moet uitleggen wat er precies wordt verwerkt. Het alleen noemen van technische afkortingen of medische termen in reactie op een verzoek om toegang zal bijvoorbeeld niet volstaan, ook niet als alleen deze afkortingen of termen zijn opgeslagen.

Informatie over de bron van de gegevens die door de voor de verwerking verantwoordelijke worden verwerkt moet na een verzoek om toegang worden verstrekt

voor zover deze informatie beschikbaar is. Deze bepaling moet worden begrepen in het licht van de beginselen van eerlijkheid en verantwoording. Een voor de verwerking verantwoordelijke mag informatie over de bron van de gegevens niet vernietigen om vrij te worden gesteld van de verplichting om ze mee te delen en mag ook niet voorbijgaan aan de gebruikelijke normen en erkende eisen voor de documentatie op het gebied van zijn activiteiten. Het niet bijhouden van documentatie over de bron van de verwerkte gegevens zal doorgaans neerkomen op het niet voldoen aan de verplichtingen van de voor de verwerking verantwoordelijke uit hoofde van het recht op toegang.

Wanneer geautomatiseerde evaluaties worden verricht, zal de algemene logica van de evaluatie moeten worden uitgelegd, waaronder de specifieke criteria die zijn toegepast bij het evalueren van de betrokkene.

De richtlijn maakt niet duidelijk of het recht op toegang tot informatie betrekking heeft op het verleden en, indien dat het geval is, op welke perioden in het verleden. In dit verband, en zoals is onderstreept in de jurisprudentie van het HvJ-EU, mag het recht op toegang tot de eigen gegevens niet onnodig worden beperkt door tijdslimieten. Betrokkenen moeten ook een redelijke kans krijgen om informatie te verkrijgen over verwerkingen in het verleden.

Voorbeeld: In de zaak *Rijkeboer*[179] werd het HvJ-EU gevraagd om te bepalen of, krachtens artikel 12, onder a), van de richtlijn gegevensbescherming, het recht van een natuurlijke persoon op toegang tot informatie over de ontvangers of categorieën ontvangers van persoonsgegevens en over de inhoud van de meegedeelde gegevens kan worden beperkt tot een jaar voorafgaand aan zijn of haar verzoek om toegang.

Om te bepalen of artikel 12, onder a), van de richtlijn de vaststelling van een dergelijke limiet toestaat, besloot het Hof om dat artikel uit te leggen in het licht van de doeleinden van de richtlijn. Het Hof merkte in de eerste plaats op dat het recht op toegang noodzakelijk is om de betrokkene in staat te stellen het recht uit te oefenen om de voor de verwerking verantwoordelijke zijn of haar gegevens te laten rectificeren, uitwissen of afschermen (artikel 12, onder b), of om aan derden aan wie de gegevens zijn verstrekt mee te delen dat de gegevens zijn gerectificeerd, uitgewist of afgeschermd (artikel 12, onder c). Het recht op

179 HvJ-EU, zaak C-553/07, *College van burgemeester en wethouders van Rotterdam / M.E.E. Rijkeboer*, 7 mei 2009.

toegang is ook noodzakelijk om de betrokkene de mogelijkheid te bieden het recht uit te oefenen om zich te verzetten tegen de verwerking van zijn of haar persoonsgegevens (artikel 14), of het recht om beroep in te stellen wanneer hij of zij schade heeft geleden (artikel en 22 en 23).

Om het praktische effect van de hierboven genoemde bepalingen te waarborgen oordeelde het Hof dat "dit recht noodzakelijkerwijs voor het verleden moet gelden. Anders zou de betrokkene zijn recht om gegevens waarvan hij vermoedt dat zij onrechtmatig of onjuist zijn, te laten rectificeren, uitwissen of afschermen, en om zich met het oog op vergoeding van de geleden schade tot de rechter te wenden, niet doeltreffend kunnen uitoefenen".

Het recht op rectificatie, uitwissing en afscherming van gegevens

"[e]en ieder [moet] over het recht (...) kunnen beschikken toegang te verkrijgen tot de gegevens die het voorwerp van een verwerking vormen en hemzelf betreffen, zodat hij zich van de juistheid en de rechtmatigheid van de verwerking ervan kan vergewissen."[180] In overeenstemming met deze beginselen moeten betrokkenen krachtens het nationale recht het recht hebben om van de voor de verwerking verantwoordelijke de rectificatie, uitwissing of afscherming te verkrijgen van de gegevens waarvan de verwerking volgens hen niet overeenstemt met de bepalingen van deze richtlijn, met name op grond van het onvolledige of onjuiste karakter van de gegevens.[181]

Voorbeeld: In *Cemalettin Canli / Turkije*[182] oordeelde het EHRM dat artikel 8 van het EVRM was geschonden als gevolg van onjuiste rapportage door de politie in een strafrechtelijke procedure.

De verzoeker was tweemaal betrokken geweest bij een strafrechtelijke procedure wegens vermeend lidmaatschap van illegale organisaties, maar was nooit veroordeeld. Toen de verzoeker opnieuw werd aangehouden en een ander strafbaar feit ten laste werd gelegd, verstrekte de politie de rechtbank die de strafzaak behandelde een rapport getiteld "Informatie over andere delicten", waarin de verzoeker werd genoemd als lid van twee illegale organisaties. Het

180 Richtlijn gegevensbescherming, overweging 41.

181 *Ibid.,* artikel 12, onder b).

182 EHRM, *Cemalettin Canli / Turkije*, nr. 22427/04, 18 november 2008, punten 33, 42 en 43; EHRM, *Dalea / Frankrijk*, nr. 964/07, 2 februari 2010.

verzoek van de verzoeker om kopieën van het rapport en van de politiedossiers leverde niets op. Het EHRM oordeelde dat de informatie in het politierapport binnen het toepassingsgebied van artikel 8 van het EVRM viel, omdat openbare informatie ook binnen de reikwijdte van het begrip "privéleven" kan vallen indien de informatie systematisch is verzameld en opgeslagen in dossiers die bij de autoriteiten berusten. Bovendien was het politierapport onjuist en was het opstellen ervan en het overleggen ervan aan de rechtbank niet in overeenstemming met de wet geweest. Het Hof concludeerde dat er een inbreuk op artikel 8 had plaatsgevonden.

Voorbeeld: In *Segerstedt-Wiberg en anderen / Zweden*[183] waren de verzoekers aangesloten geweest bij bepaalde liberale en communistische politieke partijen. Zij vermoedden dat informatie over hen in de registers van de veiligheidspolitie terecht was gekomen. Het EHRM vergewiste zich ervan dat de opslag van de gegevens in kwestie een rechtsgrondslag had en een rechtmatig doel diende. Met betrekking tot enkele verzoekers oordeelde het EHRM echter dat het blijven bewaren van de gegevens een onevenredige inmenging in hun privéleven vormde. Zo hadden de autoriteiten in het geval van de heer Schmid informatie bewaard die inhield dat hij in 1969 zou hebben gepleit voor gewelddadig verzet tegen de politie tijdens demonstraties. Het EHRM oordeelde dat deze informatie geen relevant belang van nationale veiligheid diende, met name gezien het historische karakter ervan. Het EHRM concludeerde dat er ten aanzien van vier van de vijf verzoekers sprake was van een inbreuk op artikel 8 van het EVRM.

In bepaalde gevallen zal het voor de betrokkene volstaan om de rectificatie van bijvoorbeeld de spelling van een naam, een adres of een telefoonnummer te verzoeken. Als dergelijke verzoeken echter verband houden met wettelijke kwesties, zoals de wettelijke identiteit van de betrokkene of de juiste verblijfplaats voor de bezorging van documenten, zijn verzoeken tot rectificatie mogelijk niet voldoende en kan de voor de verwerking verantwoordelijke het recht hebben om naar bewijs van de vermeende onjuistheid te vragen. Dergelijke verzoeken mogen geen onredelijke bewijslast voor de betrokkene vormen en het daarom voor de betrokkene onmogelijk maken om zijn of haar gegevens te laten rectificeren. Het EHRM heeft in verschillende zaken waarin de verzoeker of verzoekster niet in staat was de juistheid van in

183 EHRM, *Segerstedt-Wiberg en anderen / Zweden*, nr. 62332/00, 6 juni 2006, punten 89 en 90; zie ook, bijvoorbeeld, EHRM, *M.K. / Frankrijk*, nr. 19522/09, 18 april 2013.

geheime registers bewaarde informatie te betwisten, inbreuken op artikel 8 van het EVRM vastgesteld.[184]

Voorbeeld: In *Ciubotaru / Moldavië*[185] was het de verzoeker niet gelukt om de registratie van zijn etnische afkomst in officiële registers te wijzigen van Moldavisch naar Roemeens omdat hij zou hebben nagelaten zijn verzoek te motiveren. Het EHRM achtte het aanvaardbaar dat staten objectief bewijs konden verlangen alvorens iemands etnische identiteit te registreren. Als een dergelijke claim was gebaseerd op zuiver subjectieve en niet-onderbouwde gronden, konden de autoriteiten de registratie weigeren. De claim van de verzoeker was echter gebaseerd op meer dan de subjectieve perceptie van zijn eigen etniciteit; hij had objectief verifieerbare banden met de Roemeense etnische groep aangetoond, zoals taal, naam, empathie en andere elementen. Het nationale recht vereiste echter bewijs van de verzoeker dat zijn ouders tot de Roemeense etnische groep hadden behoord. Gezien de historische realiteiten van Moldavië had deze vereiste een onneembaar obstakel gecreëerd voor de registratie van een andere etnische identiteit dan die welke door de Sovjetautoriteiten was geregistreerd in verband met zijn ouders. Door te voorkomen dat de claim van de verzoeker werd getoetst aan objectief verifieerbaar bewijs, had de staat verzuimd te voldoen aan zijn positieve verplichting om de effectieve eerbiediging van het privéleven van de verzoeker te waarborgen. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Tijdens een civiele gerechtelijke procedure of een administratieve procedure bij een overheidsautoriteit waarin moet worden beslist of gegevens al dan niet juist zijn, kan de betrokkene verzoeken dat er een aantekening in zijn of haar dossier wordt opgenomen dat de juistheid van de gegevens wordt bestreden en dat gewacht wordt op een officiële beslissing. In deze periode mag de voor de verwerking verantwoordelijke de gegevens niet als zeker of definitief presenteren, met name niet tegenover derden.

Een verzoek van een betrokkene om gegevens uit te wissen of te verwijderen is vaak gebaseerd op het argument dat de verwerking geen rechtmatige grond zou hebben. Dergelijke argumenten worden vaak naar voren gebracht wanneer toestemming is ingetrokken of wanneer bepaalde gegevens niet langer het doel van de gegevensverzameling dienen. De bewijslast voor de rechtmatigheid van de

184 EHRM, *Rotaru / Roemenië* [GC], nr. 28341/95, 4 mei 2000.

185 EHRM, *Ciubotaru / Moldavië*, nr. 27138/04, 27 april 2010, punten 51 en 59.

gegevensverwerking zal bij de voor de verwerking verantwoordelijke liggen, aangezien deze verantwoordelijk is voor de rechtmatigheid van de verwerking. Volgens het verantwoordingsbeginsel moet de voor de verwerking verantwoordelijke te allen tijde kunnen aantonen dat er een deugdelijke rechtsgrondslag voor de verwerking bestaat en moet de verwerking anders worden gestopt.

Als de gegevensverwerking wordt betwist omdat de gegevens onjuist zouden zijn of onrechtmatig zouden zijn verwerkt, kan de betrokkene, in overeenstemming met het beginsel van eerlijke verwerking, eisen dat de betwiste gegevens worden afgeschermd. Dat betekent dat de gegevens niet worden uitgewist, maar dat de voor de verwerking verantwoordelijke tijdens de periode van de afscherming moet afzien van het gebruik van de gegevens. Dit is met name noodzakelijk indien aanhoudend gebruik van de gegevens of onjuiste of onrechtmatig bewaarde gegevens de betrokkene schade zouden kunnen berokkenen. Het nationale recht zou meer gedetailleerde bepalingen moeten bevatten ten aanzien van de vraag wanneer de verplichting om het gebruik van gegevens te blokkeren zich voordoet en hoe deze verplichting moet worden vervuld.

Voorts hebben betrokkenen het recht om van de voor de verwerking verantwoordelijke te verlangen dat ze derden in kennis stellen van afschermingen, rectificaties of uitwissingen als ze voorafgaand aan de verwerkingen gegevens hadden ontvangen. Omdat de verstrekking van gegevens aan derden door de voor de verwerking verantwoordelijke zou moeten zijn gedocumenteerd, zou het mogelijk moeten zijn de ontvangers van de gegevens te identificeren en om uitwissing te verzoeken. Als de gegevens ondertussen echter zijn gepubliceerd, bijvoorbeeld op internet, kan het onmogelijk zijn om de gegevens in alle gevallen uit te wissen, omdat de ontvangers van de gegevens niet kunnen worden gevonden. Volgens de richtlijn gegevensbescherming is het verplicht om contact op te nemen met ontvangers van gegevens ten behoeve van de rectificatie, uitwissing of afscherming van gegevens, "tenzij zulks onmogelijk blijkt of onevenredig veel moeite kost".[186]

5.1.2. Recht van verzet

Het recht van verzet omvat het recht om bezwaar te maken tegen geautomatiseerde individuele besluiten, het recht om bezwaar te maken vanwege de bijzondere situatie van de betrokkene en het recht om bezwaar te maken tegen verder gebruik van gegevens voor direct-marketingdoeleinden.

186 Richtlijn gegevensbescherming, artikel 12, onder c), laatste halve zin.

Recht van verzet tegen geautomatiseerde individuele besluiten

Geautomatiseerde besluiten zijn besluiten die worden genomen door persoonsgegevens uitsluitend met elektronische middelen te verwerken. Als dergelijke besluiten een aanzienlijk effect op de levens van natuurlijke personen kunnen hebben, omdat ze bijvoorbeeld verband houden met hun kredietwaardigheid, hun prestaties op het werk, hun gedrag of hun betrouwbaarheid, is bijzondere bescherming nodig om ongewenste gevolgen te voorkomen. De richtlijn gegevensbescherming bepaalt dat geautomatiseerde besluiten niet bepalend mogen zijn voor kwesties die belangrijk zijn voor personen en vereist dat de persoon het recht moet hebben om het geautomatiseerde besluit te herzien.[187]

Voorbeeld: Een belangrijk praktisch voorbeeld van geautomatiseerde besluitvorming is het vaststellen van een kredietscore. Om snel een beslissing te kunnen nemen over de kredietwaardigheid van een toekomstige klant worden bepaalde gegevens verzameld, zoals over het beroep of de gezinssituatie van de klant, die worden gecombineerd met gegevens over de betrokkene die beschikbaar zijn uit andere bronnen, zoals kredietinformatiesystemen. Deze gegevens worden automatisch ingevoerd in een algoritme waarmee een totale score wordt berekend die de kredietwaardigheid van een potentiële klant representeert. Zo kan de werknemer van het bedrijf binnen enkele seconden besluiten of de betrokkene aanvaardbaar is als klant of niet.

Dat neemt niet weg dat de lidstaten volgens de richtlijn moeten bepalen dat een persoon aan een geautomatiseerd besluit kan worden onderworpen als de belangen van de betrokkene niet in het geding zijn, omdat het besluit gunstig is voor betrokkene, of door andere passende middelen worden gewaarborgd.[188] Een recht van verzet tegen geautomatiseerde besluiten is ook inherent aan **het RvE-recht**, zoals is te zien in de aanbeveling inzake profilering.[189]

187 *Ibid.,* artikel 15, lid 1.

188 *Ibid.,* artikel 15, lid 2.

189 Aanbeveling inzake profilering, artikel 5, lid 5.

Recht van verzet op grond van de bijzondere situatie van de betrokkene

Er bestaat geen algemeen recht voor betrokkenen om zich te verzetten tegen de verwerking van hun gegevens.[190] Artikel 14, onder a), van de richtlijn gegevensbescherming biedt de betrokkene de mogelijkheid om bezwaar te maken om zwaarwegende en gerechtvaardigde redenen die verband houden met zijn of haar bijzondere situatie. Een vergelijkbaar recht is erkend in de aanbeveling inzake profilering van de RvE.[191] Deze bepalingen beogen een goed evenwicht te vinden tussen de gegevensbeschermingsrechten van de betrokkene en de rechtmatige belangen van anderen bij de verwerking van de gegevens van betrokkene.

Voorbeeld: Een bank slaat gedurende zeven jaar gegevens op van klanten die te laat zijn met de betaling van de rente en/of aflossingen op een lening. Een klant van wie gegevens zijn opgeslagen in deze databank vraagt een andere lening aan. De databank wordt geraadpleegd, er wordt een beoordeling van de financiële situatie van de klant gemaakt en de lening wordt geweigerd. De klant kan zich echter verzetten tegen de registratie van persoonsgegevens in de databank en om uitwissing van de gegevens verzoeken als hij of zij kan bewijzen dat de wanbetaling louter het gevolg was van een fout die onmiddellijk was gecorrigeerd nadat hij of zij zich ervan bewust was geworden.

Het effect van succesvol verzet is dat de gegevens in kwestie door de voor de verwerking verantwoordelijke niet langer mogen worden verwerkt. Verwerkingen van de gegevens van de betrokkene die hebben plaatsgevonden voordat de betrokkene bezwaar aantekent, blijven echter rechtmatig.

Recht van verzet tegen verder gebruik van gegevens met het oog op direct marketing

Artikel 14, onder b), van de richtlijn gegevensbescherming voorziet in een specifiek recht voor de betrokkene om zich te verzetten tegen het gebruik van zijn of haar gegevens met het oog op direct marketing. Dit recht is ook vastgelegd in

190 Zie ook EHRM, *M.S. / Zweden*, nr. 20837/92, 27 augustus 1997, waarin medische gegevens waren meegedeeld zonder toestemming of de mogelijkheid om bezwaar te maken, of EHRM, *Leander / Zweden*, nr. 9248/81, 26 maart 1987, of EHRM, *Mosley / het Verenigd Koninkrijk*, nr. 48009/08, 10 mei 2011.

191 Aanbeveling inzake profilering, artikel 5, lid 3.

de aanbeveling van de RvE inzake direct marketing.[192] Het is de bedoeling dat dit type verzet wordt ingesteld voordat de gegevens ter beschikking worden gesteld van derden met het oog op direct marketing. De betrokkene moet derhalve de kans worden geboden om bezwaar te maken voordat de gegevens worden overgedragen.

5.2. Onafhankelijk toezicht

Belangrijkste punten

- Om een doeltreffende gegevensbescherming te waarborgen, moeten krachtens het nationaal recht onafhankelijke toezichthoudende autoriteiten worden ingesteld.
- Nationale toezichthoudende autoriteiten moeten volledig onafhankelijk kunnen optreden, hetgeen moet worden gegarandeerd door de wet waarbij ze zijn ingesteld en tot uiting moet komen in de organisatiestructuur van de toezichthoudende autoriteit.
- Toezichthoudende autoriteiten hebben specifieke taken, zoals, onder meer:
  - het houden van toezicht op en het bevorderen van gegevensbescherming op nationaal niveau;
  - het verstrekken van adviezen aan betrokkenen, voor de verwerking verantwoordelijken, de overheid en het algemene publiek;
  - het behandelen van klachten en het bijstaan van betrokkenen bij vermeende inbreuken op gegevensbeschermingsrechten;
  - het houden van toezicht op voor de verwerking verantwoordelijken en verwerkers;
  - het ondernemen van actie, indien nodig, door:
    - voor de verwerking verantwoordelijken en verwerkers waarschuwingen te geven, te berispen of zelfs boetes op te leggen;
    - opdracht te geven om gegevens te rectificeren, af te schermen of uit te wissen;
    - een verbod op verwerking op te leggen;
  - het doorverwijzen van zaken naar de rechter.

192 RvE, Comité van ministers (1985), Aanbeveling Rec(85)20 aan de lidstaten inzake de bescherming van persoonsgegevens die worden gebruikt met het oog op direct marketing, 25 oktober 1985, artikel 4, lid 1.

De richtlijn gegevensbescherming vereist onafhankelijk toezicht als een belangrijk mechanisme om een doeltreffende gegevensbescherming te waarborgen. De richtlijn heeft een instrument voor de handhaving van gegevensbescherming ingevoerd dat in eerste instantie niet in Verdrag 108 of de privacyrichtsnoeren van de OESO was opgenomen.

Aangezien onafhankelijk toezicht onmisbaar is gebleken voor de ontwikkeling van doeltreffende gegevensbescherming, worden de lidstaten in een nieuwe bepaling van de herziene privacyrichtsnoeren van de OESO uit 2013 verzocht om "privacyhandhavingsautoriteiten in te stellen en in stand te houden die beschikken over de governance, de middelen en de technische deskundigheid die nodig zijn om hun bevoegdheden doeltreffend uit te oefenen en op een objectieve, onpartijdige en consistente basis besluiten te nemen."[193]

In het RvE-recht heeft het Aanvullend Protocol bij Verdrag 108 de instelling van toezichthoudende autoriteiten verplicht gesteld. Artikel 1 van dit rechtsinstrument omvat het wettelijk kader voor onafhankelijke toezichthoudende autoriteiten dat de verdragspartijen in hun nationale recht moeten integreren. In dit artikel worden vergelijkbare formuleringen gebruikt om de taken en bevoegdheden van deze autoriteiten te omschrijven als in de richtlijn gegevensbescherming. In beginsel moeten toezichthoudende autoriteiten derhalve volgens het EU-recht en het RvE-recht op dezelfde manier functioneren.

In het EU-recht zijn de bevoegdheden en de organisatiestructuur van toezichthoudende autoriteiten voor het eerst uiteengezet in artikel 28, lid 1, van de richtlijn gegevensbescherming. De verordening gegevensbescherming EU-instellingen[194] wijst de Europese Toezichthouder voor gegevensbescherming (EDPS) aan als de toezichthoudende autoriteit voor gegevensverwerking door de EU-instellingen en -organen. Bij het beschrijven van de taken en verantwoordelijkheden van de toezichthoudende autoriteit steunt deze verordening op de ervaring die is opgedaan sinds de bekendmaking van de richtlijn gegevensbescherming.

193 OESO (2013), Guidelines on governing the Protection of Privacy and transborder flows of personal data, punt 19, onder c).

194 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, PB L 8 van 12.1.2001, blz. 1, artikel 41 t/m 48.

De onafhankelijkheid van gegevensbeschermingsautoriteiten wordt gewaarborgd door artikel 16, lid 2, van het VWEU en artikel 8, lid 3, van het Handvest. Deze laatste bepaling ziet controle door een onafhankelijke autoriteit als een essentieel element van het grondrecht van gegevensbescherming. Daarnaast verplicht de richtlijn gegevensbescherming de lidstaten om toezichthoudende autoriteiten in te stellen die in volledige onafhankelijkheid toezicht moeten houden op de toepassing van de richtlijn.[195] Niet alleen moet de wet die ten grondslag ligt aan de oprichting van een toezichthoudende autoriteit bepalingen bevatten die haar onafhankelijkheid specifiek waarborgen, ook uit de specifieke organisatiestructuur van de autoriteit moet haar onafhankelijkheid blijken.

In 2010 heeft het HvJ-EU zich voor het eerst gebogen over het vraagstuk van de reikwijdte van de vereiste van onafhankelijkheid van gegevensbeschermingsautoriteiten.[196] De volgende voorbeelden illustreren de gedachtegang die het HvJ-EU daarbij heeft gevolgd.

Voorbeeld: In *Commissie / Duitsland*[197] verzocht de Europese Commissie het HvJ-EU om te verklaren dat Duitsland de eis van "volledige onafhankelijkheid" van de toezichthoudende autoriteiten voor gegevensbescherming niet correct had omgezet in Duits recht en derhalve zijn verplichting uit hoofde van artikel 28, lid 1, van de richtlijn gegevensbescherming niet had vervuld. In de opvatting van de Commissie was het probleem dat Duitsland de autoriteiten die belast waren met het toezicht op de verwerking van persoonsgegevens buiten de publieke sector in de verschillende deelstaten (*Länder*), onder staatstoezicht had geplaatst.

De beoordeling van de gegrondheid van het door de Commissie ingestelde beroep hing volgens het Hof af van de strekking van de in de genoemde bepaling neergelegde vereiste van onafhankelijkheid en dus van de uitlegging van die bepaling.

Het Hof onderstreepte dat het begrip "in volledige onafhankelijkheid" in artikel 28, lid 1, van de richtlijn moest worden uitgelegd rekening houdend met de

195 Richtlijn gegevensbescherming, artikel 28, lid 1, laatste zin; Verdrag 108, Aanvullend Protocol, artikel 1, lid 3.

196 Zie FRA (2010), *Fundamental rights: challenges and achievements in 2010*, Jaarverslag 2010, blz. 59. Het FRA is dieper ingegaan op deze kwestie in zijn verslag *Data protection in the European Union: the role of National Data Protection Authorities*, gepubliceerd in mei 2010.

197 HvJ-EU, zaak C-518/07, *Europese Commissie / Bondsrepubliek Duitsland,* 9 maart 2010, punt 27.

bewoordingen van deze bepaling en met de doelstellingen en de opzet van de richtlijn gegevensbescherming.[198] Het Hof benadrukte dat de toezichthoudende autoriteiten de "hoeders" van de rechten in verband met de verwerking van persoonsgegevens als gegarandeerd door de richtlijn waren en dat de oprichting van deze autoriteiten "van wezenlijk belang voor de bescherming van personen bij de verwerking van persoonsgegevens" was.[199] Het Hof concludeerde dat de toezichthoudende autoriteiten "[b]ij de uitoefening van hun taken (...) bijgevolg objectief en onpartijdig [moeten] handelen. Daartoe moeten zij vrij zijn van beïnvloeding van buitenaf, daaronder begrepen de – rechtstreekse of indirecte – beïnvloeding door de staat of de Länder, en niet enkel van beïnvloeding door de organen waarop zij toezicht uitoefenen".[200]

Ook oordeelde het HvJ-EU dat de betekenis van "volledige onafhankelijkheid" moet worden uitgelegd in het licht van de onafhankelijkheid van de EDPS als omschreven in de verordening gegevensbescherming EU-instellingen. Daarbij onderstreepte het Hof dat artikel 44, lid 2, van deze verordening dit begrip verduidelijkt door toe te voegen dat de EDPS "bij de vervulling van zijn taken van niemand instructies vraagt of aanvaardt". Dit sluit staatstoezicht op een onafhankelijke toezichthoudende autoriteit voor gegevensbescherming uit.[201]

Bijgevolg oordeelde het HvJ-EU dat de Duitse gegevensbeschermingsinstellingen op het niveau van de bondsstaat die belast waren met het toezicht op de verwerking van persoonsgegevens door niet-overheidsorganen onvoldoende onafhankelijk waren omdat ze waren onderworpen aan toezicht door de staat.

