Bescherming persoonsgegevens in wet en praktijk

Mr. C.L. Koppenol

Noordhoff

1e druk

Bescherming persoonsgegevens in wet en praktijk

Mr. C.L. Koppenol

Eerste druk

Noordhoff

© Noordhoff Uitgevers bv

Ontwerp omslag: G2K (Groningen/Amsterdam)
Omslagillustratie: Audrey Shtecinjo/Stocksy

Eventuele op- en aanmerkingen over deze of andere uitgaven kunt u richten aan:
Noordhoff Uitgevers bv, Afdeling Hoger Onderwijs, Antwoordnummer 13,
9700 VB Groningen of via het contactformulier op www.mijnnoordhoff.nl.

De informatie in deze uitgave is uitsluitend bedoeld als algemene informatie. Aan deze informatie kunt u geen rechten of aansprakelijkheid van de auteur(s), redactie of uitgever ontlenen.

0 / 20

© 2020 Noordhoff Uitgevers bv, Groningen/Utrecht, Nederland.

Deze uitgave is beschermd op grond van het auteursrecht. Wanneer u (her)gebruik wilt maken van de informatie in deze uitgave, dient u vooraf schriftelijke toestemming te verkrijgen van Noordhoff Uitgevers bv. Meer informatie over collectieve regelingen voor het onderwijs is te vinden op www.onderwijsenauteursrecht.nl.

This publication is protected by copyright. Prior written permission of Noordhoff Uitgevers bv is required to (re)use the information in this publication.
ISBN (ebook) 978-90-01-89636-2
ISBN 978-90-01-89635-5
NUR 820

© Noordhoff Uitgevers bv

Woord vooraf

De geschiedenis van de mensheid laat zien dat sommige uitvindingen een enorme invloed hebben op het leven en werken van de mens. Denk daarbij aan de uitvinding van het wiel, de boekdrukkunst, de pil en de elektromotor. In die rij hoort ook het ontstaan en de ontwikkeling van de informatie- en communicatietechnologie zoals we die vandaag de dag kennen. Door die ontwikkeling is onze samenleving ingrijpend veranderd. Die verandering omvat meer dan het gebruik van een computer, de vermindering van de postbezorging of een veranderend koopgedrag van burgers. Door het wereldwijd verspreiden en delen van informatie gebeuren er dingen die voorheen ondenkbaar waren. Zonder het internet zou een beweging als die van de Arabische Lente in 2010 zich waarschijnlijk anders hebben ontwikkeld, zouden we het 'beroep' van influencer niet kennen, zou besluitvorming op basis van algoritmes minder aandacht hebben gekregen en zou – wie weet – Donald Trump geen president van de Verenigde Staten van Amerika zijn geworden. Maar zonder het internet zouden Google, Apple of Amazon niet bestaan en niet zo rijk en machtig zijn als zij nu zijn en zouden we informatie afkomstig van WikiLeaks of de Panama Papers niet hebben kunnen lezen. Zonder zoekmachines zou de inhoud van dit boek er anders uitzien.

De rode draad in dit boek is de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG) die daar een uitvloeisel van is. Dit betekent dat op basis van de AVG het (persoons)gegevensbeschermingsrecht wordt toegelicht. Daar wordt echter niet mee volstaan. Het recht over de bescherming van persoonsgegevens omvat meer dan alleen de AVG en de UAVG. Ook in andere regelgeving wordt aan dit onderwerp aandacht besteed. Denk daarbij bijvoorbeeld aan de overeenkomst inzake geneeskundige behandeling in het Burgerlijk Wetboek, de PNR-richtlijn die van toepassing is op luchtvaartmaatschppijen of de Wet op het financieel toezicht. In dit boek wordt ook aan deze en andere verwante regelgeving aandacht besteed. Situaties met betrekking tot de bescherming van persoonsgegevens waar men in de dagelijkse praktijk mee te maken heeft, worden behandeld. Bijvoorbeeld als het gaat om het gebruik van cookies, de positie van hostingbedrijven, de (ethische) hacker of betaaldiensten. Ook actuele jurisprudentie – waaronder die van het Europese Hof van Justitie – wordt toegelicht.