Voorbeeld: In *Commissie / Oostenrijk*[202] wees het HvJ-EU op soortgelijke problemen met de positie van bepaalde leden en het personeel van de Oostenrijkse gegevensbeschermingsautoriteit (*Datenschutzkommission*, DSK). Het Hof concludeerde in deze zaak dat de Oostenrijkse wetgeving de Oostenrijkse gegevensbeschermingsautoriteit niet in staat stelde haar werkzaamheden in volledige onafhankelijkheid in de zin van de richtlijn gegevensbescherming uit te oefenen. De onafhankelijkheid van de Oostenrijkse gegevensbeschermingsautoriteit was onvoldoende verzekerd omdat het secretariaat van de DSK bestond

198 *Ibid.*, punten 17 en 29.

199 *Ibid.*, punt 23.

200 *Ibid.*, punt 25.

201 *Ibid.*, punt 27.

202 HvJ-EU, zaak C-614/10, *Europese Commissie / Republiek Oostenrijk*, 16 oktober 2012, punten 59 en 63.

uit ambtenaren die de bondskanselarij ter beschikking had gesteld, toezicht hield op de DSK en het recht had om te allen tijde te worden geïnformeerd over haar werkzaamheden.

Voorbeeld: In *Commissie / Hongarije*,[203] wees het HvJ-EU erop dat "het vereiste (...) dat moet worden gewaarborgd dat elke toezichthoudende autoriteit de haar opgedragen taken in volledige onafhankelijkheid vervult, impliceert dat de betrokken lidstaat verplicht is de duur van het mandaat van een dergelijke autoriteit te eerbiedigen tot het aanvankelijk voorzien einde daarvan" en oordeelde dat "Door het mandaat van de toezichthoudende autoriteit voor de bescherming van persoonsgegevens voortijdig te hebben beëindigd, is Hongarije de verplichtingen niet nagekomen die op hem rusten krachtens richtlijn 95/46/EG (...)"

Toezichthoudende autoriteiten hebben krachtens het nationale recht bevoegdheden en de capaciteit om, onder andere:[204]

- voor de verwerking verantwoordelijken en betrokkenen adviezen te verstrekken over alle gegevensbeschermingsaangelegenheden;
- verwerkingen te controleren en dienovereenkomstig in te grijpen;
- voor de verwerking verantwoordelijken te waarschuwen of te berispen;
- de rectificatie, afscherming of uitwissing van gegevens te gelasten;
- een verwerking tijdelijk of definitief te verbieden;
- de zaak door te verwijzen naar de rechter.

Om haar taken te kunnen vervullen, moet een toezichthoudende autoriteit toegang hebben tot alle persoonsgegevens en informatie die noodzakelijk is om een onderzoek te verrichten, evenals toegang tot alle bedrijfsruimten waar een voor de verwerking verantwoordelijke relevante informatie bewaart.

Er bestaan aanzienlijke verschillen tussen nationale rechtssystemen wat betreft de procedures en de rechtsgevolgen van de bevindingen van toezichthoudende

203 HvJ-EU, zaak C-288/12, *Europese Commissie / Hongarije*, 8 april 2014, punten 50 en 67.

204 Richtlijn gegevensbescherming, artikel 28; zie voorts Verdrag 108, Aanvullend Protocol, artikel 1.

autoriteiten. Deze kunnen uiteenlopen van ombudsmanachtige aanbevelingen tot onmiddellijk uitvoerbare besluiten. Bij het analyseren van de efficiëntie van de beschikbare rechtsmiddelen binnen een rechtsgebied moeten deze verhaalsinstrumenten derhalve worden beoordeeld in hun context.

5.3. Rechtsmiddelen en sancties

Belangrijkste punten

- Volgens zowel Verdrag 108 als de richtlijn gegevensbescherming moet het nationale recht passende rechtsmiddelen en sancties omvatten tegen inbreuken op het recht op gegevensbescherming.
    - Het recht op een doeltreffende voorziening in rechte vereist volgens het EU-recht dat in het nationale recht gerechtelijke procedures moeten worden opgenomen om in geval van inbreuken op gegevensbeschermingsrechten verhaal te halen, ongeacht de mogelijkheid om een toezichthoudende autoriteit te benaderen.
    - Het nationale recht moet sancties opleggen die doeltreffend, gelijkwaardig, evenredig en afschrikwekkend zijn.
- Voordat iemand naar de rechter stapt, moet hij of zij zich eerst tot de voor de verwerking verantwoordelijke wenden. Of het al dan niet verplicht is om eerst contact op te nemen met een toezichthoudende autoriteit alvorens naar de rechter te stappen, wordt overgelaten aan het nationale recht.
- Als laatste redmiddel en onder bepaalde voorwaarden kunnen betrokkenen inbreuken op gegevensbeschermingswetgeving aanhangig maken bij het EHRM.
- Daarnaast kunnen betrokken zich richten tot het HvJ-EU, zij het in slechts zeer beperkte mate.

Rechten uit hoofde van gegevensbeschermingswetgeving kunnen uitsluitend worden uitgeoefend door de persoon van wie de rechten in het geding zijn; dit zal iemand zijn die de betrokkene is of beweert te zijn. Deze persoon kan worden vertegenwoordigd in de uitoefening van zijn of haar rechten door personen die voldoen aan de door het nationale recht gestelde eisen. Minderjarigen moeten worden vertegenwoordigd door hun ouder(s) of voogd(en). In procedures bij toezichthoudende autoriteiten kan iemand ook worden vertegenwoordigd door verenigingen die als wettig doel hebben om gegevensbeschermingsrechten te bevorderen.

5.3.1. Verzoeken aan de voor de verwerking verantwoordelijke

De in paragraaf 3.2 genoemde rechten moeten in eerste instantie worden uitgeoefend vis-à-vis de voor de verwerking verantwoordelijke. Het rechtstreeks benaderen van de nationale toezichthoudende autoriteit of een rechtbank heeft geen zin, aangezien de autoriteit slechts het advies kan geven om eerst een verzoek bij de voor de verwerking verantwoordelijke in te dienen, en de rechtbank het verzoek niet-ontvankelijk zou verklaren. De formele eisen voor een wettelijk relevant verzoek aan een voor de verwerking verantwoordelijke, met name of het verzoek al dan niet schriftelijk moet worden ingediend, zouden door het nationaal recht moeten worden vastgesteld.

De entiteit die als de voor de verwerking verantwoordelijke wordt aangesproken, moet reageren op een verzoek, ook al is deze entiteit niet de voor de verwerking verantwoordelijke. In elk geval moet aan de betrokkene antwoord worden gegeven binnen de in het nationale recht vastgestelde termijn, al is het maar om mee te delen dat er geen gegevens over de indiener of indienster van het verzoek worden verwerkt. Overeenkomstig artikel 12, onder a), van de richtlijn gegevensbescherming en artikel 8, onder b), van Verdrag 108, moeten verzoeken worden behandeld "zonder bovenmatige vertraging". In het nationale recht moet daarom een beantwoordingstermijn worden vastgelegd die kort genoeg is, maar die de voor de verwerking verantwoordelijke in staat stelt om het verzoek op adequate wijze te behandelen.

Voordat de entiteit die als voor de verwerking verantwoordelijke is benaderd antwoord geeft op het verzoek, moet deze de identiteit van de verzoek(st)er vaststellen om te bepalen of hij of zij inderdaad de persoon is die hij of zij zegt te zijn en op die manier een ernstige inbreuk op de vertrouwelijkheid te voorkomen. Als de vereisten voor het vaststellen van de identiteit niet specifiek door het nationale recht zijn gereguleerd, moet de voor de verwerking verantwoordelijke daarover een besluit nemen. Het beginsel van eerlijke verwerking verlangt evenwel dat voor de verwerking verantwoordelijken geen overmatig belastende voorwaarden stellen aan het vaststellen van iemands identiteit (en van de echtheid van het verzoek, zoals is besproken in paragraaf 2.1.1).

Ook moet het nationale recht de vraag beantwoorden of voor de verwerking verantwoordelijken, voordat ze antwoord geven op een verzoek, daarvoor een vergoeding kunnen vragen van de verzoek(st)er. Artikel 12, onder a), van de richtlijn

gegevensbescherming en artikel 8, onder b), van Verdrag 108 bepalen dat verzoeken om toegang "zonder bovenmatige (...) kosten" moeten worden beantwoord. In veel Europese landen bepaalt het nationale recht dat verzoeken uit hoofde van gegevensbeschermingswetgeving voor de verzoek(st)er kosteloos moeten worden beantwoord zolang dit geen bovenmatige en ongebruikelijke moeite kost; voor de verwerking verantwoordelijken worden op hun beurt door het nationale recht beschermd tegen misbruik van het recht om antwoord op een verzoek te ontvangen.

Als de persoon, de instelling of het orgaan die of dat is benaderd als voor de verwerking verantwoordelijke niet ontkent de voor de verwerking verantwoordelijke te zijn, moet deze entiteit binnen de door het nationale recht vastgestelde termijn:

- ofwel het verzoek inwilligen en de verzoekende persoon meedelen hoe dit is gebeurd; ofwel

- de verzoekende persoon meedelen waarom zijn of haar verzoek niet is ingewilligd.

5.3.2. Bij een toezichthoudende autoriteit ingediende verzoeken

Wanneer een persoon, nadat hij of zij een verzoek om toegang heeft ingediend of bezwaar heeft aangetekend bij een voor de verwerking verantwoordelijke, niet tijdig een bevredigend antwoord ontvangt, kan deze persoon zich wenden tot de toezichthoudende autoriteit met een verzoek om hulp. In de procedure bij de toezichthoudende autoriteit moet duidelijk worden of de persoon, de instelling of het orgaan die of dat het verzoek van de verzoekende persoon heeft ontvangen inderdaad verplicht was om te reageren op het verzoek en of de reactie correct en voldoende was. De betrokken persoon moet door de toezichthoudende autoriteit in kennis worden gesteld van het resultaat van de procedure waarin het verzoek is behandeld.[205] De rechtsgevolgen van het resultaat van de procedure bij de nationale toezichthoudende autoriteiten zijn afhankelijk van het nationale recht: of de besluiten van de autoriteit al dan niet wettelijk kunnen worden uitgevoerd, hetgeen inhoudt dat ze afdwingbaar zijn door een officiële autoriteit, en of al dan niet beroep moet

205 Richtlijn gegevensbescherming, artikel 28, lid 4.

worden ingesteld bij een rechtbank als de voor de verwerking verantwoordelijke de besluiten van de toezichthoudende autoriteit niet opvolgt (advies, berisping, enz.).

Wanneer een EU-instelling of -orgaan een vermeende inbreuk heeft gepleegd op uit hoofde van artikel 16 van het VWEU gegarandeerde gegevensbeschermingsrechten, kan de betrokkene een klacht indienen bij de EDPS,[206] de onafhankelijke toezichthoudende autoriteit voor gegevensbescherming overeenkomstig de verordening gegevensbescherming EU-instellingen, waarin de taken en bevoegdheden van de EDPS zijn vastgelegd. Bij het uitblijven van een antwoord van de EDPS binnen zes maanden wordt de klacht geacht te zijn verworpen.

Tegen besluiten van een nationale toezichthoudende autoriteit moet beroep kunnen worden ingesteld bij de rechter. Dit is zowel van toepassing op betrokkenen als op voor de verwerking verantwoordelijken als ze partij zijn geweest in een procedure bij een toezichthoudende autoriteit.

Voorbeeld: Op 24 juli 2013 besloot de Informatiecommissaris van het Verenigd Koninkrijk de politie van Hertsfordshire te verzoeken om te stoppen met het gebruik van een systeem voor het traceren van kentekenplaten dat hij onrechtmatig achtte. De met behulp van camera's verzamelde gegevens werden opgeslagen in databanken van lokale politiekorpsen en in een centrale databank. Foto's van kentekenplaten werden gedurende twee jaar bewaard, en foto's van auto's gedurende 90 dagen. De Informatiecommissaris achtte een dergelijk uitgebreid gebruik van camera's en andere vormen van surveillance niet evenredig aan het probleem dat de politie probeerde op te lossen.

5.3.3. Bij een rechtbank ingediend verzoek

Volgens de richtlijn gegevensbescherming moet een persoon, indien hij of zij op grond van gegevensbeschermingswetgeving een verzoek bij een voor de verwerking verantwoordelijke heeft ingediend en niet tevreden is met het antwoord van de voor de verwerking verantwoordelijke, het recht hebben om zich tot de nationale rechter te wenden.[207]

206 Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens, PB L 8 van 12.1.2001, blz. 1.

207 Richtlijn gegevensbescherming, artikel 22.

Of het al dan niet verplicht is om eerst contact op te nemen met een toezichthoudende autoriteit alvorens een verzoek bij een rechtbank in te dienen, wordt overgelaten aan het nationale recht. In de meeste gevallen zal het voor de personen die hun gegevensbeschermingsrechten uitoefenen echter zinvol zijn om eerst de toezichthoudende autoriteit te benaderen, aangezien de procedures van deze autoriteit inzake verzoeken om hulp niet-bureaucratisch en kosteloos zouden moeten zijn. Ook kan de deskundigheid die is vervat in het gedocumenteerde besluit van de toezichthoudende autoriteit (advies, berisping, enz.) de betrokkene van pas komen bij het afdwingen van zijn of haar rechten bij de rechtbanken.

In het EU-recht kunnen vermeende schendingen van gegevensbeschermingsrechten op het nationale niveau van een partij bij het EVRM die tegelijkertijd een schending van artikel 8 van het EVRM vormen, daarnaast ook bij het EHRM aanhangig worden gemaakt nadat alle beschikbare nationale rechtsmiddelen zijn uitgeput. Een verzoek aan het EHRM naar aanleiding van een vermeende schending van artikel 8 van het EVRM moet ook voldoen aan andere ontvankelijkheidscriteria (artikel en 34 t/m 37 van het EVRM).[208]

Hoewel verzoeken aan het EHRM alleen gericht kunnen zijn tegen partijen bij het EVRM, kunnen ze indirect ook betrekking hebben op handelingen of nalatigheid door private partijen voor zover een verdragspartij haar positieve verplichtingen uit hoofde van het EVRM niet heeft vervuld en onvoldoende bescherming heeft geboden tegen inbreuken op in haar nationale recht vastgestelde gegevensbeschermingsrechten.

Voorbeeld: In *K.U. / Finland*[209] beklaagde de verzoeker, een minderjarige, zich erover dat een seksueel getinte advertentie over hem op een datingsite op internet was gezet. De identiteit van de persoon die de informatie op internet had gezet was door de internetaanbieder niet meegedeeld als gevolg van vertrouwelijkheidsverplichtingen van het Finse recht. De verzoeker stelde dat het Finse recht onvoldoende bescherming bood tegen dergelijke acties waarbij een particuliere persoon compromitterende gegevens over de verzoeker op internet plaatst. Het EHRM oordeelde dat staten niet alleen verplicht zijn zich te onthouden van willekeurige inmenging in de privélevens van natuurlijke personen, maar ook zijn onderworpen aan positieve verplichtingen, waaronder "de vaststelling van maatregelen ter verzekering van de eerbiediging van andermans

208 EVRM, artikelen 34 t/m 37.

209 EHRM, *K.U. / Finland*, nr. 2872/02, 2 maart 2009.

privéleven op het gebied van de onderlinge relaties van individuele personen". In het geval van de verzoeker vereiste zijn praktische en doeltreffende bescherming dat er effectieve stappen werden ondernomen om de dader te identificeren en te vervolgen. Deze bescherming was door de staat echter niet geboden, en het Hof concludeerde dat er een inbreuk op artikel 8 van het EVRM had plaatsgevonden.

Voorbeeld: In *Köpke / Duitsland*[210] werd de verzoekster verdacht van diefstal op haar werkplek en was ze daarom onderworpen aan surveillance met behulp van een verborgen camera. Het EHRM concludeerde dat "niets er op wijst dat de binnenlandse autoriteiten geen goed evenwicht hebben gevonden, binnen hun beoordelingsmarge, tussen het recht van verzoekster op eerbiediging van haar privéleven op grond van artikel 8 en zowel het belang van haar werkgever in het beschermen van zijn eigendomsrechten als het algemene belang van een behoorlijke rechtspraak". Het verzoek werd om die reden niet-ontvankelijk verklaard.

Als het EHRM oordeelt dat een staat die ook verdragspartij is een door het EVRM beschermd recht heeft geschonden, is deze staat verplicht om uitvoering te geven aan het arrest van het EHRM. Uitvoeringsmaatregelen moeten eerst een eind maken aan de schending en daarnaast, voor zover mogelijk, de negatieve gevolgen voor de verzoeker corrigeren. De tenuitvoerlegging van arresten kan ook algemene maatregelen vereisen om soortgelijke schendingen als die welke door het Hof zijn vastgesteld te voorkomen, door middel van wetswijzigingen, jurisprudentie of anderszins.

Wanneer het EHRM een schending van het EVRM vaststelt, voorziet artikel 41 van het EVRM erin dat het Hof billijke genoegdoening aan de benadeelde kan toekennen op kosten van de verdragspartij.

In **het EU-recht**[211] kunnen de slachtoffers van inbreuken op nationale gegevensbeschermingswetgeving, die de gegevensbeschermingswetgeving van de EU ten uitvoer legt, hun zaak in sommige gevallen aan het HvJ-EU voorleggen. Er zijn twee

210 EHRM, *Köpke / Duitsland* (dec.), nr. 420/07, 5 oktober 2010.

211 EU (2007), Verdrag van Lissabon tot wijziging van het Verdrag betreffende de Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap, ondertekend te Lissabon, 13 december 2007, PB C 306 van 17.12.2007, blz. 1. Zie ook de geconsolideerde versies van het Verdrag betreffende de Europese Unie, PB C 326 van 26.10.2012, blz. 13, en het Verdrag betreffende de werking van de Europese Unie, PB C 326 van 26.10.2012, blz. 47.

mogelijke scenario's voor de wijze waarop een claim van een betrokkene dat zijn of haar gegevensbeschermingsrechten zijn geschonden kan leiden tot een procedure bij het HvJ-EU.

In het eerste scenario zou de betrokkene het directe slachtoffer moeten zijn van een administratieve of regelgevingshandeling die een schending van het recht op gegevensbescherming van de desbetreffende persoon inhoudt. Volgens artikel 263, vierde alinea, van het VWEU kan:

> *"Iedere natuurlijke of rechtspersoon (...) beroep instellen tegen handelingen die tot hem gericht zijn of die hem rechtstreeks en individueel raken, alsmede tegen regelgevingshandelingen die hem rechtstreeks raken en die geen uitvoeringsmaatregelen met zich meebrengen."*

Slachtoffers van onrechtmatige verwerking van hun gegevens door een EU-orgaan kunnen rechtstreeks beroep instellen bij het Gerecht van de Europese Unie, dat het orgaan is dat bevoegd is om recht te spreken in zaken die onder de verordening gegevensbescherming EU-instellingen vallen. De mogelijkheid om rechtstreeks naar het HvJ-EU te gaan bestaat ook indien iemands wettelijke situatie rechtstreeks wordt beïnvloed door een wettelijke bepaling van de EU.

Het tweede scenario heeft betrekking op de bevoegdheid van het HvJ-EU krachtens artikel 267 van het VWEU om prejudiciële beslissingen te geven.

Betrokkenen kunnen, in het kader van een binnenlandse procedure, de nationale rechtbank verzoeken om bij het Hof van Justitie om verduidelijking te vragen inzake de uitleg van de EU-Verdragen en de uitleg en geldigheid van handelingen van de instellingen, organen, bureaus en agentschappen van de EU. Deze verduidelijkingen zijn bekend als prejudiciële beslissingen. Dit is geen direct beroep in rechte voor de klager, maar het stelt de nationale rechtbanken in staat ervoor te zorgen dat ze de correcte interpretatie van het EU-recht toepassen.

Als een partij bij een procedure voor de nationale rechtbank verzoekt om verwijzing van een rechtsvraag naar het HvJ-EU, zijn alleen rechtbanken die als rechtbank in laatste instantie fungeren, tegen wier uitspraak geen rechtsmiddel meer open staat, verplicht om hieraan te voldoen.

Voorbeeld: In *Kärntner Landesregierung en anderen*[212] heeft het Oostenrijkse constitutioneel hof het HvJ-EU vragen voorgelegd met betrekking tot de geldigheid van de artikel en 3 tot en met 9 van Richtlijn 2006/24/EG (*richtlijn gegevensbewaring)* in het licht van de artikel en 7, 9 en 11 van het Handvest en met betrekking tot de verenigbaarheid van sommige bepalingen van de Oostenrijkse federale telecommunicatiewet ter omzetting van de richtlijn gegevensbewaring met aspecten van de richtlijn gegevensbescherming en de verordening gegevensbescherming EU-instellingen.

De heer Seitlinger, een van de verzoekers in de procedure bij het constitutioneel hof, stelt daarin dat hij de telefoon, internet en e-mail zowel voor zijn werk als voor privédoeleinden gebruikt. Dientengevolge verstuurt en ontvangt hij informatie via openbare telecommunicatienetwerken. Volgens de Oostenrijkse telecommunicatiewet van 2003 is zijn telecommunicatieaanbieder wettelijk verplicht om gegevens over zijn gebruik van het netwerk te verzamelen en op te slaan. De heer Seitlinger realiseerde zich op een zeker moment dat deze verzameling en opslag van zijn persoonsgegevens op geen enkele wijze noodzakelijk is voor de verwezenlijking van het technische doeleinde om informatie via het netwerk van A tot B te sturen. Noch is de verzameling en de opslag van deze gegevens ook maar in de verste verte noodzakelijk voor factureringsdoeleinden. De heer Seitlinger stelt dat hij zeker geen toestemming heeft gegeven voor dit gebruik van persoonsgegevens. De enige reden voor de verzameling en opslag van al deze extra gegevens is de Oostenrijkse telecommunicatiewet van 2003.

De heer Seitlinger heeft daarom een procedure aanhangig gemaakt bij het Oostenrijkse constitutioneel hof waarin hij aanvoert dat de wettelijke verplichtingen voor zijn telecommunicatieaanbieder een inbreuk vormen op zijn grondrechten uit hoofde van artikel 8 van het Handvest.

Het HvJ-EU geeft alleen een beslissing over de bestanddelen van het bij hem ingediende verzoek om een prejudiciële beslissing. De nationale rechtbank blijft bevoegd om een beslissing over de oorspronkelijke zaak te nemen.

In beginsel moet het HvJ-EU de aan hem voorgelegde vragen beantwoorden. Het HvJ-EU kan niet weigeren om een prejudiciële beslissing te geven op grond van de

212 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland en Seitlinger en anderen*, 8 april 2014.

overweging dat dit antwoord noch relevant, noch tijdig zou zijn voor de desbetreffende zaak. Het kan echter wel weigeren als de vraag niet onder zijn bevoegdheid valt.

Tot slot kan de betrokkene, indien zijn of haar gegevensbeschermingsrechten, die worden gegarandeerd door artikel 16 van het VWEU, mogelijk zijn geschonden door een EU-instelling of -orgaan in het kader van de verwerking van persoonsgegevens, de zaak voorleggen aan het Gerecht van de Europese Unie (artikel 32, leden 1 en 4, van de verordening gegevensbescherming EU-instellingen). Hetzelfde geldt voor beslissingen van de EDPS met betrekking tot dergelijke schendingen (artikel 32, lid 3, van de verordening gegevensbescherming EU-instellingen).

Hoewel het Gerecht van de Europese Unie bevoegd is om uitspraak te doen in aangelegenheden die binnen het toepassingsgebied van de verordening gegevensbescherming EU-instellingen vallen, moet deze persoon, indien hij of zij in de hoedanigheid van personeelslid van een EU-instelling of -orgaan verhaal wil halen, beroep instellen bij het Gerecht voor ambtenarenzaken van de Europese Unie.

Voorbeeld: Het arrest *Europese Commissie / The Bavarian Lager Co. Ltd*[213] illustreert de rechtsmiddelen die open staan tegen activiteiten of besluiten van EU-instellingen en -organen die relevant zijn voor gegevensbescherming.

Bavarian Lager had de Europese Commissie verzocht om toegang tot de volledige notulen van een vergadering van de Commissie die betrekking zou hebben op wettelijke vraagstukken die relevant waren voor de onderneming. De Commissie had het toegangsverzoek van de onderneming geweigerd op grond van zwaarwegende belangen inzake gegevensbescherming.[214] Bavarian Lager had tegen dit besluit, overeenkomstig artikel 32 van de verordening gegevensbescherming EU-instellingen, een klacht ingediend bij het HvJ-EU, meer specifiek bij het Gerecht van eerste aanleg (de voorloper van het Gerecht van de Europese Unie). In zijn beslissing in zaak T-194/04, *Bavarian Lager / Commissie*, had het Gerecht van eerste aanleg het besluit van de Commissie om het toegangsverzoek te weigeren vernietigd. De Europese Commissie stelde beroep tegen deze beslissing in bij het Hof van Justitie van de Europese Unie. Het arrest van het HvJ (door de Grote kamer) legde het arrest van het Gerecht van eerste

213 HvJ-EU, zaak C-28/08 P, *Europese Commissie / The Bavarian Lager Co. Ltd*, 29 juni 2010.

214 Voor een analyse van de argumentatie, zie: EDPS (2011),"Public access to documents containing personal data after the Bavarian Lager ruling", Brussel, EDPS.

aanleg terzijde en bekrachtigde het besluit van de Europese Commissie om het verzoek om toegang niet in te willigen.

5.3.4. Sancties

In het RvE-recht bepaalt artikel 10 van Verdrag 108 dat elke Partij zich moet verbinden aan passende sancties en rechtsmiddelen ter zake van schending van bepalingen van het interne recht waarmee uitvoering wordt gegeven aan de grondbeginselen van gegevensbescherming als vervat in Verdrag 108.[215] **In het EU-recht** bepaalt artikel 24 het volgende: "De lidstaten nemen passende maatregelen om de onverkorte toepassing van de bepalingen van deze richtlijn te garanderen en stellen met name de sancties vast die gelden bij inbreuk op de (...) vastgestelde bepalingen".

Beide instrumenten geven lidstaten een ruime discretionaire marge om passende sancties en verhaalsmogelijkheden vast te stellen. Geen van beide instrumenten geeft specifieke aanwijzingen voor de aard van of het type sancties, noch worden er voorbeelden van mogelijke sancties gegeven.

Echter:

> *"Hoewel de EU-lidstaten beschikken over een discretionaire marge bij het bepalen van de maatregelen die het meest passend zijn om rechten die personen ontlenen aan het EU-recht te vrijwaren, in overeenstemming met het beginsel van loyale samenwerking als neergelegd in artikel 4, lid 3, van het VEU, moeten de minimumeisen van doeltreffendheid, gelijkwaardigheid, evenredigheid en afschrikwekkendheid worden gerespecteerd."*[216]

Het HvJ-EU heeft herhaaldelijk opgemerkt dat het nationale recht niet volledig vrij is om sancties te bepalen.

Voorbeeld: In *Von Colson en Kamann / Land Nordrhein-Westfalen*[217] heeft het HvJ-EU erop gewezen dat alle lidstaten waartoe een richtlijn is gericht verplicht zijn om in het nationale rechtsstelsel alle noodzakelijke maatregelen vast te

215 EHRM, *I. / Finland*, nr. 20511/03, 17 juli 2008; EHRM, *K.U. / Finland*, nr. 2872/02, 2 december 2008.

216 FRA (2012), *Advies van het Bureau voor de grondrechten van de Europese Unie over het voorgestelde hervormingspakket gegevensbescherming*, 2/2012, Wenen, 1 oktober 2012, blz. 27.

217 HvJ-EU, zaak C-14/83, *Von Colson en Kamann / Land Nordrhein-Westfalen*, 10 april 1984.

stellen om te waarborgen dat de richtlijn volledig doeltreffend is, in overeenstemming met de beoogde doelstelling ervan. Het Hof oordeelde dat hoewel het aan de lidstaten is om de vorm en middelen te kiezen om ervoor te zorgen dat een richtlijn ten uitvoer wordt gelegd, deze vrijheid geen effect heeft op de op hen rustende verplichting. In het bijzonder moet een doeltreffende voorziening in rechte een persoon in staat stellen om het recht in kwestie in zijn volledige inhoudelijke strekking uit te oefenen en af te dwingen. Om te bereiken dat er een daadwerkelijke en doeltreffende rechtsbescherming wordt geboden, moeten rechtsmiddelen tot strafrechtelijke en/of compensatoire procedures met een afschrikwekkend effect leiden.

Sancties voor inbreuken op het EU-recht door EU-instellingen of -organen worden, vanwege het bijzondere toepassingsgebied van de verordening gegevensbescherming EU-instellingen, alleen voorzien in de vorm van disciplinaire maatregelen. Volgens artikel 49 van de verordening kan "[d]e ambtenaar of een ander personeelslid van de Europese Gemeenschappen die, opzettelijk of uit nalatigheid, de bij of krachtens deze verordening op hem rustende verplichtingen niet nakomt, (...) aan een tuchtmaatregel worden onderworpen (...)".

6

Grensoverschrijdend verkeer van gegevens

EU	Behandelde onderwerpen	RvE
Grensoverschrijdend verkeer van gegevens		
Richtlijn gegevensbescherming, artikel 25, lid 1 HvJ-EU, zaak C-101/01, *Bodil Lindqvist*, 6 november 2003	**Definitie**	Verdrag 108, Aanvullend Protocol, artikel 2, lid 1
Vrij verkeer van gegevens		
Richtlijn gegevensbescherming, artikel 1, lid 2	**Tussen EU-lidstaten**	
	Tussen partijen bij Verdrag 108	Verdrag 108, artikel 12, lid 2
Richtlijn gegevensbescherming, artikel 25	**Naar derde landen met een passend niveau van gegevensbescherming**	Verdrag 108, Aanvullend Protocol, artikel 2, lid 1
Richtlijn gegevensbescherming, artikel 26, lid 1	**Naar derde landen in specifieke gevallen**	Verdrag 108, Aanvullend Protocol, artikel 2, lid 2, onder a)
Beperkt verkeer van gegevens naar derde landen		
Richtlijn gegevensbescherming, artikel 26, lid 2 Richtlijn gegevensbescherming, artikel 26, lid 4	**Contractbepalingen**	Verdrag 108, Aanvullend Protocol, artikel 2, lid 2, onder b) Gids voor het opstellen van contractbepalingen
Richtlijn gegevensbescherming, artikel 26, lid 2	**Bindende ondernemingsregels**	

EU	Behandelde onderwerpen	RvE
Voorbeelden: PNR-overeenkomst tussen de EU en de VS SWIFT-overeenkomst tussen de EU en de VS	Bijzondere internationale overeenkomsten	

De richtlijn gegevensbescherming voorziet niet alleen in vrij verkeer van gegevens tussen de lidstaten, maar bevat ook bepalingen met vereisten voor de doorgifte van persoonsgegevens aan derde landen buiten de EU. Ook de RvE heeft het belang van uitvoeringsvoorschriften voor grensoverschrijdend verkeer van gegevens naar derde landen onderkend en het Aanvullend Protocol bij Verdrag 108 aangenomen. In dit Protocol zijn de belangrijkste regelgevingskenmerken met betrekking tot grensoverschrijdend gegevensverkeer van de verdragspartijen en EU-lidstaten overgenomen.

6.1. Aard van het grensoverschrijdend verkeer van gegevens

Belangrijkste punten

- Grensoverschrijdend verkeer van gegevens is de doorgifte van persoonsgegevens aan een ontvanger die onderworpen is aan een buitenlandse rechtsmacht.

Artikel 2, lid 1, van het Aanvullend Protocol bij Verdrag 108 omschrijft grensoverschrijdend verkeer als de doorgifte van persoonsgegevens naar een ontvanger die valt onder een buitenlandse rechtsmacht. Artikel 25, lid 1, van de richtlijn gegevensbescherming reguleert de doorgifte van "persoonsgegevens die aan een verwerking worden onderworpen of die bestemd zijn om na doorgifte te worden verwerkt (...) naar een derde land (...)". Dergelijke doorgiften zijn alleen toegestaan als ze plaatsvinden overeenkomstig de voorschriften van artikel 2 van het Aanvullend Protocol bij Verdrag 108, en voor de EU-lidstaten tevens overeenkomstig de artikel en 25 en 26 van de richtlijn gegevensbescherming.

Voorbeeld: In *Bodil Lindqvist*[218] oordeelde het HvJ-EU dat "het vermelden van verschillende personen op een internetpagina met hun naam of anderszins,

218 HvJ-EU, zaak C-101/01, *Bodil Lindqvist*, 6 november 2003, punten 27, 68 en 69.

bijvoorbeeld met hun telefoonnummer of informatie over hun werksituatie en hun liefhebberijen, als een 'geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens' in de zin van artikel 3, lid 1, van richtlijn 95/46 is aan te merken".

Vervolgens wees het Hof erop dat de richtlijn ook specifieke voorschriften omvat die bedoeld zijn om de lidstaten in staat te stellen toezicht te houden op de doorgifte van persoonsgegevens naar derde landen.

Gezien echter, in de eerste plaats, de ontwikkeling van internet ten tijde van het opstellen van de richtlijn, en, in de tweede plaats, het ontbreken in de richtlijn van criteria voor het gebruik van internet, "kan niet worden aangenomen dat het de bedoeling was van de gemeenschapswetgever (...) het begrip 'doorgifte van gegevens naar een derde land' ook te laten gelden voor de handeling van een persoon (...) die gegevens op een internetpagina plaatst, ook wanneer die gegevens daarmee toegankelijk worden gemaakt voor personen uit derde landen die de technische middelen hebben om zich toegang daartoe te verschaffen".

Anderzijds zou, indien de richtlijn "aldus werd uitgelegd dat er sprake is van een 'doorgifte van gegevens naar een derde land' telkens wanneer persoonsgegevens op een internetpagina worden geplaatst, (...) dat noodzakelijkerwijs een doorgifte zijn naar alle derde landen waar de technische middelen voor toegang tot internet bestaan. De bijzondere regeling van (...) die richtlijn zou daarmee, voor de verrichtingen op internet, noodzakelijkerwijs een algemene toepassingsregeling worden. Immers, zodra de Commissie (...) zou vaststellen dat één enkel derde land geen waarborgen voor een passend beschermingsniveau biedt, zouden de lidstaten het plaatsen van persoonsgegevens op het internet moeten verhinderen."

Het beginsel dat het louter publiceren van (persoons)gegevens niet wordt geacht grensoverschrijdend verkeer te zijn, is ook van toepassing op openbare registers, op internet, of op massamedia, zoals (elektronische) nieuwsbladen en televisie. Alleen communicatie die is gericht tot specifieke ontvangers komt in aanmerking om onder het begrip "grensoverschrijdend verkeer van gegevens" te vallen.

6.2. Vrij verkeer van gegevens tussen de lidstaten of tussen verdragspartijen

Belangrijkste punten

- De doorgifte van persoonsgegevens aan een andere lidstaat van de Europese Economische Ruimte of een andere partij bij Verdrag 108 moet vrij zijn van beperkingen.

In **het RvE-recht** moet er volgens artikel 12, lid 2, van Verdrag 108 vrij verkeer van persoonsgegevens tussen de partijen bij het verdrag bestaan. Het nationale recht mag de uitvoer van persoonsgegevens aan een verdragspartij niet beperken, tenzij:

- de bijzondere aard van de gegevens zulks vereist;[219] of
- de beperking nodig is om omzeiling van nationale wettelijke bepalingen inzake grensoverschrijdend verkeer van gegevens aan derde partijen te voorkomen.[220]

In **het EU-recht** is het beperken of het niet toestaan van vrij verkeer van gegevens tussen lidstaten om redenen van gegevensbescherming verboden bij artikel 1, lid 2, van de richtlijn gegevensbescherming. Het grondgebied waarop vrij verkeer van gegevens van toepassing is, is uitgebreid door de Overeenkomst betreffende de Europese Economische Ruimte (EER),[221] die IJsland, Liechtenstein en Noorwegen binnen de interne markt brengt.

Voorbeeld: Als een onderneming die deel uitmaakt van een internationale groep van ondernemingen met vestigingen in verschillende EU-lidstaten, waaronder Slovenië en Frankrijk, persoonsgegevens doorgeeft van Slovenië naar Frankrijk, mag dit verkeer van gegevens niet door het Sloveense nationale recht worden beperkt of verboden.

219 Verdrag 108, artikel 12, lid 3, onder a).

220 *Ibid.,* artikel 12, lid 3, onder b).

221 Besluit van de Raad en de Commissie van 13 december 1993 betreffende de sluiting van de Overeenkomst betreffende de Europese Economische Ruimte tussen de Europese Gemeenschappen, hun Lid-Staten en de Republiek Oostenrijk, de Republiek Finland, de Republiek IJsland, het Vorstendom Liechtenstein, het Koninkrijk Noorwegen, het Koninkrijk Zweden en de Zwitserse Bondsstaat, PB L 1 van 3.1.1994, blz. 1.

Als de in Slovenië gevestigde onderneming dezelfde persoonsgegevens echter wil doorgeven aan de moedermaatschappij in de Verenigde Staten, moet de Sloveense gegevensexporteur de bij het Sloveense recht ingestelde procedure voor grensoverschrijdend verkeer van gegevens naar derde landen zonder passende gegevensbescherming volgen, tenzij de moedermaatschappij zich heeft aangesloten bij de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer (Safe Harbor Privacy Principles), een vrijwillige gedragscode voor landen die een passend niveau van gegevensbescherming willen bieden (zie paragraaf 6.3.1).

Grensoverschrijdend verkeer van lidstaten van de EER voor doeleinden die buiten het toepassingsgebied van de interne markt vallen, zoals in het kader van strafrechtelijke onderzoeken, zijn echter niet onderworpen aan de bepalingen van de richtlijn gegevensbescherming en vallen daarom niet onder het beginsel van vrij verkeer van gegevens. Wat betreft de RvE zijn alle grondgebieden opgenomen in het toepassingsgebied van Verdrag 108 en het Aanvullend Protocol bij Verdrag 108, hoewel de verdragspartijen uitzonderingen kunnen maken. Alle lidstaten van de EER zijn partij bij Verdrag 108.

6.3. Vrij verkeer van gegevens naar derde landen

Belangrijkste punten

- De doorgifte van persoonsgegevens aan derde landen mag in de nationale gegevensbeschermingswetgeving niet worden gebonden aan beperkingen indien:
  - de gepastheid van de gegevensbescherming die aan de zijde van de ontvanger wordt geboden is vastgesteld; of
  - dit noodzakelijk is in het bijzondere belang van de betrokkene of vanwege rechtmatige prevalerende belangen van anderen, in het bijzonder belangrijke algemene belangen.
- Passende gegevensbescherming in een derde land betekent dat de belangrijkste beginselen van gegevensbescherming effectief ten uitvoer zijn gelegd in het nationale recht van dit land.
- In het EU-recht wordt de gepastheid van de gegevensbescherming in een derde land beoordeeld door de Europese Commissie. In het RvE-recht wordt het overgelaten aan het nationale recht hoe wordt beoordeeld of de gegevensbescherming passend is.

6.3.1. Vrij verkeer van gegevens vanwege passende bescherming

Volgens **het RvE-recht** mag het nationale recht vrij verkeer van gegevens naar niet-verdragspartijen toestaan indien de ontvangende staat of organisatie zorgt voor een passend niveau van bescherming voor de beoogde doorgifte van gegevens.[222] Het nationale recht bepaalt hoe het niveau van gegevensbescherming in een derde land moet worden beoordeeld en wie dat moet doen.

In **het EU-recht** voorziet artikel 25, lid 1, van de richtlijn gegevensbescherming in het vrije verkeer van gegevens naar derde landen met een passend niveau van gegevensbescherming. Het vereiste dat het niveau van gegevensbescherming passend moet zijn, en niet gelijkwaardig, maakt het mogelijk om verschillende methoden voor de tenuitvoerlegging van gegevensbescherming te erkennen. Volgens artikel 25, lid 6, van de richtlijn is de Europese Commissie bevoegd om het niveau van gegevensbescherming in derde landen te beoordelen op basis van bevindingen betreffende de gepastheid van het beschermingsniveau en raadpleging van de Groep gegevensbescherming artikel 29, die substantieel heeft bijgedragen tot de interpretatie van de artikel en 25 en 26 van de richtlijn.[223]

Een bevinding betreffende de gepastheid van het beschermingsniveau van de Europese Commissie heeft een bindend effect. Wanneer de Europese Commissie een bevinding betreffende de gepastheid van het beschermingsniveau voor een bepaald land bekendmaakt in het Publicatieblad van de Europese Unie, zijn alle lidstaten van de EER en hun organen gehouden om het besluit te volgen, wat inhoudt dat gegevens vrij naar dit derde land kunnen worden doorgegeven zonder dat er eerst controle- of vergunningprocedures door nationale autoriteiten hoeven te worden uitgevoerd.[224]

222 Verdrag 108, Aanvullend Protocol, artikel 2, lid 1.

223 Zie bijvoorbeeld Groep gegevensbescherming artikel 29 (2003), *Werkdocument: doorgifte van persoonsgegevens naar derde landen: toepassing van artikel 26, lid 2, van de Richtlijn van de Europese Unie met betrekking tot gegevensbescherming bij bindende ondernemingsregels van toepassing op de internationale doorgifte van gegevens*, WP 74, Brussel, 3 juni 2003, en Groep gegevensbescherming artikel 29 (2005), *Werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995*, WP 114, Brussel, 25 november 2005.

224 Voor een voortdurend geactualiseerde lijst van landen waarvoor een positieve bevinding is afgegeven, zie de homepage van de Europese Commissie, directoraat-generaal Justitie, die is te vinden op: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

Ook kan de Europese Commissie delen van het rechtsstelsel van een derde land aan een beoordeling onderwerpen of zich tot specifieke onderwerpen beperken. Zo heeft de Commissie een bevinding uitgebracht over uitsluitend de Canadese wetgeving inzake private bedrijven die in het kader van commerciële activiteiten persoonsgegevens verwerken.[225] Ook zijn er diverse bevindingen betreffende de gepastheid van de gegevensbescherming bekendgemaakt voor doorgiften op grond van overeenkomsten tussen de EU en derde landen. Deze besluiten hebben uitsluitend betrekking op één enkel type doorgifte, zoals de doorgifte van passagiersgegevens (Passenger Name Records – PNR) door luchtvaartmaatschappijen aan grenscontroleautoriteiten van derde landen wanneer de vlucht wordt gemaakt van de EU naar bepaalde overzeese bestemmingen (zie paragraaf 6.4.3). Meer recente praktijken met de doorgifte van gegevens op grond van bijzondere overeenkomsten tussen de EU en derde landen maken dit soort bevindingen doorgaans overbodig, omdat wordt aangenomen dat de overeenkomst zelf een passend niveau van gegevensbescherming biedt.[226]

Een van de belangrijkste besluiten betreffende de gepastheid van gegevensbescherming heeft zelfs geen betrekking op een geheel van wettelijk bepalingen.[227] In plaats daarvan heeft dit besluit betrekking op een reeks regels die samen een soort gedragscode vormen en die bekend zijn onder de naam Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer. Deze beginselen zijn door de EU en de Verenigde Staten opgesteld voor Amerikaanse ondernemingen. Een onderneming kan zich bij de veiligehavenregeling aansluiten door een verklaring aan het Amerikaanse ministerie van Handel te zenden waarin zij verklaart de beginselen te onderschrijven, waarna het ministerie de onderneming in een openbare lijst opneemt. Aangezien een van de belangrijkste elementen van een passend

225 Europese Commissie (2002), Beschikking 2002/2/EG van de Commissie van 20 december 2001 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de gepastheid van de bescherming van persoonsgegevens geboden door de Canadese Personal information and Electronic Documents Act, PB L 2 van 4.1.2002, blz. 13.

226 Voorbeelden hiervan zijn de 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, PB L 215 van 11.8.2012, blz. 5-14, en de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het programma voor het traceren van terrorismefinanciering, PB L 8 van 13.1.2010, blz. 11-16.

227 Europese Commissie (2000), Beschikking 2000/520/EG van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende Vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd, PB L 215 van 15.8.2000, blz. 7.

beschermingsniveau de doeltreffendheid van de gegevensbescherming is, voorziet de veiligehavenregeling ook in een bepaalde mate van overheidstoezicht: Alleen ondernemingen die onder het toezicht van de Amerikaanse Federal Trade Commission vallen, kunnen zich bij de veiligehavenregeling aansluiten.

6.3.2. Vrij verkeer van gegevens in specifieke gevallen

In het RvE-recht staat artikel 2, lid 2, van het Aanvullend Protocol bij Verdrag 108 de overdracht van persoonsgegevens naar derde landen die geen passend niveau van gegevensbescherming waarborgen toe indien het nationale recht van dit land daarin voorziet en de overdracht noodzakelijk is vanwege de:

- bijzondere belangen van de betrokkene; of
- rechtmatige prevalerende belangen van anderen, in het bijzonder belangrijke algemene belangen.

In het EU-recht bevat artikel 26, lid 1, van de richtlijn gegevensbescherming bepalingen die vergelijkbaar zijn met die van het Aanvullend Protocol bij Verdrag 108.

Volgens de richtlijn kunnen de belangen van de betrokkene vrij verkeer van gegevens naar een derde land rechtvaardigen indien:

- de betrokkene daarvoor zijn of haar ondubbelzinnige toestemming heeft gegeven; of
- de betrokkene een contractuele verbintenis aangaat – of wil aangaan – die duidelijk vereist dat de gegevens worden doorgegeven aan een ontvanger in een derde land; of
- er een contract tussen een voor de verwerking verantwoordelijke en een derde is gesloten in het belang van de betrokkene; of
- de doorgifte noodzakelijk is om de vitale belangen van de betrokkene te vrijwaren; of

- de doorgifte geschiedt vanuit een openbaar register; dit is een geval van prevalerende algemene belangen, aangezien het publiek toegang moet hebben tot in openbare registers opgeslagen informatie.

De rechtmatige belangen van anderen kunnen vrij grensoverschrijdend verkeer van gegevens rechtvaardigen:[228]

- vanwege een zwaarwegend algemeen belang anders dan om redenen van nationale of openbare veiligheid, aangezien die niet onder de richtlijn gegevensbescherming vallen; of

- voor de vaststelling, de uitoefening of de verdediging van een recht in rechte.

De hierboven genoemde gevallen moeten worden begrepen als uitzonderingen op de regel dat ongeremde doorgifte van gegevens aan andere landen een passend niveau van gegevensbescherming in het ontvangende land vereist. Uitzonderingen moeten altijd restrictief worden uitgelegd. Dit is herhaaldelijk onderstreept door de Groep gegevensbescherming artikel 29 met betrekking tot artikel 26, lid 1, van de richtlijn gegevensbescherming, met name indien toestemming de beoogde grondslag voor de gegevensdoorgifte is.[229] De Groep gegevensbescherming artikel 29 heeft geconcludeerd dat de algemene regels voor de wettelijke betekenis van toestemming ook van toepassing zijn op artikel 26, lid 1, van de richtlijn gegevensbescherming. Indien het bijvoorbeeld in het kader van arbeidsverhoudingen niet duidelijk is of de door werknemers verleende toestemming daadwerkelijk vrije toestemming was, kunnen de gegevensdoorgiften niet worden gegrond op artikel 26, lid 1, onder a), van de richtlijn. In dergelijke gevallen zal artikel 26, lid 2, dat vereist dat nationale gegevensbeschermingsautoriteiten een vergunning moeten afgeven voor gegevensdoorgiften, van toepassing zijn.

228 Richtlijn gegevensbescherming, artikel 26, lid 1, onder d).

229 In het bijzonder Groep gegevensbescherming artikel 29 (2005), Werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995, WP 114, Brussel, 25 november 2005.

6.4. Beperkt verkeer van gegevens naar derde landen

Belangrijkste punten

- Voordat gegevens worden verzonden naar derde landen die geen passend niveau van gegevensbescherming waarborgen, moet de voor de verwerking verantwoordelijke mogelijk het beoogde verkeer van gegevens voorleggen aan de toezichthoudende autoriteit voor onderzoek.
- De voor de verwerking verantwoordelijke die gegevens wil uitvoeren moet tijdens dit onderzoek twee dingen aantonen:
  - dat er een rechtsgrondslag bestaat voor de doorgifte van gegevens aan de ontvanger; en
  - dat er aan de zijde van de ontvanger maatregelen zijn getroffen om een passende bescherming van de gegevens te waarborgen.
- Maatregelen voor het vaststellen van een passende gegevensbescherming aan de zijde van de ontvanger kunnen de volgende omvatten:
  - contractuele bepalingen tussen de gegevens uitvoerende voor de verwerking verantwoordelijke en de ontvanger van de gegevens in het derde land; of
  - bindende ondernemingsvoorschriften, doorgaans van toepassing voor gegevensdoorgiften binnen een multinationale groep van ondernemingen.
- Gegevensdoorgiften aan autoriteiten in derde landen kunnen ook in een bijzondere internationale overeenkomst worden geregeld.

De richtlijn gegevensbescherming en het Aanvullend Protocol bij Verdrag 108 staan toe dat in het nationale recht regelingen voor grensoverschrijdend verkeer naar derde landen die geen passend niveau van gegevensbescherming waarborgen worden opgenomen zolang de voor de verwerking verantwoordelijke speciale regelingen heeft getroffen om voor een passend niveau van gegevensbescherming aan de zijde van de ontvanger te zorgen en dit tegenover een bevoegde autoriteit kan aantonen. Dit vereiste wordt alleen uitdrukkelijk genoemd in het Aanvullend Protocol bij Verdrag 108; in de richtlijn gegevensbescherming wordt dit echter ook als standaardprocedure beschouwd.

6.4.1. Contractbepalingen

Zowel in **het RvE-recht** als in **het EU-recht** worden contractbepalingen tussen de gegevens exporterende voor de verwerking verantwoordelijke en de ontvanger in het derde land genoemd als mogelijk middel om een voldoende niveau van gegevensbescherming aan de zijde van de ontvanger te waarborgen.

Op **EU-niveau** heeft de Europese Commissie met ondersteuning van de Groep gegevensbescherming artikel 29 modelcontractbepalingen ontwikkeld die officieel zijn gecertificeerd bij een beschikking van de Commissie als bewijs voor een passende gegevensbescherming.[230] Omdat besluiten van de Commissie in al hun onderdelen verbindend zijn voor de lidstaten, moeten de nationale autoriteiten die belast zijn met het toezicht op grensoverschrijdend verkeer van gegevens in hun procedures deze modelcontractbepalingen erkennen.[231] Als de gegevens exporterende voor de verwerking verantwoordelijke en de ontvanger in het derde land overeenstemming bereiken en deze bepalingen ondertekenen, zou dit voor de toezichthoudende autoriteit voldoende bewijs moeten zijn dat voor passende waarborgen is gezorgd.

Het bestaan van modelcontractbepalingen in het wettelijk kader van de EU verbiedt voor de verwerking verantwoordelijken niet om andere ad-hoccontractbepalingen te formuleren. Deze zouden echter hetzelfde niveau van bescherming moeten bieden als de modelcontractbepalingen. De belangrijkste kenmerken van de modelcontractbepalingen zijn de volgende:

- Een derdenbeding dat betrokkenen in staat stelt om contractuele rechten uit te oefenen, ook als ze geen partij bij het contract zijn;

- De ontvanger of importeur van de gegevens stemt ermee in om in geval van een geschil te worden onderworpen aan de procedure van de toezichthoudende autoriteit en/of de bevoegde rechtbanken van de gegevens exporterende voor de verwerking verantwoordelijke.