Het gegevensbeschermingsrecht is een vakgebied voor juristen en ICT'ers. Beide vakgebieden kenmerken zich door het gebruik van een eigen taal. Voor buitenstaanders is dit niet altijd te begrijpen of het geeft aanleiding voor verwarring. In dit boek is een lijst opgenomen met een toelichting op enige (min of meer) specialistische begrippen die in het persoonsgegevensbeschermingsrecht worden gebruikt of daarvoor van belang zijn.

© Noordhoff Uitgevers bv

In een boek over gegevensbeschermingsrecht mogen verwijzingen naar websites niet ontbreken. Een lijst met geraadpleegde en/of aanbevolen websites is toegevoegd. Ter verduidelijking zijn een aantal schema's opgenomen. De stroomdiagrammen zijn vrijwel allemaal ontleend aan publicaties van de ministeries van Justitie en Veiligheid en van Economische Zaken en Klimaat (www.rijksoverheid.nl).

Aanvullende informatie over dit boek is te vinden op
www.beschermingpersoonsgegevens.noordhoff.nl

In dit boek wordt een jong en dynamisch rechtsgebied toegelicht. Daarbij wordt aangesloten bij situaties uit de praktijk. Het doel van het boek is het inzicht en het begrip van de gebruiker in een soms lastige materie te vergroten. De in dit boek beschreven ontwikkelingen zullen niet stilstaan. Voor nu is dit wat het is: een juridische en geactualiseerde beschrijving van een van de belangrijkste ontwikkelingen van onze tijd.

Ik dank mijn dochter Merel voor het meelezen. Haar kritische opmerkingen en suggesties waren welkom en heb ik benut. Opmerkingen en/of suggesties van de gebruikers van dit boek zijn welkom.

Het onderwerp van dit boek heeft betrekking op een nieuwe tijd waarin papieren informatie wordt/is vervangen door digitale informatie. Ik draag dit boek daarom op aan mijn pasgeboren kleinzoon Olivier, in de verwachting dat hij (nog) meer dan zijn opa die 'nieuwe tijd' zal gaan beleven.