Er zijn nu twee reeksen modelcontractbepalingen beschikbaar voor doorgiften tussen voor de verwerking verantwoordelijken, waaruit de gegevens exporterende

230 Richtlijn gegevensbescherming, artikel 26, lid 4.

231 VWEU, artikel 288.

voor de verwerking verantwoordelijke kan kiezen.[232] Voor doorgiften tussen voor de verwerking verantwoordelijken en verwerkers bestaat er slechts één reeks modelcontractbepalingen.[233]

In de context van **het RvE-recht** heeft het Raadgevend Comité van Verdrag 108 een gids uitgebracht over het opstellen van contractbepalingen.[234]

6.4.2. Bindende ondernemingsregels

Bij multilaterale bindende ondernemingsregels (Binding Corporate Rules – BCR) zijn vaak diverse Europese gegevensbeschermingsautoriteiten tegelijk betrokken.[235] Om goedkeuring van bindende ondernemingsregels te verkrijgen moet het ontwerp ervan, samen met de gestandaardiseerde aanvraagformulieren, worden toegezonden aan de leidende autoriteit.[236] De leidende autoriteit is identificeerbaar op het gestandaardiseerde aanvraagformulier. Deze autoriteit informeert alle andere toezichthoudende autoriteiten in EER-lidstaten met vestigingen van de groep, hoewel hun deelname aan de evaluatie van de bindende ondernemingsregels vrijwillig is. Hoewel het resultaat van de evaluatie niet bindend is, zouden alle gegevensbeschermingsautoriteiten dit moeten integreren in hun formele vergunningsprocedures.

232 Reeks I is vervat in de bijlage bij Europese Commissie (2001), Beschikking 2001/497/EG van de Commissie van 15 juni 2001 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen krachtens Richtlijn 95/46/EG, PB L 181 van 4.7.2001, blz. 19; Reeks II is vervat in de bijlage bij Europese Commissie (2004), Beschikking 2004/915/EG van de Commissie van 27 december 2004 tot wijziging van Beschikking 2001/497/EG betreffende de invoering van alternatieve modelcontractbepalingen voor de doorgifte van persoonsgegevens naar derde landen, PB L 385 van 29.12.2004, blz. 74.

233 Europese Commissie (2010), Besluit 2010/87 van de Commissie van 5 februari 2010 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG van het Europees Parlement en de Raad, PB L 39 van 12.2.2010, blz. 5.

234 RvE, Raadgevend Comité van Verdrag 108 (2002), "Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data".

235 De inhoud en structuur van passende bindende voorschriften voor ondernemingen als toegelicht in Groep gegevensbescherming artikel 29 (2008), *Werkdocument voor het opzetten van een kader voor de structuur van bindende ondernemingsregels*, WP 154, Brussel, 24 juni 2008, en in Groep gegevensbescherming artikel 29 (2008), Werkdocument voor het opzetten van een tabel met de elementen en beginselen die zijn te vinden in bindende ondernemingsregels, WP 153, Brussel, 24 juni 2008.

236 Groep gegevensbescherming artikel 29, *Aanbeveling 1/2007 inzake de standaardaanvraag voor goedkeuring van bindende ondernemingsregels voor de doorgifte van persoonsgegevens*, WP 133, Brussel, 10 januari 2007.

6.4.3. Bijzondere internationale overeenkomsten

De EU heeft bijzondere overeenkomsten gesloten voor twee typen gegevensdoorgiften:

Passenger Name Records

Passagiersgegevens (Passenger Name Records – PNR) worden verzameld door luchtvaartmaatschappijen tijdens het reserveringsproces en omvatten de namen, adressen, creditcardgegevens en stoelnummers van passagiers. Krachtens het recht van de Verenigde Staten zijn luchtvaartmaatschappijen verplicht om deze gegevens ter beschikking van het Amerikaanse ministerie van Binnenlandse Veiligheid te stellen voordat de vlucht vertrekt. Dit geldt voor vluchten naar en vanuit de Verenigde Staten.

Om een passend beschermingsniveau van PNR gegevens te waarborgen, en in overeenstemming met het in richtlijn 95/46/EG bepaalde, is in 2004 het "PNR-pakket"[237] aangenomen, welke de gepastheid van het beschermingsniveau van de verwerkingen uitgevoerd door het Amerikaanse ministerie van Binnenlandse Veiligheid (Department of Homeland Security – DHS) behelst.

Na de ongeldigverklaring van het PNR-pakket door het HvJ-EU[238] sloten de EU en de Verenigde Staten twee aparte overeenkomsten met een tweeledig doel: in de eerste plaats om een juridische grondslag te bieden voor de doorgifte van PNR-gegevens aan de Amerikaanse autoriteiten ; en in de tweede plaats om te zorgen voor een passend niveau van gegevensbescherming in het ontvangende land.

De eerste overeenkomst over de wijze waarop de EU-lidstaten en de Verenigde Staten gegevens delen en beheren, ondertekend in 2012, vertoonde diverse

237 Besluit 2004/496/EG van de Raad van 17 mei 2004 betreffende de sluiting van een overeenkomst tussen de Europese Gemeenschap en de Verenigde Staten van Amerika inzake de verwerking en overdracht van PNR-gegevens door luchtvaartmaatschappijen aan het Bureau of Customs and Border Protection van het ministerie van Binnenlandse Veiligheid van de Verenigde Staten van Amerika, PB L 183 van 20.05.2004, blz. 83, en Beschikking 2004/535/EG van de Commissie van 14 mei 2004 betreffende de passende bescherming van persoonsgegevens in het Passenger Name Record van vliegtuigpassagiers die aan het Bureau of Customs and Border Protection van de Verenigde Staten worden doorgegeven (Kennisgeving geschied onder nummer C(2004) 1914) PB L 235 van 06.07.2004, blz. 11–22.

238 Bijgewerkte nden moeten de gegevens gedepersonaliseerd en gemaskeerd wordenomst HvJ-EU gevoegde zaken C-317/04 en C-318/04, *Europees Parlement / Raad van de Europese Unie*, 30 mei 2006, punten 57, 58 en 59, waarin het Hof oordeelde dat zowel de beslissing omtrent gepastheid en de overeenkomst aangaande de verwerkingen buiten het toepassingsbereik van de richtlijn vallen.

tekortkomingen en is vervangen door een nieuwe overeenkomst, die voor meer rechtszekerheid zorgt.[239] De nieuwe overeenkomst houdt aanmerkelijke verbeteringen in. De overeenkomst beperkt en verduidelijkt de doeleinden waarvoor de informatie kan worden gebruikt, zoals voor de bestrijding van ernstige transnationale criminaliteit en terrorisme, en stelt een termijn voor de bewaring van gegevens: na zes maanden moeten de gegevens gedepersonaliseerd en gemaskeerd worden. Als hun gegevens worden misbruikt, heeft eenieder het recht om administratieve of gerechtelijke rechtsmiddelen uit te oefenen overeenkomstig het Amerikaanse recht. Ook hebben ze het recht om hun eigen PNR-gegevens in te zien en het ministerie van Binnenlandse Veiligheid te verzoeken de gegevens te rectificeren, met inbegrip van de mogelijkheid van uitwissing, indien de informatie onjuist is.

De overeenkomst, die in werking is getreden op 1 juli 2012, zal gedurende zeven jaar van kracht blijven, tot 2019.

In december 2011 heeft de Raad van de Europese Unie de sluiting van een bijgewerkte overeenkomst tussen de EU en Australië inzake de verwerking en doorgifte van PNR-gegevens goedgekeurd.[240] De overeenkomst tussen de EU and Australië inzake PNR-gegevens is een nieuwe stap in de uitvoering van de EU-agenda, die het opstellen van globale PNR-richtsnoeren,[241] het opzetten van een regeling voor

239 Besluit 2012/472/EU van de Raad van 26 april 2012 tot sluiting van de 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, PB L 215 van 11.8.2012, blz. 4. De tekst van de overeenkomst is gehecht aan dit besluit, PB L 215 van 11.8.2012, blz. 5-14.

240 Besluit 2012/381/EU van de Raad van 13 december 2011 inzake de sluiting van de 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, PB L 186 van 14.7.2012, blz. 3. De tekst van de overeenkomst, welke een voorgaande overeenkomst uit 2008 verving, is gehecht aan dit besluit, PB L 186 van 14.7.2012, blz. 4-16.

241 Zie met name de Mededeling van de Commissie van 21 september 2010 over de algemene aanpak van de doorgifte van passagiersgegevens (Passenger Name Record - PNR) aan derde landen, COM(2010) 492 definitief, Brussel, 21 september 2010. Zie ook Groep gegevensbescherming artikel 29 (2010), Advies 7/2010 betreffende de mededeling van de Europese Commissie over de algemene aanpak van de doorgifte van passagiersgegevens (Passenger Name Record - PNR) aan derde landen, WP 178, Brussel 12 november 2010.

PNR-gegevens voor de EU[242] en het sluiten van overeenkomsten met derde landen[243] omvat.

Betalingsberichtenverkeer

De in België gevestigde Society for Worldwide Interbank Financial Telecommunication (SWIFT), die de verwerker is voor het grootste deel van de wereldwijde financiële transacties door Europese banken, werkte met een "mirror" rekencentrum in de Verenigde Staten en werd geconfronteerd met het verzoek om gegevens te verstrekken aan het Amerikaanse ministerie van Financiën voor onderzoeksdoeleinden in verband met terrorismebestrijding.[244]

Vanuit EU-perspectief was er geen toereikende rechtsgrondslag voor de verstrekking van deze grotendeels Europese gegevens, die in de Verenigde Staten uitsluitend toegankelijk waren omdat een van de gegevensverwerkingscentra van SWIFT in de Verenigde Staten was gevestigd.

In 2010 is een bijzondere overeenkomst tussen de EU en de Verenigde Staten gesloten, die bekend is als de "SWIFT-overeenkomst", om voor de noodzakelijk rechtsgrondslag te zorgen en een passende gegevensbescherming te waarborgen.[245]

242 Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende het gebruik van persoonsgegevens van passagiers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en zware criminaliteit, COM(2011) 32 definitief, Brussel, 2 februari 2011. Op 13 april 2011 heeft het Europees Parlement het FRA verzocht om een advies over dit voorstel en de vraag of het voorstel in overeenstemming is met het Handvest van de grondrechten van de Europese Unie. Zie: FRA (2011), Advies 1/2011 – Passenger Name Record, Wenen, 14 juni 2011.

243 De EU onderhandelt over een nieuwe PNR-overeenkomst met Canada, welke de overeenkomst uit 2006 die momenteel van kracht is zal vervangen.

244 Zie in dit verband Groep gegevensbescherming artikel 29 (2011), *Advies 14/2011* over gegevensbeschermingskwesties die verband houden met het voorkomen van het witwassen van geld en van het financieren van terrorisme, WP 186, Brussel, 13 juni 2011, Groep gegevensbescherming artikel 29 (2006), *Advies 10/2006* over de verwerking van persoonsgegevens door de Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128, Brussel, 22 november 2006, en de Belgische Commissie voor de bescherming van de persoonlijke levenssfeer (Commission de la protection de la vie privée) (2008), Beslissing betreffende de controle en de aanbevelingsprocedure ingeleid met betrekking tot de maatschappij SWIFT cvba, 9 december 2008.

245 Besluit 2010/412/EU van de Raad van 13 juli 2010 betreffende de sluiting van de Overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en doorgifte van gegevens betreffende het financiële berichtenverkeer van de Europese Unie naar de Verenigde Staten ten behoeve van het programma voor het traceren van terrorismefinanciering, PB L 195 van 27.7.2010, blz. 3-4. De tekst van de overeenkomst is gehecht aan dit besluit, PB L 195 van 27.7.2010, blz. 5-14.

In het kader van deze overeenkomst blijven door SWIFT opgeslagen financiële gegevens verstrekt worden aan het Amerikaanse ministerie van Financiën met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van terrorisme of terrorismefinanciering. Het Amerikaanse ministerie van Financiën kan financiële gegevens opvragen bij SWIFT, mits een dergelijk verzoek:

- zo duidelijk mogelijk vermeldt welke financiële gegevens noodzakelijk zijn;
- een duidelijke motivering omvat van de omstandigheden waarin de gegevens nodig zijn;
- zorgvuldig op maat wordt gesneden opdat zo weinig mogelijk gegevens worden opgevraagd;
- in geen geval betrekking heeft op gegevens betreffende de gemeenschappelijke eurobetalingsruimte (Single Euro Payment Area – SEPA).

Europol moet een kopie van elk verzoek van het Amerikaanse ministerie van Financiën ontvangen en controleren of de beginselen van de SWIFT-overeenkomst worden nageleefd.[246] Indien wordt bevestigd dat dit het geval is, moet SWIFT de financiële gegevens rechtstreeks aan het Amerikaanse ministerie van Financiën verstrekken. Het ministerie moet de financiële gegevens opslaan in een beveiligde fysieke omgeving waar alleen analisten die onderzoek naar terrorisme en terrorismefinanciering uitvoeren toegang toe hebben, en de financiële gegevens mogen niet worden gekoppeld aan enige andere databank. Over het algemeen moeten financiële gegevens van SWIFT niet later dan vijf jaar na de ontvangst ervan worden uitgewist. Financiële gegevens die relevant zijn voor specifieke onderzoeken of vervolgingen mogen zo lang worden bewaard als noodzakelijk is voor het specifieke onderzoek of de specifieke vervolging waarvoor ze wordt gebruikt.

Het Amerikaanse ministerie van Financiën kan informatie uit de van SWIFT ontvangen gegevens verder doorgeven aan specifieke autoriteiten die bevoegd zijn voor rechtshandhaving, openbare veiligheid of terrorismebestrijding in of buiten de Verenigde Staten, en uitsluitend ten behoeve van onderzoek, opsporing, voorkoming of vervolging van terrorisme of terrorismefinanciering. Wanneer de informatie die verder wordt doorgegeven betrekking heeft op een burger of ingezetene van een

246 Het Gemeenschappelijk Controleorgaan van Europol heeft controles uitgevoerd op activiteiten ontplooid door Europol op dit gebied, de resultaten hiervan zijn beschikbaar op: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=nl.

EU-lidstaat, is voor het delen van deze informatie met de autoriteiten van een derde land de voorafgaande instemming van de bevoegde autoriteiten van de betrokken lidstaat vereist. Hierop kan een uitzondering worden gemaakt wanneer het uitwisselen van de gegevens van wezenlijk belang is voor het keren van een onmiddellijke en ernstige dreiging voor de openbare veiligheid.

Onafhankelijke toezichthouders, waaronder een door de Europese Commissie aangewezen persoon, controleren de naleving van de beginselen van de SWIFT-overeenkomst.

Betrokkenen hebben het recht om van de bevoegde EU-gegevensbeschermingsautoriteit bevestiging te verkrijgen dat hun gegevensbeschermingsrechten zijn geëerbiedigd. Ook hebben betrokken het recht te verlangen dat hun persoonsgegevens die door het Amerikaanse ministerie van Financiën overeenkomstig de SWIFT-overeenkomst zijn verwerkt en opgeslagen, worden gecorrigeerd, gewist of afgeschermd. De toegangsrechten van betrokkenen kunnen echter aan bepaalde wettelijke beperkingen worden gebonden. Indien de toegang tot persoonsgegevens wordt geweigerd, moet de betrokkene schriftelijk in kennis worden gesteld van die weigering en van de administratieve en gerechtelijke beroepsmogelijkheden waarover hij of zij in de Verenigde Staten beschikt.

De SWIFT-overeenkomst heeft een looptijd van vijf jaar, tot augustus 2015. De overeenkomst wordt automatisch verlengd met opeenvolgende perioden van één jaar, tenzij een van de partijen de andere ten minste zes maanden van tevoren schriftelijk in kennis stelt van haar voornemen om de overeenkomst niet te verlengen.

7

Gegevensbescherming in het kader van politiële en justitiële samenwerking in strafzaken

EU	Behandelde onderwerpen	RvE
	Algemeen	Verdrag 108
	Politie	Politieaanbeveling
		EHRM, *B.B. / Frankrijk*, nr. 5335/06, 17 december 2009
		EHRM, *S. en Marper / Verenigd Koninkrijk*, nrs. 30562/04 en 30566/04, 4 december 2008
		EHRM, *Vetter / Frankrijk*, nr. 59842/00, 31 mei 2005
	Cybercriminaliteit	Verdrag inzake cybercriminaliteit
Gegevensbescherming in het kader van grensoverschrijdende samenwerking tussen politiële en justitiële autoriteiten		
Kaderbesluit gegevensbescherming	Algemeen	Verdrag 108 Politieaanbeveling
Prüm-besluit	Voor bijzondere gegevens: vingerafdrukken, DNA, hooliganisme, enz.	Verdrag 108 Politieaanbeveling
Europol-besluit Eurojust-besluit Frontex-verordening	Door speciale agentschappen	Verdrag 108 Aanbeveling inzake politiegegevens

EU	Behandelde onderwerpen	RvE
Schengen II-besluit VIS-verordening Eurodac-verordening DIS-besluit	Door speciale gemeenschappelijke informatiesystemen	Verdrag 108 Politieaanbeveling EHRM, *Dalea / Frankrijk*, nr. 964/07, 2 februari 2010

Om de belangen van personen bij gegevensbescherming en de belangen van de samenleving bij gegevensverzameling ten behoeve van criminaliteitsbestrijding en het waarborgen van de nationale en openbare veiligheid tegen elkaar af te wegen, hebben de RvE en de EU specifieke rechtsinstrumenten vastgesteld.

7.1. RvE-recht inzake gegevensbescherming in het kader van politiële en justitiële samenwerking in strafzaken

Belangrijkste punten

- Verdrag 108 en de Politieaanbeveling van de RvE bestrijken de gegevensbescherming op alle werkterreinen van de politie.
- Het Verdrag inzake cybercriminaliteit (*Verdrag van Boedapest*) is een bindend internationaal rechtsinstrument dat betrekking heeft op strafbare feiten die zijn gepleegd tegen en door middel van elektronische netwerken.

Op Europees niveau bestrijkt Verdrag 108 alle gebieden van de verwerking van persoonsgegevens, en de bepalingen ervan beogen de verwerking van persoonsgegevens in het algemeen te reguleren. Dientengevolge is Verdrag 108 van toepassing op gegevensbescherming op het gebied van politiële en justitiële samenwerking in strafzaken, hoewel de verdragspartijen de toepassing ervan kunnen beperken.

De wettelijke taken van de politiële en justitiële autoriteiten vereisen vaak de verwerking van persoonsgegevens, wat ernstige gevolgen voor de betrokken personen met zich mee kan brengen. De Aanbeveling inzake politiegegevens die de RvE in 1987 heeft vastgesteld, bevat richtsnoeren voor de verdragspartijen over de wijze waarop ze gevolg zouden moeten geven aan de beginselen van Verdrag 108 in het kader van de verwerking van persoonsgegevens door politieautoriteiten.[247]

247 RvE, Comité van ministers (1987), Aanbeveling Rec(87)15 aan de lidstaten tot regeling van het gebruik van persoonsgegevens op politieel gebied, 17 september 1987.

7.1.1. De politieaanbeveling

Het EHRM heeft consistent geoordeeld dat de opslag en bewaring van persoonsgegevens door de politie of nationale veiligheidsautoriteiten een inmenging in artikel 8, lid 1, van het EVRM vormt. Een groot aantal arresten van het EHRM heeft betrekking op de rechtvaardiging van dergelijke inmengingen.[248]

Voorbeeld: In *B.B. / Frankrijk*[249] besloot het EHRM dat de opneming van een veroordeelde pleger van een zedendelict in een nationale databank onder artikel 8 van het EVRM viel. Aangezien echter voldoende waarborgen voor de gegevensbescherming ten uitvoer waren gelegd, zoals het recht van de betrokkene om uitwissing van de gegevens te verlangen, de beperkte opslagtermijn en de beperkte toegang tot de gegevens, was een billijk evenwicht bereikt tussen de concurrerende particuliere en algemene belangen die in het geding waren. Het Hof concludeerde dat artikel 8 van het EVRM niet was geschonden.

Voorbeeld: In *S. en Marper / Verenigd Koninkrijk*[250] waren beide verzoekers strafbare feiten ten laste gelegd, maar was geen van beiden daarvoor veroordeeld. Niettemin werden hun vingerafdrukken, DNA-profielen en celmonsters bewaard en opgeslagen door de politie. De onbeperkte bewaring van biometrische gegevens was wettelijk toegestaan indien een persoon werd verdacht van het plegen van een strafbaar feit, ook al was de verdachte later vrijgesproken of van rechtsvervolging ontslagen. Het EHRM oordeelde dat de algemene en ongedifferentieerde bewaring van persoonsgegevens, die niet tijdsgebonden was en waarbij vrijgesproken personen slechts over beperkte mogelijkheden beschikten om te verzoeken om uitwissing, een onevenredige inmenging in het recht van de verzoekers op eerbiediging van hun privéleven vormde. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Diverse andere arresten van het EHRM hebben betrekking op de rechtvaardiging van inmenging in het recht op gegevensbescherming door middel van surveillance.

248 Zie bijvoorbeeld EHRM, *Leander / Zweden*, nr. 9248/81, 26 maart 1987; EHRM, *M.M. / Verenigd Koninkrijk*, nr. 24029/07, 13 november 2012; EHRM, *M.K. / Frankrijk*, nr. 19522/09, 18 april 2013.

249 EHRM, *B.B. / Frankrijk*, nr. 5335/06, 17 december 2009.

250 EHRM, *S. en Marper / Verenigd Koninkrijk*, nrs. 30562/04 en 30566/04, 4 december 2008, punten 119 en 125.

Voorbeeld: In *Allan / Verenigd Koninkrijk*[251] waren privégesprekken van een gevangene met een vriend in de bezoekersruimte van de gevangenis en met een medegevangene in een cel in het geheim opgenomen door de autoriteiten. Het EHRM oordeelde dat het gebruik van de audio- en video-opnameapparatuur in de cel van de verzoeker en de bezoekersruimte van de gevangenis en op het lichaam van een medegevangene inmenging in het recht op een privéleven van de verzoeker inhield. Aangezien er geen wettelijk systeem bestond om het gebruik van geheime opnameapparatuur door de politie te reguleren, was genoemde inmenging niet in overeenstemming met de wet. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Voorbeeld: In *Klass en anderen / Duitsland*[252] stelden de verzoekers dat verschillende Duitse wetgevingshandelingen die de geheime surveillance van e-mail, post en telecommunicatie toestonden een schending van artikel 8 van het EVRM vormden, met name omdat de betrokken personen niet op de hoogte werden gebracht van de surveillancemaatregelen en geen rechtsmiddel konden instellen bij de rechtbanken zodra de maatregelen waren beëindigd. Het EHRM oordeelde dat een dreigende surveillance noodzakelijkerwijs een inmenging in de vrijheid van communicatie tussen gebruikers van de post- en telecommunicatiediensten vormde. Het Hof oordeelde echter dat er voor voldoende waarborgen tegen misbruik was gezorgd. De overweging van de Duitse wetgevende macht dat zulke maatregelen noodzakelijk waren in een democratische samenleving, in het belang van de nationale veiligheid en ter voorkoming van wanordelijkheden of strafbare feiten, was gerechtvaardigd. Het Hof concludeerde dat artikel 8 van het EVRM niet was geschonden.

Omdat gegevensverwerking door politieautoriteiten significante gevolgen kan hebben voor de betrokken personen, zijn gedetailleerde gegevensbeschermingsvoorschriften voor het bijhouden van databanken op dit gebied bijzonder noodzakelijk. In de Politieaanbeveling van de RvE worden met het oog hierop richtsnoeren gegeven voor de wijze waarop gegevens door de politie moeten worden verzameld, hoe gegevensbestanden op dit gebied moeten worden bewaard, wie toegang mag hebben tot deze bestanden, met inbegrip van de voorwaarden voor de doorgifte van gegevens aan politieautoriteiten van derde landen, hoe betrokkenen hun gegevensbeschermingsrechten moeten kunnen uitoefenen en hoe de controle door

251 EHRM, *Allan / Verenigd Koninkrijk*, nr. 48539/99, 5 november 2002.

252 EHRM, *Klass en anderen / Duitsland*, nr. 5029/71, 6 september 1978.

onafhankelijke autoriteiten moet worden uitgevoerd. Ook wordt een verplichting om voor een passende gegevensbeveiliging te zorgen vastgesteld.

De aanbeveling voorziet niet in een ongelimiteerde, ongedifferentieerde verzameling van gegevens door politieautoriteiten. De verzameling van persoonsgegevens door politieautoriteiten wordt beperkt tot wat noodzakelijk is om een reëel gevaar of een specifiek strafbaar feit te voorkomen. Het verzamelen van aanvullende gegevens moet zijn gebaseerd op specifieke nationale wetgeving. De verwerking van gevoelige gegevens moet worden beperkt tot wat absoluut noodzakelijk is in het kader van een specifiek onderzoek.

Wanneer persoonsgegevens worden verzameld zonder dat de betrokkene daarvan op de hoogte is, zou de betrokkene in kennis van de gegevensverzameling moeten worden gesteld zodra deze kennisgeving niet langer een belemmerend effect op onderzoeken heeft. Ook de verzameling van gegevens door technische surveillance of andere geautomatiseerde middelen moet zijn gebaseerd op specifieke wettelijke bepalingen.