Rotterdam, maart 2020

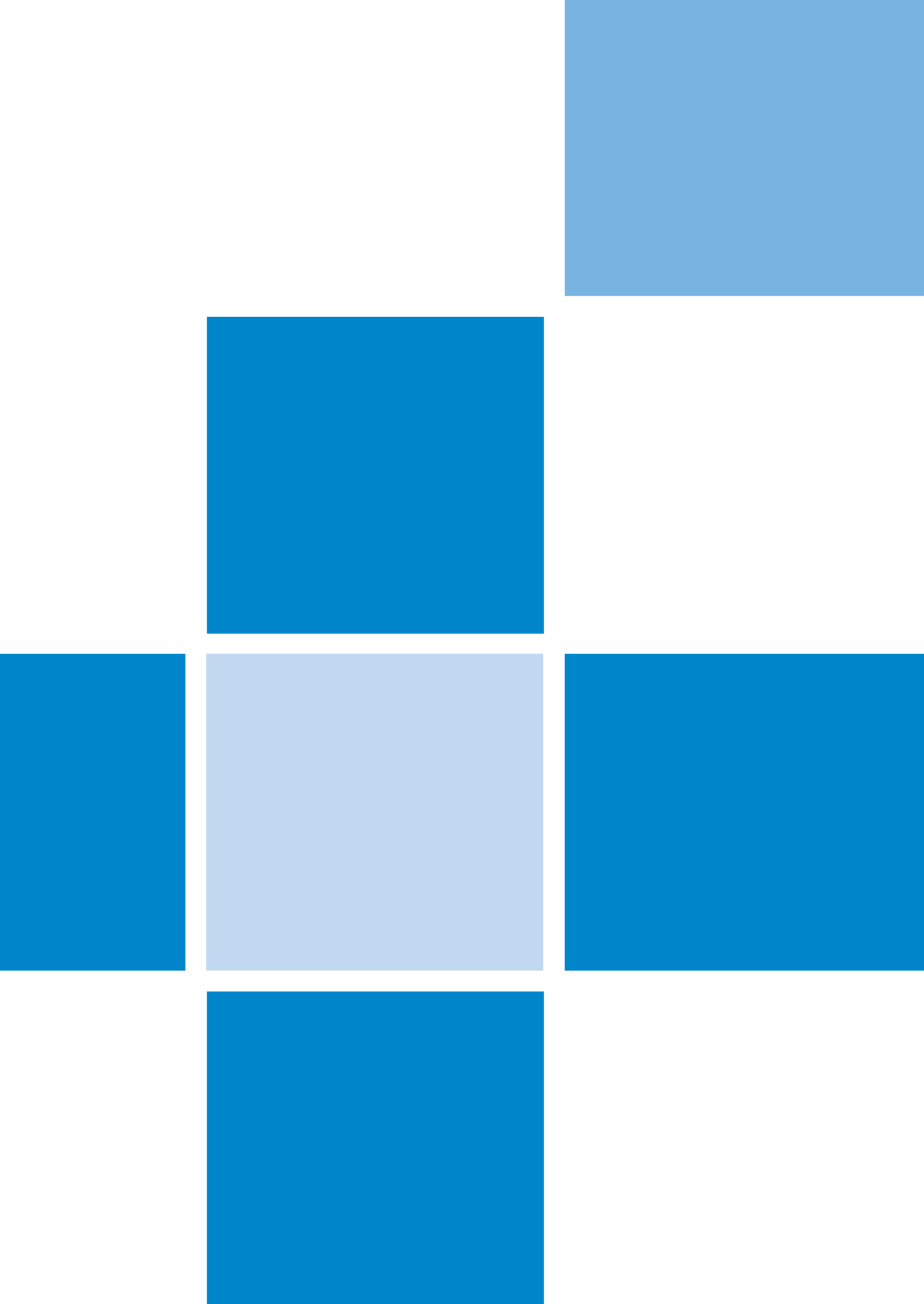
Kees Koppenol

© Noordhoff Uitgevers bv

Inhoud

© Noordhoff Uitgevers bv

© Noordhoff Uitgevers bv



1 Privacybescherming en bescherming persoonsgegevens

In dit hoofdstuk wordt ingegaan op het begrip persoonlijke levenssfeer. Welk belang hecht onze maatschappij aan de persoonlijke levenssfeer en hoe wordt dit zichtbaar in het recht (paragraaf 1.1)? Met behulp van praktijkvoorbeelden wordt geschetst welke motieven een rol kunnen spelen bij het verzamelen van gegevens over personen. In dat kader wordt onder andere aandacht besteed aan de volkstelling: een specifieke en oude vorm van verzamelen van persoonsgegevens (paragraaf 1.2). Vervolgens wordt toegelicht hoe de aandacht van de wetgever voor de bescherming van de persoonlijke levenssfeer van burgers zich in de loop van de tijd heeft ontwikkeld. Daarbij worden ontwikkelingen in internationaal en Europees verband meegenomen (paragraaf 1.3). Met behulp van persoonsgegevens kunnen personen worden geïdentificeerd. Op de vraag wat persoonsgegevens zijn, wordt ingegaan in paragraaf 1.4. Aandacht wordt besteed aan een aantal specifieke kwesties, zoals de status van IP-adressen en hoe om te gaan met de gegevens van overleden personen. In paragraaf 1.5 wordt – aan de hand van voorbeelden – beschreven hoe de bescherming van de persoonlijke levenssfeer in de praktijk kan verlopen. Hoe wordt omgegaan met een conflict tussen de bescherming van de persoonlijke levenssfeer en grondrechten en hoe staat het met de privacybescherming in arbeidsrelaties?

© Noordhoff Uitgevers bv

1.1 Privacy

Dit boek gaat over de bescherming van persoonsgegevens en heeft daarmee betrekking op de privacy van personen. Wat houdt het begrip privacy in en hoe wordt daar in het recht mee omgegaan?
In de Harvard Law Review werd in 1890 het recht op privacy voor het eerst door de Amerikaanse advocaten Samuel Warren en Louis Brandeis omschreven als 'the Right to be left alone'. In Nederland wordt pas later aandacht besteed aan het recht op privacy. Dat blijkt onder meer uit het taalgebruik. Het woord privacy wordt pas na 1950 in het Nederlands gebruikt. Vóór die tijd was het – anders dan nu – kennelijk geen algemeen gebruikt begrip. In woordenboeken wordt het woord privacy in de regel omschreven als 'persoonlijke vrijheid, het ongehinderd alleen, in eigen kring of met een partner ergens kunnen vertoeven; gelegenheid om zich af te zonderen, om storende invloeden van de buitenwereld te ontgaan'. In het recht wordt dit vaak samengevat als 'persoonlijke levenssfeer'.