Voorbeeld: In *Vetter / Frankrijk*[253] hadden anonieme getuigen de verzoeker beschuldigd van moord. Omdat de verzoeker regelmatig naar het huis van een vriend ging, had de politie daar met toestemming van de onderzoeksrechter afluisterapparatuur geïnstalleerd. Op grond van de bewijskracht van de opgenomen gesprekken werd de verzoeker aangehouden en vervolgd voor moord. Hij verzocht dat de opnamen ontoelaatbaar werden verklaard, voornamelijk op basis van het argument dat deze niet rechtmatig waren verkregen. Voor het EHRM was de belangrijkste rechtsvraag of het gebruik van afluisterapparatuur al dan niet "in overeenstemming met de wet" was geweest. Het plaatsen van afluisterapparatuur in privéruimten viel duidelijk niet binnen het toepassingsgebied van artikel 100 et. seq. van het Franse wetboek van strafvordering, aangezien deze bepalingen betrekking hadden op het aftappen van telefoongesprekken. Artikel 81 van dit wetboek van strafvordering gaf geen redelijke duidelijkheid over de wijze waarop de discretionaire bevoegdheid van de autoriteiten om privégesprekken af te luisteren moest worden uitgeoefend. Bijgevolg had de verzoeker niet het minimumniveau van bescherming genoten waarop burgers recht hebben in een democratische samenleving met een

253 EHRM, *Vetter / Frankrijk*, nr. 59842/00, 31 mei 2005.

rechtsstaat. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

In de aanbeveling wordt geconcludeerd dat bij de opslag van persoonsgegevens duidelijk onderscheid moet worden gemaakt tussen: administratieve gegevens en politiegegevens, verschillende typen betrokkenen, zoals verdachten, veroordeelde personen, slachtoffers en getuigen, en gegevens die als harde feiten worden beschouwd en gegevens die zijn gebaseerd op vermoedens of speculatie.

Politiegegevens moeten strikt aan specifieke doeleinden worden gebonden. Dit heeft gevolgen voor de communicatie van politiegegevens aan derden: de overdracht of mededeling van dergelijke gegevens binnen de politiesector moet worden onderworpen aan de vraag of er al dan niet sprake is van een rechtmatig belang bij het delen van de informatie. De overdracht of communicatie van deze gegevens buiten de politiesector mag alleen worden toegestaan indien er een duidelijke verplichting voor de autoriteiten bestaat. De internationale overdracht of communicatie moet worden beperkt tot politieautoriteiten van derde landen en moet zijn gebaseerd op bijzondere wettelijke bepalingen, mogelijkerwijs internationale overeenkomsten, tenzij de overdracht noodzakelijk is om een ernstig en dreigend gevaar te voorkomen.

Om naleving van de nationale gegevensbeschermingswetgeving te waarborgen, moet gegevensverwerking door de politie zijn onderworpen aan onafhankelijk toezicht. Betrokkenen moeten alle in Verdrag 108 vervatte toegangsrechten kunnen uitoefenen. Wanneer de toegangsrechten van betrokkenen overeenkomstig artikel 9 van Verdrag 108 zijn beperkt in het belang van doeltreffende politieonderzoeken, moet de betrokkene krachtens het nationale recht het recht hebben om beroep in te stellen bij de nationale toezichthouder voor gegevensbescherming of een ander onafhankelijk orgaan.

7.1.2. Het Verdrag van Boedapest inzake cybercriminaliteit

Omdat bij criminele activiteiten in toenemende mate gebruik wordt gemaakt van en deze activiteiten steeds sterker van invloed zijn op elektronische gegevensverwerkingsystemen, zijn nieuwe strafrechtelijke wettelijke bepalingen nodig om deze uitdaging het hoofd te kunnen bieden. Om die reden heeft de RvE een internationaal rechtsinstrument aangenomen, het Verdrag inzake cybercriminaliteit – ook bekend

als het Verdrag van Boedapest – als antwoord op het probleem van tegen en door middel van elektronische netwerken gepleegde strafbare feiten.[254] Dit verdrag staat ook open voor toetreding door niet-lidstaten van de RvE, en medio 2013 waren vier staten buiten de RvE – Australië, de Dominicaanse Republiek, Japan en de Verenigde Staten – partij bij het verdrag en hadden twaalf andere niet-lidstaten het verdrag ondertekend of waren ze uitgenodigd om toe te treden.

Het Verdrag inzake cybercriminaliteit blijft het meest invloedrijke internationale verdrag inzake inbreuken op de wet via internet of andere informatienetwerken. Het verdrag vereist van de verdragsluitende partijen dat ze hun strafrechtelijke bepalingen tegen hacken en andere inbreuken, waaronder inbreuken op het auteursrecht, computergerelateerde fraude, kinderpornografie en andere illegale cyberactiviteiten, actualiseren en harmoniseren. Ook voorziet het verdrag in procedurele bevoegdheden voor het doorzoeken van computernetwerken en het onderscheppen van communicatie in het kader van de bestrijding van cybercriminaliteit. Tot slot maakt het verdrag doeltreffende internationale samenwerking mogelijk. Een aanvullend protocol bij het verdrag heeft betrekking op de strafbaarstelling van racistische en xenofobische propaganda in computernetwerken.

Hoewel het verdrag geen instrument is voor de bevordering van gegevensbescherming, stelt het activiteiten die het recht van een betrokkene op bescherming van zijn of haar persoonsgegevens mogelijk kunnen schenden strafbaar. Ook worden de verdragsluitende partijen verplicht om bij de tenuitvoerlegging van het verdrag te voorzien in een passende bescherming van mensenrechten en vrijheden, waaronder door het EVRM gegarandeerde rechten, zoals het recht op gegevensbescherming.[255]

254 Raad van Europa, Comité van ministers (2001), Verdrag inzake cybercriminaliteit, CETS nr. 185, Boedapest, 23 november 2001, in werking getreden op 1 juli 2004.

255 *Ibid.,* artikel 15, lid 1.

7.2. EU-recht inzake gegevensbescherming in het kader van politiële en justitiële samenwerking in strafzaken

Belangrijkste punten

- Op EU-niveau wordt gegevensbescherming in de politiële en justitiële sector alleen geregeld in het kader van grensoverschrijdende samenwerking tussen politiële en justitiële autoriteiten.
- Er bestaan bijzondere gegevensbeschermingsregelingen voor de Europese Politiedienst (Europol) en de Europese Eenheid voor justitiële samenwerking (Eurojust), beide EU-organen die bijstand verlenen aan grensoverschrijdende wetshandhaving en deze bevorderen.
- Ook bestaan er bijzondere gegevensbeschermingsregelingen voor de gemeenschappelijke informatiesystemen die op EU-niveau zijn ingesteld voor grensoverschrijdende informatie-uitwisseling tussen bevoegde politie- en justitiële autoriteiten. Belangrijke voorbeelden zijn Schengen II, het Visa Informatiesysteem (VIS) en Eurodac, een centraal systeem waarin de dactyloscopische gegevens van onderdanen van derde landen die asiel aanvragen in een van de EU-lidstaten worden bewaard.

De richtlijn gegevensbescherming is niet van toepassing op politiële en justitiële samenwerking in strafzaken. In paragraaf 7.2.1 worden de belangrijkste rechtsinstrumenten op dit gebied beschreven.

7.2.1. Het kaderbesluit gegevensbescherming

Kaderbesluit 2008/977/JBZ van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken (*kaderbesluit gegevensbescherming*)[256] heeft als doel de bescherming van persoonsgegevens van natuurlijke personen te waarborgen wanneer hun persoonsgegevens worden verwerkt met het oog op preventie, onderzoek, opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van een straf. Namens de lidstaten van de EU wordt opgetreden door bevoegde autoriteiten op het gebied van politie en justitie. Deze autoriteiten zijn EU-agentschappen of -organen, evenals

256 Raad van de Europese Unie (2008), Kaderbesluit 2008/977/JBZ van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken (*kaderbesluit gegevensbescherming*), PB L 350 van 30.12.2008, blz. 60.

autoriteiten van de lidstaten.[257] Het toepassingsgebied van het kaderbesluit is beperkt tot het waarborgen van gegevensbescherming in de grensoverschrijdende samenwerking tussen deze autoriteiten en strekt zich niet uit tot nationale veiligheid.

Het kaderbesluit gegevensbescherming is in hoge mate gegrondvest op de in Verdrag 108 en de richtlijn gegevensbescherming vervatte beginselen en definities.

Gegevens mogen alleen worden gebruikt door een bevoegde autoriteit en uitsluitend voor het doel waarvoor ze zijn doorgegeven of ter beschikking zijn gesteld. De ontvangende lidstaat moet alle bij de wet van de versturende lidstaat gestelde beperkingen aan de gegevensuitwisseling eerbiedigen. Het gebruik van gegevens door de ontvangende staat voor een ander doeleinde is onder bepaalde omstandigheden echter toegestaan. Het bijhouden van logboeken en het documenteren van overdrachten is een specifieke taak van de bevoegde autoriteiten met het oog op de verduidelijking van verantwoordelijkheden naar aanleiding van klachten. De verdere overdracht van in het kader van grensoverschrijdende samenwerking ontvangen gegevens aan derden vereist de toestemming van de lidstaten waaruit de gegevens oorspronkelijk afkomstig zijn, hoewel er in urgente gevallen uitzonderingen bestaan.

De bevoegde autoriteiten moeten de noodzakelijke beveiligingsmaatregelen nemen om persoonsgegevens te beschermen tegen onrechtmatige vormen van verwerking.

Elke lidstaat moet ervoor zorgen dat een of meer onafhankelijke toezichthoudende autoriteiten belast worden met het verstrekken van adviezen over en het houden van toezicht op de toepassing van de bepalingen die krachtens het kaderbesluit gegevensbescherming zijn vastgesteld. Ook behandelen ze klachten van personen over de bescherming van hun rechten en vrijheden in het kader van de verwerking van persoonsgegevens door bevoegde autoriteiten.

De betrokkene heeft recht op informatie over de verwerking van zijn of haar persoonsgegevens en op toegang, rectificatie, uitwissing en afscherming. Wanneer de uitoefening van deze rechten wordt geweigerd om dwingende redenen, moet de betrokkene het recht hebben om beroep in te stellen bij de bevoegde nationale toezichthoudende autoriteit en/of een rechtbank. Als een persoon schade ondervindt

257 *Ibid.,* artikel 2, onder h).

door schendingen van het nationale recht ter uitvoering van het kaderbesluit gegevensbescherming, heeft deze persoon recht op schadevergoeding door de voor de verwerking verantwoordelijke.[258] Over het algemeen moeten betrokkenen in geval van schending van rechten die hun door nationale wetgeving ter uitvoering van het kaderbesluit gegevensbescherming worden gegarandeerd, toegang hebben tot een rechtsmiddel.[259]

De Europese Commissie heeft een hervorming voorgesteld die bestaat uit een algemene verordening gegevensbescherming[260] en een richtlijn inzake gegevensverwerking door justitie.[261] De nieuwe richtlijn zal het huidige kaderbesluit gegevensbescherming vervangen en algemene beginselen en regels toepassen op politiële en justitiële samenwerking in strafzaken.

7.2.2. Meer specifieke rechtsinstrumenten op het gebied van gegevensbescherming in het kader van grensoverschrijdende samenwerking tussen politie en wetshandhavingsautoriteiten

Behalve door het kaderbesluit gegevensbescherming wordt de uitwisseling van bij de lidstaten berustende informatie op specifieke gebieden gereguleerd door een aantal rechtsinstrumenten, zoals Kaderbesluit 2009/315/JBZ van de Raad betreffende de organisatie en de inhoud van uitwisseling van gegevens uit het strafregister tussen de lidstaten en het Besluit van de Raad inzake een regeling voor

258 *Ibid.*, artikel 19.

259 *Ibid.*, artikel 20.

260 Europese Commissie (2012), 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), COM(2012) 11 definitief, Brussel, 25 januari 2012.

261 Europese Commissie (2012), 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, COM(2012) 10 definitief, Brussel, 25 januari 2012.

samenwerking tussen de financiële inlichtingeneenheden van de lidstaten bij de uitwisseling van gegevens.[262]

Belangrijk is dat bij grensoverschrijdende samenwerking[263] tussen bevoegde autoriteiten steeds vaker immigratiegegevens worden uitgewisseld. Dit rechtsdomein valt niet onder de politiële en justitiële samenwerking in strafzaken, maar is in veel opzichten relevant voor het werk van politiële en justitiële autoriteiten. Hetzelfde geldt voor gegevens over goederen die in de EU worden in- of uitgevoerd. De afschaffing van de interne grenscontroles binnen de EU heeft het risico op fraude verhoogd, waardoor het noodzakelijk is dat de lidstaten hun samenwerking intensiveren, met name door de grensoverschrijdende informatie-uitwisseling te versterken, om schendingen van de nationale en EU-douanewetgeving beter te kunnen opsporen en vervolgen.

Het Prüm-besluit

Een belangrijk voorbeeld van geïnstitutionaliseerde grensoverschrijdende samenwerking door de uitwisseling van nationaal bewaarde gegevens is Besluit 2008/615/JBZ van de Raad inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit (*Prüm-besluit*), waarbij het Prüm-Verdrag in 2008 in het EU-recht is geïntegreerd.[264] Het Prüm-Verdrag was een overeenkomst inzake internationale politiesamenwerking die in 2005 was ondertekend door België, Duitsland, Frankrijk, Luxemburg, Nederland, Oostenrijk en Spanje.[265]

---

262 Raad van de Europese Unie (2009), Kaderbesluit 2009/315/JBZ van de Raad van 26 februari 2009 betreffende de organisatie en de inhoud van uitwisseling van gegevens uit het strafregister tussen de lidstaten, PB L 93 van 7.4.2009, blz. 23; Raad van de Europese Unie (2000), Besluit 2000/642/JBZ van de Raad van 17 oktober 2000 inzake een regeling voor samenwerking tussen de financiële inlichtingeneenheden van de lidstaten bij de uitwisseling van gegevens, PB L 271 van 24.10.2000, blz. 4.

263 Europese Commissie (2012), Mededeling van de Commissie aan het Europees Parlement en de Raad – Samenwerking op het gebied van rechtshandhaving in de EU versterken: het Europees model voor informatie-uitwisseling (EIXM), COM(2012) 735 definitief, Brussel, 7 december 2012.

264 Raad van de Europese Unie (2008), Besluit 2008/615/JBZ van de Raad van 23 juni 2008 inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit, PB L 210 van 6.8.2008, blz. 1.

265 Verdrag tussen het Koninkrijk België, de Bondsrepubliek Duitsland, het Koninkrijk Spanje, de Republiek Frankrijk, het Groothertogdom Luxemburg, het Koninkrijk der Nederlanden en de Republiek Oostenrijk inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie, beschikbaar op: http://register.consilium.europa.eu/pdf/nl/05/st10/st10900.nl05.pdf.

Het doel van het Prüm-besluit is om de lidstaten te helpen bij het verbeteren van de informatie-uitwisseling met het oog op de preventie en bestrijding van criminaliteit op drie gebieden: terrorisme, grensoverschrijdende criminaliteit en illegale migratie. Hiertoe bevat het besluit bepalingen inzake:

- geautomatiseerde bevraging van DNA-profielen, dactyloscopische gegevens en bepaalde gegevens uit nationale kentekenregisters;
- de verstrekking van gegevens in samenhang met grootschalige evenementen met een grensoverschrijdende dimensie;
- de verstrekking van gegevens ter voorkoming van terroristische strafbare feiten;
- andere maatregelen om de grensoverschrijdende politiesamenwerking te intensiveren.

De databanken die beschikbaar worden gesteld krachtens het Prüm-besluit vallen volledig onder het nationale recht, maar de uitwisseling van gegevens valt ook onder het besluit en, meer recentelijk, onder het kaderbesluit gegevensbescherming. De bevoegde organen voor het houden van toezicht op dit gegevensverkeer zijn de nationale toezichthoudende autoriteiten voor gegevensbescherming.

7.2.3. Gegevensbescherming bij Europol en Eurojust

Europol

Europol, het rechtshandhavingsagentschap van de EU, heeft zijn hoofdkantoor in Den Haag, terwijl in elke lidstaat nationale Europol-eenheden (NEE's) zijn ingesteld. Europol is opgericht in 1998; zijn huidige wettelijke status als EU-instelling is gebaseerd op het besluit van de Raad tot oprichting van de Europese politiedienst (*Europol-besluit*).[266] Het doel van Europol is om ondersteuning te verlenen bij het voorkomen en onderzoeken van georganiseerde criminaliteit, terrorisme en andere vormen van ernstige criminaliteit als vermeld in de bijlage bij het Europol-besluit waarbij twee of meer EU-lidstaten betrokken zijn.

266 Raad van de Europese Unie (2009), Besluit van de Raad van 6 april 2009 tot oprichting van de Europese politiedienst, PB L 121 van 15.5.2009, blz. 37 (Europol). Zie ook het voorstel van de Commissie voor een verordening voor een nieuw wettelijk kader voor een nieuwe Europol die de opvolger en vervanger is van Europol als opgericht bij Besluit 2009/371/JBZ van de Raad van 6 april 2009 tot oprichting van de Europese politiedienst (Europol) en CEPOL als opgericht bij Besluit 2005/681/JBZ van de Raad tot oprichting van de Europese Politieacademie (CEPOL), COM(2013) 173 definitief.

Om deze doelen te verwezenlijken heeft Europol het Europol-informatiesysteem opgezet, dat een databank omvat waarin de lidstaten inlichtingen en informatie over criminele activiteiten kunnen uitwisselen via hun NEE's. Het Europol-informatiesysteem kan worden gebruikt om gegevens beschikbaar te stellen die verband houden met personen die worden verdacht van of zijn veroordeeld voor een strafbaar feit dat onder de bevoegdheid van Europol valt of met personen ten aanzien van wie er feitelijke aanwijzingen zijn dat zij dergelijke strafbare feiten zullen plegen. Europol en de NEE's kunnen gegevens rechtstreeks invoeren in het Europol-informatiesysteem en gegevens uit het systeem opvragen. Alleen de partij die de gegevens in het systeem heeft ingevoerd, mag deze wijzigen, corrigeren of verwijderen.

Voor zover dat noodzakelijk is voor de vervulling van zijn taken, kan Europol gegevens over strafbare feiten in analysebestanden opslaan, wijzigen en gebruiken. Analysebestanden worden geopend met het oog op de verzameling, de verwerking of het gebruik van gegevens ten behoeve van de ondersteuning van concrete onderzoeken naar strafbare feiten die door Europol in samenwerking met de EU-lidstaten worden verricht.

In reactie op nieuwe ontwikkelingen is op 1 januari 2013 het Europees Centrum voor de bestrijding van cybercriminaliteit opgericht.[267] Dit centrum fungeert als het EU-knooppunt voor informatie over cybercriminaliteit en draagt bij tot snellere reacties in geval van via het internet gepleegde strafbare feiten, de ontwikkeling en inzet van forensische capaciteit en de ontwikkeling van beste praktijken in onderzoeken naar cybercriminaliteit. Het centrum concentreert zich op computerdelicten die:

- worden gepleegd door georganiseerde groepen en die zeer winstgevend zijn, zoals internetfraude;
- de slachtoffers ernstige schade berokkenen, zoals seksuele uitbuiting van kinderen via het internet;
- de kritieke infrastructuur- en informatiesystemen in de Unie schaden.

De gegevensbeschermingsregels die van toepassing zijn op de activiteiten van Europol worden versterkt. Artikel 27 van het Europol-besluit bepaalt dat de beginselen

267 Zie ook de EDPS (2012), *Advies van de Europese toezichthouder voor gegevensbescherming (EDPS) over de mededeling van de Europese Commissie aan de Raad en het Europees Parlement over de oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit*, Brussel, 29 juni 2012.

van Verdrag 108 en de Aanbeveling inzake politiegegevens van toepassing zijn op de geautomatiseerde en niet-geautomatiseerde verwerking van gegevens. De overdracht van gegevens tussen Europol en de lidstaten moet daarnaast ook voldoen aan de regels van het kaderbesluit gegevensverwerking.

Om de naleving van de toepasselijke gegevensbeschermingswetgeving te waarborgen, en in het bijzonder om ervoor te zorgen dat de rechten van de betrokkene niet worden geschonden door de verwerking van de gegevens, houdt het onafhankelijke Gemeenschappelijk Controleorgaan (GCO) toezicht op de werkzaamheden van Europol.[268] Eenieder heeft recht op toegang tot de persoonsgegevens die Europol mogelijk over hem of haar heeft opgeslagen, naast het recht om te verzoeken dat deze gegevens worden gecontroleerd, gecorrigeerd of verwijderd. Als iemand niet tevreden is met het besluit van Europol ten aanzien van de uitoefening van zijn of haar rechten, kan deze persoon beroep instellen bij het comité van beroep van het GCO.

Als schade is ontstaan als gevolg van door Europol onrechtmatig of feitelijk onjuist opgeslagen of verwerkte gegevens, kan de benadeelde partij alleen een vordering indienen bij de bevoegde rechtbank van de lidstaat waar het schadebrengende feit zich heeft voorgedaan.[269] Europol zal de lidstaat de schade vergoeden als de schade het resultaat is van het niet naleven door Europol van zijn wettelijke verplichtingen.

Eurojust

Eurojust, dat is opgericht in 2002, is een EU-orgaan dat is gevestigd in Den Haag en dat de samenwerking tussen justitiële autoriteiten bevordert in onderzoeken en vervolgingen van ernstige criminaliteit waarbij ten minste twee lidstaten zijn betrokken.[270] Eurojust is bevoegd om:

268 Europol-besluit, artikel 34.

269 *Ibid.*, artikel 52.

270 Raad van de Europese Unie (2002), Besluit 2002/187/JBZ van 28 februari 2002 betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken, PB L 63 van 6.3.2002, blz.1; Raad van de Europese Unie (2003), Besluit 2003/659/JBZ van de Raad van 18 juni 2003 tot wijziging van Besluit 2002/187/JBZ betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken, PB L 245 van 29.9.2003, blz. 44; Raad van de Europese Unie (2009), Besluit 2009/426/JBZ van de Raad van 16 december 2008 inzake het versterken van Eurojust en tot wijziging van Besluit 2002/187/JBZ betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken, PB L 138 van 4.6.2009, blz. 14 (*Eurojust-besluiten*).

- de coördinatie van onderzoeken en vervolgingen tussen de bevoegde autoriteiten van de verschillende lidstaten te bevorderen en te verbeteren;

- de uitvoering van verzoeken en besluiten in verband met justitiële samenwerking te vergemakkelijken.

De functies van Eurojust worden uitgevoerd door de nationale leden. Elke lidstaat detacheert één rechter of openbare aanklager bij Eurojust, die is onderworpen aan het nationale recht en over de nodige bevoegdheden beschikt om de taken uit te voeren die noodzakelijk zijn om de justitiële samenwerking te bevorderen en te verbeteren. Daarnaast treden de nationale leden gezamenlijk op, als een college, bij de uitvoering van bijzondere taken van Eurojust.

Eurojust kan persoonsgegevens verwerken voor zover dat noodzakelijk is om zijn doelstellingen te verwezenlijken. Dit is echter beperkt tot specifieke informatie over personen die verdacht worden van het plegen van of deelnemen aan het plegen van, of die veroordeeld zijn voor, een strafbaar feit dat onder de bevoegdheid van Eurojust valt. Eurojust kan ook bepaalde informatie verwerken met betrekking tot getuigen of slachtoffers van strafbare feiten die onder de bevoegdheid van Eurojust vallen.[271] In uitzonderlijke omstandigheden kan Eurojust echter ook, gedurende een beperkte periode, andere persoonsgegevens betreffende de omstandigheden van een strafbaar feit verwerken wanneer die van onmiddellijk belang zijn voor en deel uitmaken van lopende onderzoeken. Binnen zijn bevoegdheidsgebied kan Eurojust samenwerken en persoonsgegevens uitwisselen met andere EU-instellingen, -organen en -agentschappen. Ook kan Eurojust samenwerken en persoonsgegevens uitwisselen met derde landen en organisaties.

Wat betreft gegevensbescherming moet Eurojust een beschermingsniveau waarborgen dat ten minste gelijk is aan het niveau dat resulteert uit de toepassing van de beginselen van Verdrag 108 en de latere wijzigingen daarvan. In geval van gegevensuitwisseling moeten specifieke regels en beperkingen in acht worden genomen die zijn neergelegd in samenwerkingsovereenkomsten of werkregelingen in overeenstemming met de Eurojust-besluiten van de Raad en de gegevensbeschermingsvoorschriften voor Eurojust.[272]

271 Geconsolideerde versie van Besluit 2002/187/JBZ van de Raad als gewijzigd bij Besluit 2003/659/JBZ van de Raad en bij Besluit 2009/426/JBZ van de Raad, artikel 15, lid 2.

272 Interne reglement betreffende de verwerking en bescherming van persoonsgegevens bij Eurojust, PB C 68 van 19.3.2005, blz. 1.

Binnen Eurojust is een onafhankelijk Gemeenschappelijk Controleorgaan (GCO) ingesteld, dat als taak heeft om toezicht te houden op de verwerking van persoonsgegevens door Eurojust. Betrokkenen kunnen bij het GCO beroep instellen als ze niet tevreden zijn met het antwoord van Eurojust op een verzoek om toegang tot of correctie, afscherming of uitwissing van persoonsgegevens. Wanneer Eurojust onrechtmatig persoonsgegevens verwerkt, is Eurojust aansprakelijk overeenkomstig het nationale recht van de lidstaat waar zijn hoofdkantoor is gevestigd, Nederland, voor schade die aan de betrokkene is veroorzaakt.

7.2.4. Gegevensbescherming in de gemeenschappelijke informatiesystemen op EU-niveau

Naast de gegevensuitwisseling tussen lidstaten en de oprichting van gespecialiseerde EU-autoriteiten voor de bestrijding van grensoverschrijdende criminaliteit, zijn op EU-niveau diverse gemeenschappelijke informatiesystemen opgezet die fungeren als platform voor de uitwisseling van gegevens tussen de bevoegde nationale en EU-autoriteiten voor gespecificeerde rechtshandhavingsdoeleinden, met inbegrip van de immigratie- en douanewetgevingsdoeleinden. Enkele van deze systemen zijn ontwikkeld op basis van multilaterale overeenkomsten die vervolgens zijn aangevuld met EU-rechtsinstrumenten en -systemen, zoals het Schengeninformatiesysteem, het Visuminformatiesysteem, Eurodac, Eurosur en het Douane-informatiesysteem.

Het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (eu-LISA),[273] dat in 2012 is opgericht, is belast met het langetermijnbeheer van het Schengeninformatiesysteem van de tweede generatie (SIS II), het Visuminformatiesysteem (VIS) en Eurodac. De kerntaak van het eu-LISA is om te zorgen voor de effectieve, veilige en continue werking van grootschalige IT-systemen. Ook is het agentschap verantwoordelijk voor het nemen van de noodzakelijke maatregelen om de beveiliging van de systemen en van de gegevens te waarborgen.