Persoonlijke levenssfeer
Het begrip persoonlijke levenssfeer is een ruim begrip en omvat meer dan uitsluitend 'the Right to be left alone'. Zo kan er sprake zijn van aantasting van de persoonlijke levenssfeer die geen betrekking heeft op het gebruik van persoonsgegevens. Een onjuist gebruik van persoonsgegevens kan echter in bepaalde gevallen ook een aantasting zijn van 'the Right to be left alone'.

Aan het recht op privacy – en de bescherming daarvan – wordt in diverse wetten in meer of mindere mate aandacht besteed. Een paar voorbeelden.

- In artikel 10 van de Grondwet (Gw) is het recht op eerbiediging van de persoonlijke levenssfeer opgenomen, behoudens beperkingen die bij of krachtens wet worden gesteld.
- Op grond van artikel 285b van het Wetboek van Strafrecht (Sr) maakt degene die een ander belaagt zich schuldig aan een strafbaar feit. Onder belagen wordt verstaan het wederrechtelijk stelselmatig en opzettelijk inbreuk maken op iemand anders persoonlijke levenssfeer met het oogmerk de ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen.
- Artikel 7:456 BW bepaalt dat een hulpverlener een patiënt geen inzage in zijn dossier hoeft te geven, 'voor zover dit noodzakelijk is in het belang van de bescherming van de persoonlijke levenssfeer van een ander'.
- In het bestuursrecht kan de overheid op grond van artikel 10 van de Wet openbaarheid van bestuur (Wob) verzoeken om informatie weigeren als de verstrekking daarvan inbreuk maakt op de persoonlijke levenssfeer.
- Op grond van artikel 11.2 van de Telecommunicatiewet (Tw) dragen de aanbieders van een openbaar elektronisch communicatienetwerk of -dienst zorg voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van het netwerk of de dienst.

Het gegevensbeschermingsrecht is een onderdeel van het recht op privacy. Door technische ontwikkelingen en de toenemende digitalisering van gegevens neemt het belang van dit recht toe. Wat zijn persoonsgegevens, voor welk doel mogen zij – door wie – worden gebruikt en hoe moet ermee worden omgegaan? Wat te doen als persoonsgegevens op onjuiste wijze wor-

© Noordhoff Uitgevers bv

den gebruikt? Dit zijn in de kern de vragen waar het gegevensbeschermingsrecht zich mee bezighoudt. Daarbij wordt een onderscheid gemaakt in relationele en informationele privacy.

Relationele en informationele privacy
De relationele privacy is gericht op 'the Right to be left alone'. De informationele privacy heeft betrekking op het recht om zelf te beschikken over de eigen persoonsgegevens en te kunnen bepalen hoe, en in welke mate die gegevens aan anderen beschikbaar worden gesteld. Sinds 2018 is dit geregeld in de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG). In de praktijk wordt de AVG ook wel aangeduid met de letters GDPR. Dit staat voor General Data Protection Regulation.

Privacyparadox
De praktijk laat zien dat burgers die aangeven privacy belangrijk te vinden, zelf vaak slordig met hun persoonsgegevens omgaan en/of niet of nauwelijks weten wanneer, door wie en hoe hun persoonsgegevens worden verwerkt. Dit staat bekend als de privacyparadox. Het is de neiging om aan de ene kant de persoonlijke levenssfeer belangrijk te vinden, maar er aan de andere kant zelf niet of nauwelijks naar te handelen, bijvoorbeeld als het gaat om het regelmatig vervangen van wachtwoorden of toegangscodes. Ook hebben veel burgers er geen moeite mee om – in ruil voor een 'gratis' voorziening – persoonsgegevens te vertrekken, zonder precies te weten wat daarmee gebeurt. Er ontstaan pas problemen als wordt geconstateerd dat men op basis van de verstrekte persoonsgegevens wordt gediscrimineerd, onjuiste of niet gewenste informatie ontvangt of bepaalde informatie niet krijgt.

Geen absoluut recht
Het recht op privacy is niet absoluut. Er kunnen zich situaties voordoen waarin dat recht moet wijken voor een ander recht. Zo is het de overheid toegestaan om in het kader van terroristenbestrijding het recht op privacy te beperken. De veiligheid van burgers weegt in dat geval zwaarder dan het individuele recht op bescherming van de persoonlijke levenssfeer. Ook is het recht op privacy van een patiënt in een ziekenhuis in de regel beperkter dan thuis. Wil een arts een patiënt goed kunnen behandelen, dan is veelal niet te vermijden dat dit de relationele privacy van de patiënt beperkt. Het belang van de patiënt om weer gezond te worden, weegt in dat geval zwaarder dan het recht op privacy. Gaat het om de medische gegevens van een patiënt, dan is vaak het omgekeerde het geval. Patiënten willen dat met hun medische gegevens vertrouwelijk wordt omgegaan en (mogen) verwachten van het ziekenhuis dat met dit informationele aspect van de privacy zorgvuldig wordt omgegaan.