273 Verordening (EU) nr. 1077/2011 van het Europees Parlement en de Raad van 25 oktober 2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht, PB L 286 van 1.11.2011, blz. 1.

Het Schengeninformatiesysteem

In 1985 hebben verschillende lidstaten van de voormalige Europese Gemeenschappen een overeenkomst gesloten tussen de staten van de Benelux Economische Unie, Duitsland en Frankrijk betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen (*Schengenovereenkomst*), die als doel had om een ruimte te creëren voor het vrije verkeer van personen, ongehinderd door grenscontroles, binnen de Schengenruimte.[274] Om de mogelijk uit de open grenzen voortvloeiende dreiging voor de openbare veiligheid tegen te gaan, zijn versterkte controles aan de buitengrenzen van de Schengenruimte ingesteld, evenals nauwe samenwerking tussen nationale politiële en justitiële autoriteiten.

Als gevolg van de toetreding van nieuwe staten tot de Schengenovereenkomst is het Schengensysteem uiteindelijk bij het Verdrag van Amsterdam geïntegreerd in het wettelijk kader van de EU.[275] De tenuitvoerlegging van dit besluit vond plaats in 1999. De nieuwste versie van het Schengeninformatiesysteem, het zogeheten SIS II, trad in werking op 9 april 2013. Het systeem wordt nu gebruikt door alle EU-lidstaten plus IJsland, Liechtenstein, Noorwegen en Zwitserland.[276] Ook Europol en Eurojust hebben toegang tot het SIS II.

Het SIS II bestaat uit een centraal systeem (C.SIS), een nationaal systeem (N.SIS) in elke lidstaat en een communicatie-infrastructuur tussen het centrale system en de nationale systemen. Het C.SIS bevat bepaalde door de lidstaten ingevoerde gegevens over personen en voorwerpen. Het C.SIS wordt gebruikt door nationale grenscontrole-, politie-, douane- en gerechtelijke autoriteiten in de hele Schengenruimte. Elke lidstaat beheert een nationale kopie van het C.SIS, die tezamen bekend zijn als de nationale Schengeninformatiesystemen (N.SIS) en voortdurend worden bijgewerkt, waarmee ook het C.SIS wordt bijgewerkt. De N.SIS worden geraadpleegd en zullen een waarschuwing afgeven indien:

274 Overeenkomst ter uitvoering van het tussen de regeringen van de staten van de Benelux Economische Unie, de Bondsrepubliek Duitsland en de Franse Republiek op 14 juni 1985 te Schengen gesloten akkoord betreffende de geleidelijke afschaffing van de controles aan de gemeenschappelijke grenzen, PB L 239 van 22.9.2000, blz. 19.

275 Europese Gemeenschappen (1997), Verdrag van Amsterdam houdende wijziging van het Verdrag betreffende de Europese Unie, de Verdragen tot oprichting van de Europese Gemeenschappen en sommige bijbehorende akten, PB C 340 van 10.11.1997, blz. 1.

276 Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (*SIS II*), PB L 381 van 28.12.2006, blz. 4 en Raad van de Europese Unie (2007), Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (*SISII*), PB L 205 van 7.7.2007, blz. 63.

- de persoon geen recht heeft om de Schengenruimte binnen te komen of erin te verblijven; of
- de persoon of het voorwerp wordt gezocht door gerechtelijke of rechtshandhavingsautoriteiten; of
- de persoon als vermist is opgegeven; of
- goederen, zoals bankbiljetten, auto's, bestelwagens, vuurwapens en identiteitsdocumenten, zijn opgegeven als gestolen of verloren.

In geval van een waarschuwing worden follow-upactiviteiten geïnitieerd via de nationale Schengeninformatiesystemen.

Het SIS II heeft nieuwe functionaliteiten, zoals de mogelijkheid om biometrische gegevens, zoals vingerafdrukken en foto's, nieuwe categorieën waarschuwingen, bijvoorbeeld over gestolen boten, vliegtuigen, containers of betaalmiddelen, nadere waarschuwingen over personen en voorwerpen, en kopieën van Europese aanhoudingsbevelen met betrekking tot personen die worden gezocht voor aanhouding, uitlevering of overlevering, in te voeren.

Besluit 2007/533/JBZ van de Raad betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (Schengen II-besluit) integreert Verdrag 108: "In toepassing van dit besluit verwerkte persoonsgegevens worden beschermd overeenkomstig (...) Verdrag [108] van de Raad van Europa".[277] Wanneer het gebruik van persoonsgegevens door nationale politieautoriteiten geschiedt overeenkomstig het Schengen II-besluit, moeten de bepalingen van Verdrag 108, evenals die van de Aanbeveling inzake politiegegevens, ten uitvoer worden gelegd in het nationale recht.

De bevoegde nationale toezichthoudende autoriteit in elke lidstaat houdt toezicht op het eigen N.SIS. Met name moet deze autoriteit de kwaliteit van de door de lidstaten via het N.SIS in het C.SIS ingevoerde gegevens controleren. De nationale toezichthoudende autoriteit moet ervoor zorgen dat ten minste elke vier jaar een audit van de gegevensverwerkingen binnen de eigen N.SIS wordt verricht. De nationale toezichthoudende autoriteiten en de EDPS werken samen en zorgen voor

277 Raad van de Europese Unie (2007), Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (*SIS II*), PB L 205 van 7.7.2007, blz. 63, artikel 57.

gecoördineerd toezicht op het SIS, terwijl de EDPS verantwoordelijk is voor het toezicht op het C.SIS. Met het oog op de transparantie wordt om de twee jaar een gezamenlijk activiteitenverslag toegezonden aan het Europees Parlement, de Raad en het eu-LISA.

De toegangsrechten van personen in verband met het SIS II kunnen worden uitgeoefend in elke lidstaat, omdat elke N.SIS een exacte kopie van het C.SIS is.

Voorbeeld: In *Dalea / Frankrijk*[278] had de verzoeker geen visum voor Frankrijk gekregen omdat de Franse autoriteiten aan het Schengeninformatiesysteem hadden gemeld dat hem de toegang tot het land moest worden geweigerd. De verzoeker had zonder succes bij de Franse commissie gegevensbescherming, en uiteindelijk bij de Franse raad van state, verzocht om toegang tot en rectificatie of uitwissing van de gegevens. Het EHRM oordeelde dat de aanmelding van de verzoeker bij het Schengeninformatiesysteem in overeenstemming met de wet was geweest en het rechtmatige doel had gediend om de nationale veiligheid te beschermen. Aangezien de verzoeker niet had aangetoond hoe hij feitelijk was benadeeld door de weigering van toegang tot de Schengenruimte, was de inmenging in het recht op eerbiediging van het privéleven evenredig geweest. De klacht van de verzoeker op grond van artikel 8 werd daarom niet-ontvankelijk verklaard.

Het Visuminformatiesysteem

Het Visuminformatiesysteem (VIS), dat eveneens wordt beheerd door het eu-LISA, is ontwikkeld om de uitvoering van een gemeenschappelijk EU-visumbeleid te ondersteunen.[279] Het VIS stelt de Schengenlanden in staat om gegevens over visa uit te wisselen via een systeem dat de in niet-EU-lidstaten gevestigde consulaten van de Schengenlanden verbindt met de externe grensdoorlaatposten van alle Schengenlanden. Het VIS verwerkt gegevens over aanvragen voor visa voor kort

278 EHRM, *Dalea / Frankrijk,* nr. 964/07, 2 februari 2010.

279 Raad van de Europese Unie (2004), Beschikking van de Raad van 8 juni 2004 betreffende het opzetten van het Visuminformatiesysteem (VIS), PB L 213 van 15.6.2004, blz. 5; Verordening (EG) nr. 767/2008 van het Europees Parlement en de Raad van 9 juli 2008 betreffende het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf, PB L 218 van 13.8.2008, blz. 60 (*VIS-verordening*); Raad van de Europese Unie (2008), Besluit 2008/633/JBZ van de Raad van 23 juni 2008 over de toegang tot het Visuminformatiesysteem (VIS) voor raadpleging door aangewezen autoriteiten van de lidstaten en door Europol, met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten, PB L 218 van 13.8.2008, blz. 129.

verblijf met het oog op verblijf in of doorreis door de Schengenruimte. Het VIS biedt grensautoriteiten de mogelijkheid om met behulp van biometrische gegevens te controleren of de persoon die een visum toont al dan niet de rechtmatige houder is en om personen zonder of met frauduleuze documenten te identificeren.

Volgens Verordening (EG) nr. 767/2008 van het Europees Parlement en de Raad betreffende het opzetten van het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf (*VIS-verordening*), mogen alleen gegevens over de aanvrager, zijn of haar visum, foto's, vingerafdrukken, koppelingen met eerdere aanvragen en aanvraagdossiers van personen die hem of haar begeleiden in het VIS worden geregistreerd.[280] De toegang tot het VIS om gegevens in te voeren, te wijzigen of uit te wissen is beperkt tot uitsluitend de visumautoriteiten van de lidstaten, terwijl de toegang voor de raadpleging van gegevens is voorbehouden aan visumautoriteiten en autoriteiten die bevoegd zijn voor controles aan de externe grensdoorlaatposten, immigratiecontroles en asielzaken. Onder bepaalde omstandigheden kunnen nationale bevoegde politieautoriteiten en Europol verzoeken om toegang tot in het VIS ingevoerde gegevens met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten.[281]

Eurodac

De naam Eurodac is afgeleid van het woord dactylogram, ofwel vingerafdruk. Eurodac is een centraal systeem waarin de vingerafdrukken van onderdanen van derde landen die in een van de EU-lidstaten asiel aanvragen worden opgeslagen.[282] Het systeem is in werking sinds januari 2003 en het doel ervan is om te helpen bij het bepalen van de lidstaat die krachtens Verordening (EG) nr. 343/2003 van de Raad

280 Artikel 5 van Verordening (EG) nr. 767/2008 van het Europees Parlement en de Raad van 9 juli 2008 betreffende het opzetten van het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf (*VIS-verordening*), PB L 218 van 13.8.2008, blz. 60.

281 Raad van de Europese Unie (2008), Besluit 2008/633/JBZ van de Raad van 23 juni 2008 over de toegang tot het Visuminformatiesysteem (VIS) voor raadpleging door aangewezen autoriteiten van de lidstaten en door Europol, met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten, PB L 218 van 13.8.2008, blz. 129.

282 Verordening (EG) nr. 2725/2000 van de Raad van 11 december 2000 betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van de Overeenkomst van Dublin, PB L 316 van 15.12.2000, blz. 1; Verordening (EG) nr. 407/2002 van de Raad van 28 februari 2002 tot vaststelling van sommige uitvoeringsbepalingen voor Verordening (EG) nr. 2725/2000 betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van de Overeenkomst van Dublin, PB L 62 van 5.3.2002, blz. 1 (*Eurodac-verordeningen*).

tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een asielverzoek dat door een onderdaan van een derde land bij een van de lidstaten wordt ingediend (*Dublin II-verordening*) verantwoordelijk is voor het onderzoeken van een specifieke asielaanvraag.[283] Persoonsgegevens in Eurodac mogen alleen worden gebruikt om de toepassing van de Dublin II-verordening te faciliteren; aan elk ander gebruik zijn sancties verbonden.

Eurodac bestaat uit een centrale eenheid voor het opslaan en vergelijken van vingerafdrukken, die wordt beheerd door het eu-LISA, en een systeem voor elektronische doorzending van gegevens tussen de lidstaten en de centrale databank. De lidstaten nemen vingerafdrukken af van iedere onderdaan van een niet-EU-lidstaat of staatloze persoon van veertien jaar of ouder die asiel aanvraagt op hun grondgebied of die is aangehouden wegens het illegaal overschrijden van hun buitengrens en zenden deze door. Ook kunnen de lidstaten vingerafdrukken afnemen en doorzenden van onderdanen van niet-EU-lidstaten of staatloze personen die zonder verblijfsvergunning op hun grondgebied verblijven.

De dactyloscopische gegevens worden alleen in gepseudonimiseerde vorm opgeslagen in de databank van Eurodac. Bij een match wordt het pseudoniem, samen met de naam van de eerste lidstaat die de dactyloscopische gegevens heeft doorgezonden, meegedeeld aan de tweede lidstaat. Deze tweede lidstaat zal vervolgens de eerste lidstaat benaderen, aangezien volgens de Dublin II-verordening de eerste lidstaat verantwoordelijk is voor de verwerking van de asielaanvraag.

In Eurodac opgeslagen persoonsgegevens die verband houden met asielaanvragen worden bewaard gedurende tien jaar vanaf de datum waarop de vingerafdrukken zijn afgenomen, tenzij de betrokkene het burgerschap van een EU-lidstaat verwerft. In dat geval moeten de gegevens onmiddellijk worden uitgewist. Gegevens over onderdanen van derde landen die illegaal de buitengrens zijn overschreden, worden gedurende twee jaar opgeslagen. Deze gegevens moeten onmiddellijk worden uitgewist als de betrokkene een verblijfsvergunning verkrijgt, het grondgebied van de EU verlaat of het burgerschap van een EU-lidstaat verwerft.

Behalve alle EU-lidstaten passen ook IJsland, Noorwegen, Liechtenstein en Zwitserland Eurodac toe op basis van internationale overeenkomsten.

283 Verordening (EG) nr. 343/2003 van de Raad van 18 februari 2003 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een asielverzoek dat door een onderdaan van een derde land bij een van de lidstaten wordt ingediend (*Dublin II-verordening*), PB L 50 van 25.3.2003, blz. 1.

Eurosur

Het Europees grensbewakingssysteem (*Eurosur*)[284] is ontworpen om de controle van de buitengrenzen van de Schengenruimte te versterken door de opsporing, voorkoming en bestrijding van illegale immigratie en grensoverschrijdende criminaliteit. Eurosur is opgezet om de informatie-uitwisseling en operationele samenwerking tussen nationale coördinatiecentra en Frontex, het EU-agentschap dat is belast met de ontwikkeling en toepassing van het nieuwe concept van geïntegreerd grensbeheer, te verbeteren.[285] De algemene doelstellingen zijn de volgende:

- het verminderen van het aantal illegale immigranten dat onopgemerkt de EU binnenkomt;
- het verminderen van het aantal sterfgevallen onder illegale migranten door meer levens op zee te redden;
- het verbeteren van de interne veiligheid van de EU als geheel door bij te dragen tot de preventie van grensoverschrijdende criminaliteit.[286]

De werkzaamheden van Eurosur zijn op 2 december 2013 van start gegaan in alle lidstaten met buitengrenzen, en op 1 december 2014 zal een aanvang worden gemaakt met de werkzaamheden in alle andere lidstaten. De verordening zal van toepassing zijn op controles aan de land-, zee- en luchtbuitengrenzen van de EU.

284 Verordening (EG) nr. 1052/2013 van het Europees Parlement en de Raad van 22 oktober 2013 tot instelling van het Europees grensbewakingssysteem (Eurosur), PB L 295 van 22.10.2013, blz. 1.

285 Verordening (EU) nr. 1168/2011 van het Europees Parlement en de Raad van 25 oktober 2011 tot wijziging van Verordening (EG) nr. 2007/2004 van de Raad tot oprichting van een Europees agentschap voor het begeer van de operationele samenwerking aan de buitengrenzen van de lidstaten van de Europese Unie, PB L 304 van 22.11.2011, blz. 1 (*Frontex-verordening*).

286 Zie ook: Europese Commissie (2008), Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's: Onderzoek naar de mogelijkheden tot instelling van een Europees grensbewakingssysteem (Eurosur), COM(2008) 68 definitief, Brussel, 13 februari 2008; Europese Commissie (2011), Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur), werkdocument van de diensten van de Commissie, SEC(2011) 1536 definitief, Brussel,12 december 2011, blz. 18.

Douane-informatiesysteem

Een ander belangrijk gemeenschappelijk informatiesysteem dat op EU-niveau is opgezet is het Douane-informatiesysteem (DIS).[287] Tijdens de totstandbrenging van de interne markt zijn alle controles en formaliteiten met betrekking tot het goederenverkeer op het grondgebied van de EU afgeschaft, wat tot een verhoogd risico op fraude heeft geleid. Dit risico is tegengegaan door een versterkte samenwerking tussen de douanediensten van de lidstaten. Het doel van het DIS is om de lidstaten bij te staan bij het voorkomen, onderzoeken en vervolgen van ernstige inbreuken op douane- en landbouwwetgeving van de lidstaten en van de EU.

De informatie in het DIS omvat persoonsgegevens met betrekking tot goederen, vervoersmiddelen, bedrijven, personen en ingehouden, in beslag genomen of geconfisqueerde goederen en contanten. Deze informatie mag uitsluitend worden gebruikt voor de melding van waarnemingen of voor het verrichten van gerichte controles en strategische of operationele analyses met betrekking tot personen die worden verdacht van het overtreden van de douanevoorschriften.

Toegang tot het DIS wordt alleen verleend aan de nationale douane-, belasting-, landbouw-, volksgezondheids- en politieautoriteiten, evenals aan Europol en Eurojust.

De verwerking van persoonsgegevens moet voldoen aan de specifieke voorschriften van Verordening (EG) nr. 515/97 en de DIS-overeenkomst,[288] evenals aan de bepalingen van de richtlijn gegevensbescherming, de verordening gegevensbescherming EU-instellingen, Verdrag 108 en de Aanbeveling inzake politiegegevens. De EDPS is verantwoordelijk voor het toezicht op het DIS en de naleving van Verordening (EG) nr. 45/2001, en belegt ten minste eenmaal per jaar een vergadering met alle nationale gegevensbeschermingsautoriteiten belast met DIS-gerelateerde toezichtstaken.

287 Raad van de Europese Unie (1995), Akte van de Raad van 26 juli 1995 tot vaststelling van de Overeenkomst inzake het gebruik van informatica op douanegebied, PB C 316 van 27.11.1995, blz. 33, gewijzigd bij Raad van de Europese Unie (2009), Verordening (EG) nr. 515/97 van de Raad van 13 maart 1997 betreffende de wederzijdse bijstand tussen de administratieve autoriteiten van de lidstaten en de samenwerking tussen deze autoriteiten en de Commissie met het oog op de juiste toepassing van de douane- en landbouwvoorschriften, PB L 82 van 22.03.1997, blz. 1, Besluit 2009/917/JBZ van de Raad van 30 november 2009 inzake het gebruik van informatica op douanegebied, PB L 323 van 10.12.2009, blz. 20 (*DIS-besluit*).

288 *Ibid.*

8

Andere specifieke Europese gegevensbeschermingswetgeving

EU	Behandelde onderwerpen	RvE
Richtlijn gegevensbescherming E-privacyrichtlijn	Elektronische communicatie	Verdrag 108 Aanbeveling inzake telecommunicatiediensten
Richtlijn gegevensbescherming, artikel 8, lid 2, onder b)	Arbeidsverhoudingen	Verdrag 108 Aanbeveling inzake arbeidsgegevens
		EHRM, *Copland / Verenigd Koninkrijk*, nr. 62617/00, 3 april 2007
Richtlijn gegevensbescherming, artikel 8, lid 3	Medische gegevens	Verdrag 108 Aanbeveling inzake medische gegevens
		EHRM, *Z. / Finland*, nr. 22009/93, 25 februari 1997
Richtlijn inzake klinische proeven	Klinische proeven	
Richtlijn gegevensbescherming, artikel 6, lid 1, onder b), en artikel 13, lid 2	Statistieken	Verdrag 108 Aanbeveling inzake statistische gegevens
Verordening (EG) nr. 223/2009 betreffende de Europese statistiek HvJ-EU, zaak C-524/06, *Huber / Bondsrepubliek Duitsland*, 16 december 2008	Officiële statistieken	Verdrag 108 Aanbeveling inzake statistische gegevens

EU	Behandelde onderwerpen	RvE
Richtlijn 2004/39/EG betreffende markten voor financiële instrumenten Verordening (EU) nr. 648/2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters Verordening (EG) nr. 1060/2009 inzake ratingbureaus Richtlijn 2007/64/EG betreffende betalingdiensten in de interne markt	Financiële gegevens	Verdrag 108 Aanbeveling 90(19) inzake de bescherming van persoonsgegevens die worden gebruikt voor betalingen en andere, aanverwante verrichtingen EHRM, *Michaud / Frankrijk*, nr. 12323/11, 6 december 2012

Op Europees niveau zijn diverse bijzondere rechtsinstrumenten vastgesteld die de algemene beginselen van Verdrag 108 en de richtlijn gegevensbescherming meer in detail toepassen op specifieke situaties.

8.1. Elektronische communicatie

Belangrijkste punten

- Specifieke voorschriften voor de gegevensbescherming op het gebied van telecommunicatie, en in het bijzonder telefoniediensten, zijn opgenomen in de aanbeveling van de RvE van 1995.
- De verwerking van persoonsgegevens in verband met de verrichting van telecommunicatiediensten op EU-niveau wordt gereguleerd in de e-privacyrichtlijn.
- De vertrouwelijkheid van elektronische communicaties geldt niet alleen voor de inhoud van een communicatie, maar ook voor het gegevensverkeer, zoals informatie over wie met wie heeft gecommuniceerd, en wanneer en hoe lang, met inbegrip van locatiegegevens, zoals waar de gegevens zijn gecommuniceerd.

Communicatienetwerken hebben een verhoogd potentieel voor ongerechtvaardigde inmenging in de persoonlijke levenssfeer van de gebruikers, omdat ze extra technische mogelijkheden bieden om de communicatie die in deze netwerken plaatsvindt af te luisteren en te bewaken. Dientengevolge werden bijzondere gegevensbeschermingsregels noodzakelijk geacht om de specifieke risico's voor gebruikers van communicatiediensten aan banden te leggen.

In 1995 heeft de RvE een aanbeveling uitgebracht inzake gegevensbescherming op het gebied van telecommunicatie, met bijzondere nadruk op telefoondiensten.[289] Volgens deze aanbeveling moeten de doeleinden van het verzamelen en verwerken van persoonsgegevens in het kader van telecommunicatie worden beperkt tot het verbinden van een gebruiker met het netwerk, het beschikbaar stellen van de specifieke telecommunicatiedienst, facturering, controle, zorgen voor een optimale technische exploitatie en ontwikkelen van het netwerk en de dienst.

Ook wordt bijzondere aandacht geschonken aan het gebruik van communicatienetwerken voor het verzenden van boodschappen in het kader van direct marketing. Als algemene regel mogen direct-marketingberichten niet worden gezonden aan abonnees die uitdrukkelijk te kennen hebben gegeven dat ze geen reclameboodschappen wensen te ontvangen. Geautomatiseerde oproepinrichtingen voor het verzenden van vooraf opgenomen reclameboodschappen mogen alleen worden gebruikt als een abonnee daar uitdrukkelijk toestemming voor heeft gegeven. In het nationale recht moeten gedetailleerde voorschriften op dit gebied worden vastgesteld.

Wat het **wettelijk kader van de EU** betreft is in 2002, na een eerste poging in 1997, de richtlijn betreffende privacy en elektronische communicatie (*e-privacyrichtlijn*) aangenomen (die in 2009 is gewijzigd) om de bepalingen van de richtlijn gegevensbescherming voor de telecommunicatiesector aan te vullen en te specificeren.[290] De toepassing van de e-privacyrichtlijn is beperkt tot communicatiediensten in openbare elektronische netwerken.

In de e-privacyrichtlijn wordt onderscheid gemaakt tussen drie hoofdcategorieën gegevens die tijdens een communicatie worden gegenereerd:

289 RvE, Comité van ministers (1995), Aanbeveling Rec(95)4 aan de lidstaten inzake de bescherming van persoonsgegevens op het gebied van telecommunicatiediensten, met bijzondere nadruk op telefoondiensten, 7 februari 1995.

290 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, PB L 201 van 31.7.2002, blz. 37 (*richtlijn betreffende privacy en elektronische communicatie*), als gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, PB L 337 van 18.12.2009, blz. 11.

- de gegevens die de inhoud vormen van de berichten die tijdens de communicatie worden verzonden; deze gegevens zijn strikt vertrouwelijk;

- de gegevens die nodig zijn voor het tot stand brengen en in stand houden van de communicatie, de zogeheten verkeersgegevens, zoals informatie over de communicatiepartners en de tijd en de duur van de communicatie;

- binnen de verkeersgegevens zijn er gegevens die specifiek betrekking hebben op de locatie van de communicatieapparatuur, de zogeheten locatiegegevens; deze gegevens zijn tegelijkertijd gegevens over de locatie *van de gebruikers* van de communicatieapparatuur en zijn met name relevant waar het gaat om gebruikers van mobiele communicatieapparaten.

Verkeersgegevens kunnen door de dienstverlener alleen worden gebruikt voor facturering en om de dienst technisch te kunnen aanbieden. Indien de betrokkene daar toestemming voor geeft, kunnen deze gegevens echter ook worden verstrekt aan andere voor de verwerking verantwoordelijken die diensten met toegevoegde waarde aanbieden, zoals informatie over de locatie van het dichtstbijzijnde metrostation of de dichtstbijzijnde apotheek, of weersvoorspellingen voor deze locatie.

Andere toegang tot gegevens over communicatie in elektronische netwerken, zoals toegang met het oog op het onderzoeken van strafbare feiten, moet volgens artikel 15 van de e-privacyrichtlijn voldoen aan de eisen van gerechtvaardigde inmenging in het recht op gegevensbescherming als neergelegd in artikel 8, lid 2, van het EVRM en bevestigd door het Handvest in de artikel en 8 en 52.

Bij de wijzigingen van de e-privacyrichtlijn van 2009[291] zijn de volgende bepalingen ingevoerd:

- De restricties op het verzenden van e-mails voor direct-marketingdoeleinden zijn uitgebreid tot sms-diensten, multimediaberichtdiensten en andere, vergelijkbare typen toepassingen; e-mails met het oog op direct marketing zijn verboden tenzij voorafgaande toestemming is verkregen. Zonder deze toestemming

291 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, PB L 337 van 18.12.2009, blz. 11.

mogen alleen eerdere klanten worden benaderd met e-mails met het oog op direct marketing, indien deze hun e-mailadres ter beschikking hebben gesteld en geen bezwaar maken.

- Aan de lidstaten is een verplichting opgelegd om ervoor te zorgen dat betrokkenen rechtsvorderingen kunnen instellen in verband met inbreuken op het verbod op verzending van ongevraagde boodschappen.[292]

- Het installeren van cookies, software die het gebruik van een computer door een gebruiker monitort en registreert, is niet langer toegestaan zonder toestemming van de gebruiker van de computer. Het nationale recht moet meer gedetailleerd regelen hoe de toestemming moet worden uitgedrukt en verkregen om voor voldoende bescherming te zorgen.[293]

Wanneer een inbreuk op gegevensbeschermingswetgeving plaatsvindt als gevolg van onbevoegde toegang tot of verlies of vernietiging van gegevens, moet de toezichthoudende autoriteit onmiddellijk worden geïnformeerd. De abonnees moeten indien mogelijk worden geïnformeerd wanneer een dergelijke inbreuk mogelijk tot schade voor hen leidt.[294]

De richtlijn gegevensbewaring[295] (ongeldig verklaard op 8 april 2014) verplichtte aanbieders van communicatiediensten om verkeersgegevens beschikbaar te stellen, met name met het oog op de bestrijding van ernstige criminaliteit, gedurende een termijn van ten minste zes, maar niet langer dan 24 maanden, ongeacht of de aanbieder deze gegevens nog steeds nodig had voor factureringsdoeleinden of om de dienst technisch te kunnen aanbieden.

De EU-lidstaten moesten onafhankelijke overheidsautoriteiten aanwijzen die belast zijn met het toezicht op de beveiliging van de bewaarde gegevens.

---

292 Zie de gewijzigde richtlijn, artikel 13.

293 Zie *Ibid.*, artikel 5; zie ook Groep gegevensbescherming artikel 29 (2012), *Advies 04/2012 over ontheffing van de toestemmingsverplichting voor cookies*, WP 194, Brussel, 7 juni 2012.

294 Zie ook Groep gegevensbescherming artikel 29 (2011), *Werkdocument 01/2011 betreffende het momenteel in de EU van kracht zijnde juridisch kader met betrekking tot schendingen van persoonsgegevens en aanbevelingen voor in de toekomst te ondernemen acties,* WP 184, Brussel, 5 april 2011.

295 Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG (*richtlijn gegevensbewaring*), PB L 105 van 13.4.2006, blz. 54.

Het bewaren van telecommunicatiegegevens is duidelijk een inmenging in het recht op gegevensbescherming.[296] Of deze inmenging al dan niet is gerechtvaardigd, is een vraag die aan de orde is gesteld in verschillende gerechtelijke procedures in EU-lidstaten.[297]

Voorbeeld: In *Digital Rights Ireland en Seitlinger en anderen*[298] verklaarde het HvJ-EU de richtlijn gegevensbewaring ongeldig. Het Hof oordeelde dat de richtlijn "een zeer ruime en bijzonder zware inmenging in deze fundamentele rechten in de rechtsorde van de Unie impliceert, zonder dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke."

Een cruciaal aspect in het kader van elektronische communicatie is inmenging door overheidsautoriteiten. Middelen voor de surveillance of onderschepping van communicatie, zoals afluister- of tapapparatuur, zijn alleen toegestaan indien de wet daarin voorziet en ze een noodzakelijke maatregel in een democratische samenleving vormen die in het belang is van de bescherming van de staatsveiligheid, de openbare veiligheid of de monetaire belangen van de staat of de repressie van strafbare feiten, of van de bescherming van de betrokkene of de rechten en vrijheden van anderen.

Voorbeeld: In *Malone / Verenigd Koninkrijk*,[299] was de verzoeker een aantal strafbare feiten in verband met de onwettige behandeling van gestolen goederen ten laste gelegd. Tijdens zijn proces bleek dat een telefoongesprek van de verzoeker op grond van een door de staatssecretaris van het ministerie van Binnenlandse Zaken afgegeven bevel was onderschept. Hoewel de wijze waarop de communicatie van de verzoeker was onderschept volgens het nationale recht rechtmatig was, oordeelde het EHRM dat er geen wettelijke voorschriften waren inzake het toepassingsgebied en de wijze van uitvoering van de discretionaire bevoegdheid door de overheidsautoriteiten op dit gebied en

296 EDPS (2011), *Advies van 31 mei 2011 over het evaluatieverslag van de Commissie aan de Raad en het Europees Parlement over de richtlijn gegevensbewaring (Richtlijn 2006/24/EG)*.

297 Duitsland, Duits constitutioneel hof (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 maart 2010; Roemenië, Roemeens constitutioneel hof (*Curtea Constituțională a României*), nr. 1258, 8 oktober 2009; Tsjechië, Tsjechisch constitutioneel hof (*Ústavní soud České republiky*), 94/2011 Coll., 22 maart 2011.

298 HvJ-EU, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland en Seitlinger en anderen*, 8 april 2014.

299 EHRM, *Malone / Verenigd Koninkrijk*, nr. 8691/79, 26 april 1985.

dat de inmenging die het gevolg was van het bestaan van de praktijk in kwestie derhalve niet "in overeenstemming met de wet" was. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

8.2. Arbeidsgegevens

Belangrijkste punten

- Specifieke regels voor gegevensbescherming in arbeidsverhoudingen zijn vervat in de Aanbeveling inzake arbeidsgegevens van het RvE.
- In de richtlijn gegevensbescherming worden arbeidsverhoudingen alleen specifiek genoemd in het kader van de verwerking van gevoelige gegevens.
- De geldigheid van toestemming, die vrijelijk moet zijn gegeven, als een rechtsgrondslag voor de verwerking van gegevens over werknemers kan twijfelachtig zijn, gezien de economische ongelijkheid tussen werkgever en werknemer. De omstandigheden van de verlening van toestemming moeten zorgvuldig worden beoordeeld.

Er is geen specifiek wettelijk kader in **de EU** dat gegevensverwerking in het kader van arbeid reguleert. In de richtlijn gegevensbescherming worden arbeidsverhoudingen alleen specifiek genoemd in artikel 8, lid 2, van de richtlijn, dat betrekking heeft op de verwerking van gevoelige gegevens. **De RvE** heeft in 1989 een Aanbeveling inzake arbeidsgegevens aangenomen, die momenteel wordt geactualiseerd.[300]

Een enquête naar de meest voorkomende problemen die specifiek zijn voor de arbeidscontext is te vinden in een werkdocument van de Groep gegevensbescherming artikel 29.[301] Daarin heeft de werkgroep het belang van toestemming als rechtsgrondslag voor de verwerking van arbeidsgegevens geanalyseerd.[302] De werkgroep oordeelde dat de economische ongelijkheid tussen de werkgever die

300 Raad van Europa, Comité van ministers (1989), Aanbeveling Rec(89)2 aan de lidstaten inzake de bescherming van persoonsgegevens die worden gebruikt voor arbeidsdoeleinden, 18 januari 1989. Zie voorts het Raadplegend Comité van Verdrag 108, Studie van Aanbeveling Rec(89)2 aan de lidstaten inzake de bescherming van persoonsgegevens die worden gebruikt voor arbeidsdoeleinden en om voorstellen voor de herziening van bovengenoemde aanbeveling te doen, 9 september 2011.

301 Groep gegevensbescherming artikel 29 (2001), *Advies 8/2001 betreffende de verwerking van persoonsgegevens in het kader van de arbeidsverhouding*, WP 48, Brussel, 13 september 2001.

302 Groep gegevensbescherming artikel 29 (2005), *Werkdocument over een gemeenschappelijke interpretatie van artikel 26, lid 1, van Richtlijn 95/46/EG van 24 oktober 1995*, WP 114, Brussel, 25 november 2005.

om toestemming vraagt en de werknemer die toestemming geeft in veel gevallen vragen zal oproepen over of de toestemming vrijelijk is gegeven of niet. Bij het beoordelen van de geldigheid van toestemming in de arbeidscontext moeten de omstandigheden waaronder toestemming is vereist derhalve zorgvuldig worden onderzocht.

Een veel voorkomend gegevensbeschermingsprobleem in de typische werkomgeving van nu is in hoeverre het rechtmatig is om de elektronische communicatie van werknemers op de werkplek te monitoren. Vaak wordt gesteld dat dit probleem gemakkelijk kan worden opgelost door het privégebruik van communicatiefaciliteiten op het werk te verbieden. Een dergelijk algemeen verbod zou echter onevenredig en onrealistisch kunnen zijn. In dit verband is het volgende arrest van het EHRM van bijzonder belang:

> Voorbeeld: In *Copland / Verenigd Koninkrijk*[303] was het telefoon-, e-mail- en internetgebruik van een werkneemster van een school heimelijk gemonitord om vast te stellen of zij buitensporig veel gebruikmaakte van schoolfaciliteiten voor persoonlijke doeleinden. Het EHRM oordeelde dat telefoongesprekken vanuit bedrijfsruimten onder de begrippen privéleven en correspondentie vielen. Dergelijke vanaf het werk gevoerde gesprekken en verstuurde e-mails, evenals uit de monitoring van persoonlijk internetgebruik afgeleide informatie, worden daarom beschermd door artikel 8 van het EVRM. In het geval van de verzoekster bestonden er geen bepalingen die de omstandigheden reguleerden waaronder werkgevers het telefoon-, e-mail- en internetgebruik van werknemers konden monitoren. De inmenging was derhalve niet in overeenstemming met de wet. Het Hof concludeerde dat er sprake was van een inbreuk op artikel 8 van het EVRM.

Volgens de Aanbeveling inzake arbeidsgegevens van de RvE moeten persoonsgegevens die worden verzameld voor arbeidsdoeleinden rechtstreeks bij de individuele werknemers worden betrokken.

De verzameling van persoonsgegevens voor aanwervingsdoeleinden moet worden beperkt tot de informatie die noodzakelijk is om de geschiktheid van kandidaten en hun carrièrepotentieel te beoordelen.

303 EHRM, *Copland / Verenigd Koninkrijk*, nr. 62617/00, 3 april 2007.

Ook wordt in de aanbeveling specifiek verwezen naar op oordeelsvorming gebaseerde gegevens met betrekking tot de prestaties of het potentieel van individuele werknemers. Op oordeelsvorming gebaseerde gegevens moeten zijn gebaseerd op eerlijke en redelijke evaluaties en mogen niet beledigend geformuleerd zijn. Dit wordt vereist door de beginselen van eerlijke gegevensverwerking en juistheid van de gegevens.

Een specifiek aspect van gegevensbeschermingswetgeving in de verhouding werkgever-werknemer is de rol van werknemersvertegenwoordigers. Dergelijke vertegenwoordigers mogen alleen persoonsgegevens van werknemers ontvangen voor zover dit noodzakelijk is om ze in staat te stellen de werknemers te vertegenwoordigen.

Gevoelige persoonsgegevens die worden verzameld voor arbeidsdoeleinden mogen alleen in specifieke gevallen worden verwerkt en zijn onderworpen aan de in het nationale recht neergelegde waarborgen. Werkgevers mogen werknemers of sollicitanten alleen naar hun gezondheidstoestand vragen en medisch laten keuren indien dit noodzakelijk is om hun geschiktheid voor de baan te beoordelen, de vereisten van preventieve geneeskunde te vervullen of de toekenning van sociale uitkeringen mogelijk te maken. Gezondheidsgegevens mogen niet worden verzameld uit andere bronnen dan de betrokken werknemer, behoudens wanneer uitdrukkelijke en geïnformeerde toestemming is verkregen of het nationale recht daarin voorziet.

Volgens de Aanbeveling inzake arbeidsgegevens moeten werknemers worden geïnformeerd over het doeleinde van de verwerking van hun persoonsgegevens, het type opgeslagen persoonsgegevens, de entiteiten waaraan de gegevens regelmatig worden meegedeeld en het doeleinde en de rechtsgrondslag van deze mededelingen. Ook moeten werkgevers hun werknemers van tevoren informeren over de invoering of aanpassing van geautomatiseerde systemen voor de verwerking van persoonsgegevens of voor het monitoren van de bewegingen of de productiviteit van werknemers.

Werknemers moeten recht op toegang tot hun arbeidsgegevens hebben, evenals een recht op rectificatie of uitwissing. Indien op oordeelsvorming gebaseerde gegevens worden verwerkt, moeten werknemers voorts het recht hebben om het oordeel aan te vechten. Deze rechten mogen echter tijdelijk worden beperkt voor interne onderzoeksdoeleinden. Indien een werknemer toegang, rectificatie of

uitwissing van persoonlijke arbeidsgegevens wordt geweigerd, moet het nationale recht voorzien in passende procedures om de weigering te betwisten.

8.3. Medische gegevens

Belangrijkste punt

- Medische gegevens zijn gevoelige gegevens en genieten daarom specifieke bescherming.

Persoonsgegevens die de gezondheidstoestand van de betrokkene betreffen worden door artikel 8, lid 1, van de richtlijn gegevensbescherming en artikel 6 van Verdrag 108 aangemerkt als gevoelige gegevens. Medische gegevens zijn daarom onderworpen aan strengere gegevensverwerkingsregels dan niet-gevoelige gegevens.

Voorbeeld: In *Z. / Finland*[304] had de ex-echtgenoot van de verzoekster, die besmet was met hiv, een aantal seksuele misdrijven gepleegd. Vervolgens was hij veroordeeld voor doodslag op grond van het feit dat hij zijn slachtoffers bewust had blootgesteld aan het risico van een hiv-infectie. De nationale rechtbank had verordend dat de volledige gerechtelijke uitspraak en de zaaksdocumenten gedurende een termijn van tien jaar vertrouwelijk moesten blijven, ondanks verzoeken van de verzoeksters om een langere termijn vast te stellen. Deze verzoeken werden door het hof van beroep afgewezen, en in het arrest van het hof werden de volledige namen van zowel de verzoekster als haar ex-echtgenoot genoemd. Het EHRM oordeelde dat de inmenging niet noodzakelijk moest worden geacht in een democratische samenleving, aangezien de bescherming van medische gegevens van wezenlijk belang is voor de uitoefening van het recht op eerbiediging van het privé-, familie- en gezinsleven, met name wanneer het gaat om hiv-infecties, gezien het stigma dat daar in veel samenlevingen op rust. Het Hof oordeelde bijgevolg dat het verlenen van toegang tot de identiteit en de medische toestand van de verzoekster als beschreven in het arrest van het hof van beroep na een termijn van niet langer

304 EHRM, *Z. / Finland*, nr. 22009/93, 25 februari 1997, punten 94 en 112; zie ook EHRM, *M.S. / Zweden*, nr. 20837/92, 27 augustus 1997, EHRM, *L.L. / Frankrijk*, nr. 7508/02, 10 oktober 2006, EHRM, *I. / Finland*, nr. 20511/03, 17 juli 2008, EHRM, *K.H. en anderen / Slowakije*, nr. 32881/04, 28 april 2009, EHRM, *Szuluk / het Verenigd Koninkrijk*, nr. 36936/05, 2 juni 2009.

dan tien jaar na de datum van het arrest een schending van artikel 8 van het EHRM zou vormen.

Artikel 8, lid 3, van de richtlijn gegevensbescherming staat de verwerking van medische gegevens toe wanneer dit noodzakelijk is voor de doeleinden van preventieve geneeskunde of medische diagnose, het verstrekken van zorg of behandelingen of het beheer van gezondheidsdiensten. Deze verwerking is echter alleen toegestaan wanneer de gegevens worden verwerkt door een gezondheidswerker die onderworpen is aan het beroepsgeheim of door een andere persoon voor wie een gelijkwaardige geheimhoudingsplicht geldt.[305]

In zijn Aanbeveling inzake medische gegevens van 1997 heeft de RvE de beginselen van Verdrag 108 meer in detail toegepast op gegevensverwerking op medisch gebied.[306] De voorgestelde regels zijn in overeenstemming met die van de richtlijn gegevensbescherming wat betreft het rechtmatige doeleinde van de verwerking van medische gegevens, het noodzakelijk beroepsgeheim voor personen die gezondheidsgegevens gebruiken en de rechten van de betrokkenen op transparantie, toegang, rectificatie en uitwissing. Voorts mogen medische gegevens die rechtmatig door gezondheidswerkers worden verwerkt niet worden overgedragen aan rechtshandhavingsautoriteiten, tenzij er "voldoende waarborgen worden geboden om openbaarmaking die niet consistent is met (...) de eerbiediging van het privéleven als gegarandeerd door artikel 8 van het EHRM, te voorkomen".[307]

Voorts bevat de Aanbeveling inzake medische gegevens bijzondere bepalingen ten aanzien van de medische gegevens van ongeboren kinderen en wilsonbekwame personen en de verwerking van generieke gegevens. Wetenschappelijk onderzoek wordt uitdrukkelijk erkend als een reden om gegevens langer te bewaren dan dat ze nodig zijn, hoewel dit doorgaans anonimisering zal vereisen. Artikel 12 van de Aanbeveling inzake medische gegevens bevat gedetailleerde regels voor situaties waarin onderzoekers persoonsgegevens nodig hebben en geanonimiseerde gegevens onvoldoende zijn.

Pseudonimisering kan een passend beveiligingsmiddel zijn om wetenschappelijke behoeften te vervullen en tegelijkertijd de belangen van de betrokken patiënten te

305 Zie ook EHRM, *Biriuk / Litouwen*, nr. 23373/03, 25 november 2008.

306 RvE, Comité van ministers (1997), Aanbeveling Rec(97)5 aan de lidstaten tot bescherming van de medische gegevens, 13 februari 1997.

307 EHRM, nr. 1585/09, *Avilkina en anderen / Rusland*, 6 juni 2013, punt 53 (niet definitief).

beschermen. Het concept pseudonimisering in het kader van gegevensbescherming wordt nader toegelicht in paragraaf 2.3.1.

Op nationaal en Europees niveau vinden intensieve discussies plaats over initiatieven om gegevens over de medische behandelingen van een patiënt op te slaan in een elektronisch patiëntendossier.[308] Een bijzonder aspect van nationale systemen van elektronische gezondheidsdossiers is de grensoverschrijdende beschikbaarheid ervan: een onderwerp dat in het kader van grensoverschrijdende gezondheidszorg binnen de EU van specifiek belang is.[309]

Een ander gebied ten aanzien waarvan wordt gediscussieerd over nieuwe bepalingen, zijn klinische proeven, d.w.z. het uittesten van nieuwe geneesmiddelen op patiënten in een gedocumenteerde onderzoeksomgeving; ook dit onderwerp heeft aanzienlijke gegevensbeschermingsimplicaties. Klinische proeven van medische producten voor menselijk gebruik zijn gereguleerd in Richtlijn 2001/20/EG van het Europees Parlement en de Raad van 4 april 2001 betreffende de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten inzake de toepassing van goede klinische praktijken bij de uitvoering van klinische proeven met geneesmiddelen voor menselijk gebruik (*richtlijn inzake klinische proeven*).[310] In december 2012 heeft de Europese Commissie een voorstel voor een verordening ingediend ter vervanging van de richtlijn inzake klinische proeven, met als doel om klinische procedures uniformer en efficiënter te maken.[311]

Op EU-niveau is een groot aantal andere wetgevings- en andere initiatieven geïnitieerd met betrekking tot persoonsgegevens in de gezondheidszorgsector.[312]

---

308 Groep gegevensbescherming artikel 29 (2007), Werkdocument inzake de verwerking van persoonsgegevens betreffende gezondheid in elektronische medische dossiers, WP 131, Brussel, 15 februari 2007.

309 Richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg, PB L 88 van 4.4.2011, blz. 45.

310 Richtlijn 2001/20/EG van het Europees Parlement en de Raad van 4 april 2001 betreffende de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten inzake de toepassing van goede klinische praktijken bij de uitvoering van klinische proeven met geneesmiddelen voor menselijk gebruik, PB L 121 van 1.5.2001, blz. 34.

311 Europese Commissie (2012), Voorstel voor een verordening van het Europees Parlement en de Raad betreffende klinische proeven met geneesmiddelen voor menselijk gebruik en tot intrekking van Richtlijn 2001/20/EG, COM(2012) 369 definitief, Brussel, 17 juli 2012.

312 EDPS (2013), *Advies van de Europese Toezichthouder voor gegevensbescherming inzake de mededeling van de Commissie over een "Actieplan e-gezondheidszorg 2012-2020 – Innovatieve gezondheidszorg voor de 21e eeuw",* Brussel, 27 maart 2013.

8.4. Gegevensverwerking voor statistische doeleinden

Belangrijkste punten

- Gegevens die worden verwerkt voor statistische doeleinden mogen niet voor andere doeleinden worden gebruikt.
- Gegevens die rechtmatig worden verzameld voor andere doeleinden mogen verder worden gebruikt voor statistische doeleinden, mits het nationale recht passende garanties biedt die door de gebruikers worden gerespecteerd. Hiertoe moet met name worden voorzien in anonimisering of pseudonomisering van de gegevens voordat ze aan derden worden meegedeeld.

In de richtlijn gegevensbescherming wordt gegevensverwerking voor statistische doeleinden genoemd in het kader van mogelijke uitzonderingen op gegevensverwerkingsbeginselen. Artikel 6, lid 1, onder b), van de richtlijn bepaalt dat het beginsel van doelbinding in het nationale recht ondergeschikt kan worden gemaakt aan het verdere gebruik van gegevens voor statistische doeleinden, hoewel het nationale recht in dat geval alle noodzakelijke garanties moet bieden. Artikel 13, lid 2, van de richtlijn voorziet in de mogelijkheid om de toegangsrechten bij nationaal recht te beperken wanneer de gegevens uitsluitend voor statistische doeleinden worden verwerkt; ook hier weer moet het nationale recht in dat geval passende garanties bieden. In dit verband stelt de richtlijn gegevensbescherming de specifieke vereiste dat geen van de gegevens die in de loop van statistische onderzoek worden verworven of gecreëerd mag worden gebruikt om concrete besluiten ten aanzien van individuele betrokkenen te nemen.

Hoewel gegevens die door een voor de verwerking verantwoordelijke rechtmatig voor enig doel zijn verzameld, door deze voor de verwerking verantwoordelijke mogen worden hergebruikt voor eigen statistische doeleinden – zogeheten secundaire statistieken – zouden de gegevens al naar gelang de context moeten worden geanonimiseerd of gepseudonimiseerd voordat ze aan derden worden meegedeeld voor statistische doeleinden, tenzij de betrokkene daarvoor toestemming heeft verleend of daar in het nationale recht specifiek in wordt voorzien. Dit volgt uit de eis van passende garanties van artikel 6, lid 1, onder b), van de richtlijn gegevensbescherming.

De belangrijkste voorbeelden van het gebruik van gegevens voor statistische doeleinden zijn officiële statistieken die door bureaus voor de statistiek op nationaal en EU-niveau worden opgesteld op grond van nationale en EU-wetgeving inzake officiele statistieken. Volgens deze wetgeving zijn burgers en ondernemingen doorgaans verplicht om gegevens aan de statistische autoriteiten te verstrekken. Ambtenaren die bij bureaus voor de statistiek werken zijn gebonden aan een bijzonder beroepsgeheim dat zorgvuldig in acht moet worden genomen, aangezien dat essentieel is voor een hoog niveau van vertrouwen onder burgers, dat weer nodig is voor het verkrijgen van gegevens door de statistische autoriteiten.

Verordening (EG) nr. 223/2009 betreffende de Europese statistiek (*verordening betreffende de Europese statistiek*) bevat essentiële voorschriften voor gegevensbescherming in officiële statistieken en kan derhalve ook als relevant worden beschouwd voor bepalingen inzake officiële statistieken op nationaal niveau.[313] De verordening gaat uit van het beginsel dat het opstellen van officiële statistieken een voldoende precieze rechtsgrondslag vereist.[314]

Voorbeeld: In *Huber / Bondsrepubliek Duitsland*[315] oordeelde het HvJ-EU dat de verzameling en opslag van persoonsgegevens door een autoriteit voor statistische doeleinden op zichzelf niet een voldoende reden vormden om een verwerking rechtmatig te maken. De wet die voorzag in de verwerking van persoonsgegevens moest ook voldoen aan de vereiste van noodzakelijkheid, hetgeen in de gegeven context niet het geval was.

De Aanbeveling inzake statistische gegevens van de RvE van 1997 heeft betrekking op het opstellen van statistieken in de publieke en private sector.[316] Bij deze

313 Verordening (EG) nr. 223/2009 van het Europees Parlement en de Raad van 11 maart 2009 betreffende de Europese statistiek en tot intrekking van Verordening (EG, Euratom) nr. 1101/2008 van het Europees Parlement en de Raad betreffende de toezending van onder de statistische geheimhoudingsplicht vallende gegevens aan het Bureau voor de Statistiek van de Europese Gemeenschappen, Verordening (EG) nr. 322/97 van de Raad betreffende de communautaire statistiek en Besluit 89/382/EEG, Euratom van de Raad tot oprichting van een Comité statistisch programma van de Europese Gemeenschappen, PB L 87 van 31.3.2009, blz. 164.

314 Dit beginsel wordt verder uitgewerkt in de Praktijkcode voor Europese statistiek van Eurostat, die overeenkomstig artikel 11 van de verordening betreffende de Europese statistiek een ethische leidraad biedt voor het opstellen van officiële statistieken, met inbegrip van het weloverwogen gebruik van persoonsgegevens, en die beschikbaar is op: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 HvJ-EU, zaak C-524/06 , *Huber / Bondsrepubliek Duitsland*, 16 december 2008, zie met name punt 68.

316 Raad van Europa, Comité van ministers (1997), Aanbeveling Rec(97)18 aan de lidstaten inzake de bescherming van persoonsgegevens die worden verzameld en verwerkt voor statistische doeleinden, 30 september 1997.

aanbeveling werden beginselen ingevoerd die overeenkomen met de belangrijkste, hierboven beschreven voorschriften van de richtlijn gegevensbescherming. Ten aanzien van de hiernavolgende aangelegenheden worden meer gedetailleerde regels gegeven.