Privacy geen statisch begrip
De persoonlijke levenssfeer is geen statisch begrip. Wat wel of niet tot de persoonlijke levenssfeer behoort, wordt door tijd, plaats en cultuur bepaald. Zo was het vroeger gebruikelijk dat kinderen en ouders in dezelfde kamer sliepen, dat zuigelingen in het openbaar de borst kregen en dat pastoors ouders aanmoedigden een groot gezin te stichten. Allemaal situaties die vandaag de dag tot de persoonlijke levenssfeer worden gerekend. Aan de andere kant storten media zich tegenwoordig massaal op het privéleven van bekende personen en publiceren daar openlijk over. De soms zeer per-

© Noordhoff Uitgevers bv

soonlijke details die men daarover meldt, treft men in het verleden of in andere culturen niet vaak aan. Duidelijk is ook dat in een totalitair geleide staat – waarin de gehele maatschappij ondergeschikt wordt gemaakt aan de ideologie van de staat, zoals bijvoorbeeld in nazi-Duitsland en Noord-Korea – de persoonlijke levenssfeer van burgers er heel anders uitziet dan in een samenleving zoals Nederland die tegenwoordig kent.

1.2 Het verzamelen van gegevens over personen

Vaststaat dat in onze maatschappij veel – en steeds meer – informatie over personen wordt verzameld. De reden waarom men dit doet, verschilt. Besluit een overheid of een bedrijf informatie over personen te verzamelen, dan betekent dit niet dat er steeds sprake is van persoonsgegevens in de juridische betekenis. Als bijvoorbeeld een overheid wil weten hoeveel personen in een bepaald gebied wonen, dan zijn dat geen persoonsgegevens omdat het slechts om aantallen gaat en de informatie niet te herleiden is tot een individu.
Vaak is het verzamelen van informatie over personen noodzakelijk – of wordt door de verzamelaar noodzakelijk gevonden – om een bepaalde activiteit te kunnen uitvoeren. Hierna volgt een aantal voorbeelden.

Wettelijke verplichting
Op grond van de wet kan een organisatie verplicht worden gegevens over personen te verzamelen. Zo houden gemeenten op grond van de Wet basisregistratie personen (BRP) gegevens bij over hun ingezetenen. Wanneer iemand trouwt, een kind krijgt, overlijdt of verhuist, wordt dit vastgelegd. Ook informatie over bijvoorbeeld de ouders van de ingezetene, zijn of haar nationaliteit en gegevens over reisdocumenten zijn in de basisregistratie te vinden (artikel 2.8 en 2.24 BRP).

Op grond van artikel 7.52, 7.52a en 7.52b van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW) zijn instellingen voor hoger onderwijs verplicht persoonsgegevens over studenten te verzamelen en die informatie te delen met de Minister van Onderwijs, Cultuur en Wetenschap (OCW) en de Inspectie van het onderwijs.

Commerciële of organisatorische redenen
Ondernemingen verzamelen informatie over personen om (potentiële) klanten beter te bedienen. De informatie wordt niet altijd door de ondernemingen zelf verzameld, maar gekocht van organisaties die zich bezighouden met marktonderzoek. Die marktonderzoeken kunnen gebaseerd zijn op adresbestanden maar ook op andere informatie over personen, zoals bijvoorbeeld het surfgedrag op het internet. Dit laatste staat bekend als digital analytics. Ook de behoefte van overheden, bedrijven en organisaties om met behulp van algoritmes profielen van burgers op te stellen om daarmee kansen of (bedrijfs- of uitvoerings)risico's in kaart te brengen, leidt tot het verzamelen van informatie over personen.

Voor maatschappelijke organisaties is er vaak een praktische reden om gegevens over personen te verzamelen. De organisaties willen weten wie bij hun activiteiten betrokken zijn of kunnen worden. Een voorbeeld daarvan is het Koningin Wilhelmina Fonds voor de Nederlandse kankerbestrijding. Uit

© Noordhoff Uitgevers bv

de website van die organisatie (www.kwf.nl) blijkt dat men graag in contact treedt met vrijwilligers en/of donateurs.

Wetenschappelijk onderzoek
Bij wetenschappelijk onderzoek worden veel gegevens over personen verzameld. Dat kunnen medische gegevens zijn maar ook gegevens over bijvoorbeeld gedrag of erfelijk materiaal. Daarbij kan het gaan om oude of nieuwe gegevens, van volwassenen, kinderen of overledenen en/of informatie die niet op schrift staat maar op beeld- of geluidsdragers is vastgelegd. Van dit laatste kan sprake zijn als in het kader van het onderzoek van belang is het gedrag van personen vast te leggen.

Statistiek
Veel gegevens over personen worden om statistische redenen verzameld. Dat gebeurt zowel door de overheid als door bedrijven en andere organisaties. De statistische gegevens worden in de regel gebruikt als vergelijkingsmateriaal, voor de ontwikkeling van beleid of het opstellen van plannen. Zo willen basisscholen graag weten hoe oud-leerlingen presteren in het voortgezet onderwijs. Die informatie wordt vervolgens gebruikt bij de werving van nieuwe leerlingen. Universiteiten verzamelen soms informatie over het carrièreverloop van hun gediplomeerden. Blijkt de oud-student een glanzende carrière te hebben, dan kan die informatie worden gebruikt bij de werving van nieuwe studenten. Ook de behoefte van veel organisaties om te weten of men tevreden is met de geleverde producten of verleende diensten, kan leiden tot het verzamelen van persoonsgegevens.

Archief
Soms worden gegevens die over personen zijn verzameld, gearchiveerd. Dit gebeurt in de regel in het algemeen belang. De gearchiveerde informatie kan in dat geval gebruikt worden voor historisch, wetenschappelijk of statistisch onderzoek. Bekende voorbeelden hiervan zijn het archief van de Verenigde Oost-Indische Compagnie (VOC) en de Surinaamse slavenregisters (www.nationaalarchief.nl).

Beveiliging
Uit het oogpunt van beveiliging kan het van belang zijn gegevens over personen te verzamelen. Dat is bijvoorbeeld het geval als geheime diensten ‘verdachte’ personen observeren of als bedrijven ‘zwarte lijsten’ aanleggen met namen van oud-klanten of andere personen waar men geen zaken mee wil doen. Het argument van beveiliging, meer specifiek het voorkomen van terroristische aanslagen, wordt ook gebruikt door vliegtuigmaatschappijen die persoonsgegevens van passagiers verzamelen en doorgeven aan de autoriteiten.

Volkstelling
De hiervoor gegeven voorbeelden hebben betrekking op het heden. Uit archieven en archeologische bronnen blijkt dat het verzamelen van informatie over personen van alle tijden is. Een bekend voorbeeld uit de oudheid is de volkstelling. Zo werden aan het begin van onze jaartelling in het Romeinse Rijk al volkstellingen gehouden. In Nederland zijn in de periode 1795-1971 volkstellingen gehouden. Doel daarvan was de bevolkingsgrootte en een aantal andere kenmerken zoals leeftijd, geslacht, burgerlijke staat en godsdienst vast te stellen. De uitkomsten van de volkstelling wer-

© Noordhoff Uitgevers bv

den onder meer gebruikt om te kunnen zien hoeveel belasting er kon worden geheven.
Om een volkstelling te kunnen uitvoeren, werd gebruikgemaakt van vragenlijsten en werden door enquêteurs tellingen verricht. Deze manier van werken vergt veel mankracht en is daarom kostbaar en tijdrovend. Na 1971 wordt er in Nederland niet meer op deze traditionele manier aan een volkstelling gewerkt. In plaats daarvan worden de gegevens gebaseerd op registers. Dit gebeurt door het Centraal Bureau voor de Statistiek (www.cbs.nl). De eerste keer dat dit gebeurde was in 2011. Bij deze 'virtuele volkstelling' worden bestanden automatisch gekoppeld aan de gemeentelijke basisadministratie op basis van het burgerservicenummer (BSN). De uitkomsten van volkstellingen zijn van belang voor sociaalwetenschappelijk onderzoek en worden ook gebruikt om Nederland te vergelijken met andere landen.