Terwijl gegevens die door een voor de verwerking verantwoordelijke worden verzameld voor statistische doeleinden niet mogen worden gebruikt voor andere doeleinden, moeten gegevens die worden verzameld voor niet-statistische doeleinden beschikbaar zijn voor verder statistisch gebruik. De Aanbeveling inzake statistische gegevens staat zelfs toe dat gegevens aan derden worden meegedeeld als dit uitsluitend voor statistische doeleinden is. In dergelijke gevallen moeten de partijen overeenstemming bereiken over het rechtmatige verdere gebruik voor statistische doeleinden en dit schriftelijk vastleggen. Aangezien dit niet als een substituut voor toestemming door de betrokkene kan dienen, moet worden aangenomen dat het nationale recht voorziet in aanvullende passende garanties om de risico's van verkeerd gebruik van persoonsgegevens te minimaliseren, zoals een verplichting om gegevens voorafgaand aan een doorgifte te anonimiseren of te pseudonimiseren.

Personen die beroepsmatig te maken hebben met statistisch onderzoek moeten krachtens het nationale recht worden gebonden aan een bijzonder beroepsgeheim – zoals dat typisch ook geldt voor personen die betrokken zijn bij het opstellen van officiële statistieken. Dit dient zich ook uit te strekken tot interviewers indien deze betrokken zijn bij de verzameling van gegevens bij betrokkenen of andere personen.

Als een statistische enquête waarin gebruik wordt gemaakt van persoonsgegevens niet wettelijk is voorgeschreven, zouden betrokkenen toestemming moeten geven voor het gebruik van hun gegevens om dit gebruik rechtmatig te maken of zou hun ten minste de mogelijkheid moeten worden geboden om zich tegen het gebruik van hun gegevens te verzetten. Indien persoonsgegevens worden verzameld voor statistische doeleinden door personen te interviewen, moet aan deze personen duidelijk worden meegedeeld of de verstrekking van gegevens volgens het nationale recht verplicht is of niet. Gevoelige gegevens mogen nooit op zodanige wijze worden verzameld dat een persoon kan worden geïdentificeerd, tenzij het nationale recht dit uitdrukkelijk toestaat.

Wanneer een statistische enquête niet kan worden uitgevoerd zonder anonieme gegevens, en persoonsgegevens inderdaad noodzakelijk zijn, moeten de gegevens die voor dit doeleinde worden verzameld zo spoedig als haalbaar is worden

geanonimiseerd. De resultaten van de statistische enquête mogen op geen enkele wijze de identificatie van enige betrokkene mogelijk maken, tenzij hier duidelijk geen risico's aan verbonden zijn.

Nadat de statistische analyse is verricht, moeten de gebruikte persoonsgegevens ofwel worden uitgewist, ofwel anoniem worden gemaakt. In dit geval wordt in de Aanbeveling inzake statistische gegevens voorgesteld dat identificatiegegevens gescheiden van andere persoonsgegevens worden opgeslagen. Dit betekent bijvoorbeeld dat de gegevens moeten worden gepseudonimiseerd en dat de encryptiesleutel of de lijst met de identificerende synoniemen gescheiden van de gepseudonimiseerde gegevens moet worden opgeslagen.

8.5. Financiële gegevens

Belangrijkste punten

- Hoewel financiële gegevens geen gevoelige gegevens in de zin van Verdrag 108 of de richtlijn gegevensbescherming zijn, moeten passende waarborgen worden geboden voor de verwerking ervan met het oog op de juistheid en de beveiliging van de gegevens.
- In elektronische betalingssystemen moet gegevensbescherming zijn ingebouwd (de zogeheten privacy by design).
- Op dit gebied doen zich bijzondere gegevensbeschermingsvraagstukken voor als gevolg van de noodzaak om over passende authenticatiemechanismen te beschikken.

Voorbeeld: In *Michaud / Frankrijk*[317] betwistte de verzoeker, een Franse advocaat, zijn verplichting uit hoofde van het Franse recht om verdenkingen over mogelijke witwasactiviteiten door zijn cliënten te melden. Het EHRM merkte op dat een verplichting voor advocaten om informatie met betrekking tot een andere persoon, die in hun bezit is gekomen door middel van uitwisselingen met die persoon, aan de administratieve autoriteiten te melden, een inmenging in het recht van advocaten op eerbiediging van hun correspondentie en privéleven als neergelegd in artikel 8 van het EVRM vormde, aangezien dat begrip ook beroeps- of zakelijke activiteiten omvatte. De inmenging was echter in

317 EHRM, *Michaud / Frankrijk*, nr. 12323/11, 6 december 2012; zie ook EHRM, *Niemietz / Duitsland*, nr. 13710/88, 16 december 1992, punt 29, en EHRM, *Halford / Verenigd Koninkrijk*, nr. 20605/92, 25 juni 1997, punt 42.

overeenstemming met de wet en diende een rechtmatig doel, namelijk de preventie van wanordelijkheden en strafbare feiten. Aangezien advocaten waren onderworpen aan de verplichting om verdenkingen alleen in zeer beperkte omstandigheden te melden, oordeelde het Hof dat deze verplichting evenredig was en concludeerde het dat er geen inbreuk op artikel 8 had plaatsgevonden.

Een toepassing van het algemene wettelijk kader voor gegevensbescherming, zoals vervat in Verdrag 108, op de context van betalingen is door de RvE ontwikkeld in Aanbeveling Rec(90)19 van 1990.[318] In deze aanbeveling wordt het toepassingsgebied van rechtmatige verzameling en rechtmatig gebruik van gegevens in het kader van betalingen, in het bijzonder betalingen door middel van creditcards, verduidelijkt. Voorts worden aan de nationale wetgevers voorstellen gedaan voor gedetailleerde regelgeving inzake de grenzen aan de communicatie van betalingsgegevens aan derden, termijnen voor het bewaren van deze gegevens, transparantie, gegevensbeveiliging en grensoverschrijdend gegevensverkeer en, tot slot, toezicht en rechtsmiddelen. De voorgestelde oplossingen komen overeen met wat later het algemene gegevensbeschermingskader van de EU is geworden in de richtlijn gegevensbescherming.

Voor de regulering van markten voor financiële instrumenten en de activiteiten van kredietinstellingen en beleggingsondernemingen wordt een aantal rechtsinstrumenten gecreëerd.[319] Andere rechtsinstrumenten zijn bedoeld om de bestrijding van handel in voorkennis en markmanipulatie te ondersteunen.[320] De meest

318 RvE, Comité van ministers (1990), Aanbeveling Rec(90)19 inzake de bescherming van persoonsgegevens die worden gebruikt voor betalingen en aanverwante activiteiten, 13 september 1990.

319 Europese Commissie (2011), Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende markten voor financiële instrumenten en houdende intrekking van Richtlijn 2004/39/EG van het Europees Parlement en de Raad, COM(2011) 656 definitief, Brussel, 20 oktober 2011; Europese Commissie (2011), Voorstel voor een verordening van het Europees Parlement en de Raad betreffende markten in financiële instrumenten en tot wijziging van Verordening [EMIR] betreffende otc-derivaten, centrale tegenpartijen en transactieregisters, COM(2011) 652 definitief, Brussel, 20 oktober 2011; Europese Commissie (2011), Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de toegang tot de werkzaamheden van kredietinstellingen en het bedrijfseconomisch toezicht op kredietinstellingen en beleggingsondernemingen en tot wijziging van Richtlijn 2002/87/EG van het Europees Parlement en de Raad betreffende het aanvullende toezicht op kredietinstellingen, verzekeringsondernemingen en beleggingsondernemingen in een financieel conglomeraat, COM(2011) 453 definitief, Brussel, 20 juli 2011.

320 Europese Commissie (2011), *Voorstel voor een verordening van het Europees Parlement en de Raad betreffende handel met voorwetenschap en marktmanipulatie (marktmisbruik)*, COM(2011) 651 definitief, Brussel, 20 oktober 2011; Europese Commissie (2011), Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende strafrechtelijke sancties voor handel met voorwetenschap en marktmanipulatie, COM(2011) 654 definitief, Brussel, 20 oktober 2011.

fundamentele vraagstukken op deze gebieden die van invloed zijn op gegevensbescherming zijn:

- de bewaring van bestanden over financiële transacties;
- de doorgifte van persoonsgegevens aan derde landen;
- het opnemen van telefoongesprekken of elektronische communicaties, met inbegrip van de bevoegdheid van de bevoegde autoriteiten om bestanden van telefoon- en gegevensverkeer op te vragen;
- het meedelen van persoonlijke informatie, waaronder de publicatie van sancties;
- de toezicht- en onderzoeksbevoegdheden van de bevoegde autoriteiten, met inbegrip van inspecties ter plaatse en het betreden van private ruimten om documenten in beslag te nemen;
- de mechanismen voor het melden van inbreuken, d.w.z. klokkenluidersregelingen;
- de samenwerking tussen bevoegde autoriteiten van de lidstaten van de Europese Autoriteit voor effecten en markten (ESMA).

Ook zijn er op dit gebied andere onderwerpen die specifiek zijn gereguleerd, zoals de verzameling van gegevens over de financiële status van betrokkenen[321] of grensoverschrijdende betalingen door middel van bankoverschrijvingen, die onvermijdelijk tot verkeer van persoonsgegevens leiden.[322]

321 Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad van 16 september 2009 inzake ratingbureaus, PB L 302 van 17.11.2009, blz. 1; Europese Commissie, Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EG) nr. 1060/2009 van het Europees Parlement en de Raad inzake ratingbureaus, COM(2010) 289 definitief, Brussel, 2 juni 2010.

322 Richtlijn 2007/64/EG van het Europees Parlement en de Raad van 13 november 2007 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG, PB L 319 van 5.12.2007, blz. 1.

Aanbevolen literatuur

Hoofdstuk 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Wenen, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection*, Brussel, beschikbaar op: www.edri.org/files/paper06_datap.pdf.

Frowein, J. en Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlijn, N. P. Engel Verlag.

Grabenwarter, C. en Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. en Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. en Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerpen, Intersentia N.V., Neuer Wissenschaftlicher Verlag.

Picharel, C. en Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brussel, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, nr. 5, blz. 281-288.

Warren, S. en Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review,* vol. 4, nr. 5, blz. 193-220, beschikbaar op: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. en Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Hoofdstuk 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Parijs, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. en Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Londen, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, vol. 57, nr. 6, blz. 1701-1777.

Tinnefeld, M., Buchner, B. en Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*, beschikbaar op: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Hoofdstukken 3 tot en met 5

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' in: Grabitz, E., Hilf, M. en Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, München, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cádiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. en Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Europees Bureau voor de grondrechten van de Europese Unie) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxemburg, Publicatiebureau van de Europese Unie (Publicatiebureau).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conferentie-editie), Wenen, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburg, Publicatiebureau.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*, beschikbaar op: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Hoofdstuk 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. en Nouwt, S. (2009), *Reinventing data protection?*, Berlijn, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *European data protection law*, Oxford, Oxford University Press.

Hoofdstuk 7

Europol (2012), *Data Protection at Europol*, Luxemburg, Publicatiebureau, beschikbaar op: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Den Haag, Eurojust.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime,* ERA Forum, vol. 13, nr. 3, blz. 381-395.

Gutwirth, S., Poullet, Y. en De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. en Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, vol. 36, nr. 5, blz. 722-776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2, beschikbaar op: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Hoofdstuk 8

Büllesbach, A., Gijrath, S., Poullet, Y. en Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. en Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. en De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. en Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, *European Law Review*, vol. 36, nr. 5, blz. 722-776.

Rosemary, J. en Hamilton, A. (2012), *Data protection law and practice*, Londen, Sweet & Maxwell.

Jurisprudentie

Geselecteerde jurisprudentie van het Europees Hof voor de Rechten van de Mens

Toegang tot persoonsgegevens

Gaskin / Verenigd Koninkrijk, nr. 10454/83, 7 juli 1989
Godelli / Italië, nr. 33783/09, 25 september 2012
K.H. en anderen / Slowakije, nr. 32881/04, 28 april 2009
Leander / Zweden, nr. 9248/81, 26 maart 1987
Odièvre / Frankrijk [GC], nr. 42326/98, 13 februari 2003

Afwegen van gegevensbescherming met de vrijheid van meningsuiting

Axel Springer AG / Duitsland [GC], nr. 39954/08, 7 februari 2012
Von Hannover / Duitsland, nr. 59320/00, 24 juni 2004
Von Hannover / Duitsland (nr. 2) [GC], nrs. 40660/08 en 60641/08, 7 februari 2012

Uitdagingen in de bescherming van gegevens op internet

K.U. / Finland, nr. 2872/02, 2 december 2008

Correspondentie

Amann / Zwitserland [GC], nr. 27798/95, 16 februari 2000
Bernh Larsen Holding AS en anderen / Noorwegen, nr. 24117/08, 14 maart 2013
Cemalettin Canli / Turkije, nr. 22427/04, 18 november 2008

Dalea / Frankrijk, nr. 964/07, 2 februari 2010
Gaskin / Verenigd Koninkrijk, nr. 10454/83, 7 juli 1989
Haralambie / Roemenië, nr. 21737/03, 27 oktober 2009
Khelili / Zwitserland, nr. 16188/07, 18 oktober 2011
Leander / Zweden, nr. 9248/81, 26 maart 1987
Malone / Verenigd Koninkrijk, nr. 8691/79, 26 april 1985
McMichael / Verenigd Koninkrijk, nr. 16424/90, 24 februari 1995
M.G. / Verenigd Koninkrijk, nr. 39393/98, 24 september 2002
Rotaru / Roemenië [GC], nr. 28341/95, 4 mei 2000
S. en Marper / Verenigd Koninkrijk, nrs. 30562/04 en 30566/04, 4 december 2008
Shimovolos / Rusland, nr. 30194/09, 21 juni 2011
Turek / Slowakije, nr. 57986/00, 14 februari 2006

Strafrechtelijke databanken

B.B. / Frankrijk, nr. 5335/06, 17 december 2009
M.M. / Verenigd Koninkrijk, nr. 24029/07, 13 november 2012

Dna-databanken

S. en Marper / Verenigd Koninkrijk, nrs. 30562/04 en 30566/04, 4 december 2008

Gps-gegevens

Uzun / Duitsland, nr. 35623/05, 2 september 2010

Gezondheidsgegevens

Biriuk / Litouwen, nr. 2337/03, 25 november 2008
I. / Finland, nr. 20511/03, 17 juli 2008
L.L. / Frankrijk, nr. 7508/02, 10 oktober 2006
M.S. / Zweden, nr. 34209/96, 2 juli 2002
Szuluk / Verenigd Koninkrijk, nr. 36936/05, 2 juni 2009
Z. / Finland, nr. 22009/93, 25 februari 1997

Identiteit

Ciubotaru / Moldavië, nr. 27138/04, 27 april 2010
Godelli / Italië, nr. 33783/09, 25 september 2012
Odièvre / Frankrijk [GC], nr. 42326/98, 13 februari 2003

Informatie met betrekking tot beroepswerkzaamheden

Michaud / Frankrijk, nr. 12323/11, 6 december 2012
Niemietz / Duitsland, nr. 13710/88, 16 december 1992

Onderscheppen van communicatie

Amann / Zwitserland [GC], nr. 27798/95, 16 februari 2000
Copland / Verenigd Koninkrijk, nr. 62617/00, 3 april 2007
Cotlet / Roemenië, nr. 38565/97, 3 juni 2003
Kruslin / Frankrijk, nr. 11801/85, 24 april 1990
Lambert / Frankrijk, nr. 23618/94, 24 augustus 1998
Liberty en anderen / Verenigd Koninkrijk, nr. 58243/00, 1 juli 2008
Malone / Verenigd Koninkrijk, nr. 8691/79, 26 april 1985
Halford / Verenigd Koninkrijk, nr. 20605/92, 25 juni 1997
Szuluk / Verenigd Koninkrijk, nr. 36936/05, 2 juni 2009

Verplichtingen voor instellingen die verantwoordelijkheden hebben ten aanzien van het realiseren van rechten ("duty bearers")

B.B. / Frankrijk, nr. 5335/06, 17 december 2009
I. / Finland, nr. 20511/03, 17 juli 2008
Mosley / Verenigd Koninkrijk, nr. 48009/08, 10 mei 2011

Foto's

Sciacca / Italië, nr. 50774/09, 11 januari 2005
Von Hannover / Duitsland, nr. 59320/00, 24 juni 2004

Recht om te worden vergeten

Segerstedt-Wiberg en anderen / Zweden, nr. 62332/00, 6 juni 2006

Recht van verzet

Leander / Zweden, nr. 9248/81, 26 maart 1987
Mosley / Verenigd Koninkrijk, nr. 48009/08, 10 mei 2011
M.S. / Zweden, nr. 34209/96, 2 juli 2002
Rotaru / Roemenië [GC], nr. 28341/95, 4 mei 2000

Categorieën gevoelige gegevens

I. / Finland, nr. 20511/03, 17 juli 2008
Michaud / Frankrijk, nr. 12323/11, 6 december 2012
S. en Marper / Verenigd Koninkrijk, nrs. 30562/04 en 30566/04, 4 december 2008

Toezicht en handhaving (taken van verschillende actoren, waaronder gegevensbeschermingsautoriteiten)

I. / Finland, nr. 20511/03, 17 juli 2008
K.U. / Finland, nr. 2872/02, 2 december 2008
Von Hannover / Duitsland, nr. 59320/00, 24 juni 2004
Von Hannover / Duitsland (nr. 2) [GC], nrs. 40660/08 en 60641/08, 7 februari 2012.

Surveillancemethoden

Allan/ Verenigd Koninkrijk, nr. 48539/99, 5 november 2002
Vereniging "21 Décembre 1989" en anderen / Roemenië, nrs. 33810/07 en 18817/08, 24 mei 2011
Bykov / Rusland [GC], nr. 4378/95, 10 maart 2009
Kennedy / Verenigd Koninkrijk, nr. 26839/05, 18 mei 2010
Klass en anderen / Duitsland, nr. 5029/71, 6 september 1978
Rotaru / Roemenië [GC], nr. 28341/95, 4 mei 2000
Taylor-Sabori / Verenigd Koninkrijk, nr. 47114/99, 22 oktober 2002
Uzun / Duitsland, nr. 35623/05, 2 september 2010
Vetter / Frankrijk, nr. 59842/00, 31 mei 2005

Videobewaking

Köpke / Duitsland, nr. 420/07, 5 oktober 2010
Peck / Verenigd Koninkrijk, nr. 44647/98, 28 januari 2003

Stemmonsters

P.G. en J.H. / Verenigd Koninkrijk, nr. 44787/98, 25 september 2001
Wisse / Frankrijk, nr. 71611/11, 20 december 2005

Geselecteerde jurisprudentie van het Hof van Justitie van de Europese Unie

Jurisprudentie met betrekking tot de richtlijn gegevensbescherming

Zaak C-73/07, *Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy en Satamedia Oy*, 16 december 2008

[Begrip "journalistieke activiteiten" in de zin van artikel 9 van de richtlijn gegevensbescherming]

Gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke GbR en Hartmut Eifert / Land Hessen*, 9 november 2010

[Evenredigheid van de wettelijke verplichting om persoonsgegevens van de begunstigden van bepaalde EU-landbouwfondsen te publiceren]

Zaak C-101/01, *Bodil Lindqvist*, 6 november 2003

[Rechtmatigheid van de publicatie van gegevens over het privéleven van anderen op internet door een particulier]

Zaak C-131/12, *Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González*, verzoek om een prejudiciële beslissing van de *Audiencia Nacional* (Spanje), ingediend op 9 maart 2012, 25 mei 2012, in behandeling

[Verplichting van aanbieders van zoekmachines om op verzoek van de betrokkene af te zien van het tonen van persoonsgegevens in de zoekresultaten]

Zaak C-270/11, *Europese Commissie / Koninkrijk Zweden*, 30 mei 2013

[Boete voor het niet ten uitvoer leggen van een richtlijn]

Zaak C-275/06, *Productores de Música de España (Promusicae) / Telefónica de España SAU*, 29 januari 2008

[Verplichting van aanbieders van toegang tot internet om de identiteit van gebruikers van KaZaA-programma's voor de uitwisseling van bestanden mee te delen aan de vereniging voor de bescherming van intellectuele-eigendomsrechten]

Zaak C-288/12, *Europese Commissie / Hongarije*, 8 april 2014

[Rechtmatigheid van de ontzetting uit zijn ambt van de nationale toezichthouder gegevensbescherming]

Zaak C-291/12, *Michael Schwarz / Stadt Bochum*, conclusie van de advocaat-generaal, 13 juni 2013
[Schending van het primaire EU-recht door Verordening (EG) nr. 2252/2004 door de bepaling dat vingerafdrukken in paspoorten moeten worden opgeslagen]

Zaak C-360/10, *SABAM / Netlog N.V.*, 16 februari 2012
[Verplichting van aanbieders van sociale netwerken om onrechtmatig gebruik van muzikale en audiovisuele werken door gebruikers van hun netwerk te voorkomen]

Gevoegde zaken C-465/00, C-138/01 en C-139/01, *Rechnungshof / Österreichischer Rundfunk en anderen en Neukomm en Lauermann / Österreichischer Rundfunk*, 20 mei 2003
[Evenredigheid van wettelijke verplichtingen om persoonsgegevens over de salarissen van werknemers van bepaalde categorieën van aan de publieke sector gerelateerde instellingen te publiceren]

Gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) en Federación de Comercio Electrónico y Marketing Directo (FECEMD) / Administración del Estado*, 24 november 2011
[Correcte tenuitvoerlegging van artikel 7, onder f), van de richtlijn gegevensbescherming – "gerechtvaardigd belang van anderen" – in het nationale recht]

Zaak C-518/07, *Europese Commissie / Bondsrepubliek Duitsland*, 9 maart 2010
[Onafhankelijkheid van een nationale toezichthoudende autoriteit]

Zaak C-524/06, *Huber / Bondsrepubliek Duitsland*, 16 december 2008
[Rechtmatigheid van het houden van gegevens over onderdanen van derde landen in een statistisch register]

Zaak C-543/09, *Deutsche Telekom AG / Bondsrepubliek Duitsland*, 5 mei 2011
[Noodzaak van hernieuwde toestemming]

Zaak C-553/07, *College van burgemeester en wethouders van Rotterdam / M.E.E. Rijkeboer*, 7 mei 2009
[Recht op toegang van de betrokkene]

Gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland en Seitlinger en anderen*, 8 april 2014
[Schending van het primaire EU-recht door de richtlijn gegevensbewaring]

Zaak C-614/10, *Europese Commissie / Republiek Oostenrijk*, 16 oktober 2012
[Onafhankelijkheid van een nationale toezichthoudende autoriteit]

Jurisprudentie met betrekking tot de verordening gegevensbescherming EU-instellingen

Zaak C-28/08 P, *Europese Commissie / The Bavarian Lager Co. Ltd*, 29 juni 2010
[Toegang tot documenten]

Zaak C-41/00 P, *Interporc Im- und Export GmbH / Commissie van de Europese Gemeenschappen*, 6 maart 2003
[Toegang tot documenten]

Zaak F-35/08, *Pachtitis / Commissie en EPSO*, 15 juni 2010
[Gebruik van persoonsgegevens in het kader van arbeid in EU-instellingen]

Zaak F-46/09, *V. / Parlement*, 5 juli 2011
[Gebruik van persoonsgegevens in het kader van arbeid in EU-instellingen]

Jurisprudentieregister

Rechtspraak van het Europees Hof van Justitie

Rechtspraak van het Europees Hof voor de rechten van de mens

Rechtspraak van nationale rechterlijke instanties

Bureau van de Europese Unie voor de grondrechten
Raad van Europa — Europees Hof voor de Rechten van de Mens

Handboek Europese gegevensbeschermingswetgeving

2014 — 227 blz — 14,8 × 21 cm

ISBN 978-92-871-9941-6 (Raad van Europa)
ISBN 978-92-9239-497-4 (FRA)
doi:10.2811/73787

Op het internet is veel informatie over het Bureau van de Europese Unie voor de grondrechten beschikbaar. Deze informatie kan worden geraadpleegd op het FRA's website via (fra.europa.eu).

Meer informatie over de Raad van Europa vindt u op internet via de server hub.coe.int.

Meer informatie over de rechtspraak van het Europees Hof voor de Rechten van de Mens is te vinden op de website van het Hof: echr.coe.int. Het via internet toegankelijke gegevensbestand HUDOC biedt toegang tot arresten en beslissingen in het Engels en/of Frans, vertalingen in andere talen, maandelijkse informatieve nota's over de rechtspraak, persberichten en andere informatie over de werkzaamheden van het Hof.

10.2811/73787
TK-01-13-772-NL-C

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

De snelle ontwikkeling van informatie- en communicatietechnologieën onderstreept de groeiende noodzaak van een robuuste bescherming van persoonsgegevens — een recht dat wordt gewaarborgd door instrumenten van zowel de Europese Unie (EU) als de Raad van Europa (RvE). De technologische vooruitgang verlegt de grenzen van bijvoorbeeld surveillance, het onderscheppen van communicatie en de opslag van gegevens, waardoor belangrijke uitdagingen met betrekking tot het recht op gegevensbescherming ontstaan. Dit handboek is bedoeld om beoefenaars van juridische beroepen die niet gespecialiseerd zijn in gegevensbescherming bekend te maken met dit rechtsdomein. In het handboek wordt een overzicht gegeven van de toepasselijke rechtskaders van de EU en de RvE. Daarbij passeert de belangrijkste jurisprudentie de revue, met samenvattingen van belangrijke arresten van het Europees Hof voor de Rechten van de Mens (EHRM) en het Hof van Justitie van de Europese Unie (HvJ-EU). Als er geen jurisprudentie bestaat, worden praktische voorbeelden met hypothetische scenario's gegeven. Het doel van dit handboek, in een notendop, is om bij te dragen tot een krachtige en resolute handhaving van het recht op gegevensbescherming.

BUREAU VAN DE EUROPESE UNIE VOOR DE GRONDRECHTEN
Schwarzenbergplatz 11 – 1040 Wenen – Oostenrijk
Tel +43 (1) 580 30-60 – Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

RAAD VAN EUROPA
EUROPEES HOF VOOR DE RECHTEN VAN DE MENS
67075 Straatsburg Cedex – Frankrijk
Tel +33 (0) 3 88 41 20 00 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Publicatiebureau

ISBN 978-92-871-9941-6 (Raad van Europa)
ISBN 978-92-9239-497-4 (FRA)