Digitalisering en globalisering
Het verzamelen van informatie over personen is dus van alle tijden. De mate waarin dit gebeurt, verschilt van tijd tot tijd. Anders dan in het verleden, wordt informatie nu vaak niet meer (uitsluitend) op een bepaalde plaats in een papieren archief bewaard. Het gebruik van de computer en de mogelijkheden die digitalisering van informatie ons bieden, maken dat we over het verzamelen van persoonsinformatie anders gaan denken. Veel informatie wordt tegenwoordig bewaard in de 'cloud' en gaat via het 'World Wide Web' (www) de wereld over. Hierdoor en door incidenten die laten zien dat met verkregen (persoons)informatie niet altijd goed wordt omgegaan, klinkt de roep om bescherming van de persoonlijke levenssfeer luider. Burgers willen weten wie welke informatie over hen verzamelt en hoe daarmee wordt omgegaan. Zij willen ook de mogelijkheid hebben vergeten te worden en onjuiste informatie te corrigeren. Ook overheden zijn zich ervan bewust dat digitalisering de maatschappij ingrijpend verandert en nieuwe wetgeving noodzakelijk maakt. De invoering van de AVG is daar een voorbeeld van.

Het Streisandeffect
De behoefte van burgers om hun persoonlijke levenssfeer te beschermen, kan ook een tegengesteld effect hebben. Een effect dat in ons digitale tijdperk wordt versterkt door de snelle en omvangrijke verspreiding van veel informatie. Dit staat bekend als het Streisandeffect.

Streisandeffect

In 2003 spande de Amerikaanse zangeres en actrice Barbara Streisand een rechtszaak aan om luchtfoto's van haar huis in Malibu van een website te verwijderen. Zij meende dat het publiceren van de foto's van haar huis haar privacy schond. De foto's waren gemaakt in het kader van een project over erosie van de kust en onderdeel van een serie foto's die van de kust van Californië waren gemaakt. Voor de rechtszaak begon, had bijna niemand de foto's van het huis van Streisand bekeken. Nadat de rechtszaak – die door Streisand werd verloren – in het nieuws kwam, werden de foto's door 400.000 mensen bekeken.

© Noordhoff Uitgevers bv

Wat Streisand overkwam, gebeurde in 2019 in Nederland bij een oud-hoogleraar van de Universiteit van Amsterdam. Deze probeerde via een kort geding te voorkomen dat zijn naam zou worden vermeld in een krantenartikel over hem in de *Nieuwe Rotterdamsche Courant* (*NRC*) dat ging over grensoverschrijdend gedrag. In ECLI:NL:RBAMS:2019:3451 (*Hoogleraar vs. NRC*) kreeg de oud-hoogleraar gedeeltelijk gelijk van de voorzieningenrechter. Het effect van het nieuws over de uitspraak – waarin *NRC* werd verboden de volledige naam te publiceren – was echter dat de naam van de oud-hoogleraar binnen de kortste keren was te vinden op Twitter en op zoekmachines als Google. De naam werd hierdoor algemeen bekend. Door de uitkomst van het kort geding gebeurde wat de hoogleraar met het kort geding had geprobeerd te voorkomen. Tegen deze uitspraak heeft *NRC* hoger beroep ingesteld. Hierop wordt ingegaan in subparagraaf 4.4.4.

1.3 Aandacht voor de bescherming van de privacy in het recht

Dat het verzamelen van informatie over personen een inbreuk op de persoonlijke levenssfeer kan zijn, is iets waar in het verleden niet of nauwelijks bij werd stilgestaan. Maatschappelijke aandacht voor de bescherming van de persoonlijke levenssfeer is in Nederland pas in de jaren zestig van de vorige eeuw ontstaan. Aanleiding daarvoor was onder meer de volkstelling van 1971. Bij die volkstelling werden meer gegevens verzameld dan tot dan gebruikelijk was. Dit riep maatschappelijke weerstand op en was voor sommigen aanleiding te weigeren de gevraagde gegevens te verstrekken. Het toenemende gebruik van de computer versterkte dit sentiment. In discussies die over de volkstelling werden gevoerd, werd onder meer gewezen op de Jodenvervolging in Nederland. De registratie van de bevolking zou vóór het uitbreken van de Tweede Wereldoorlog zo goed op orde zijn geweest dat het de Duitse bezetter niet veel moeite kostte de adressen en geloofsopvattingen van individuele Nederlanders te achterhalen.

1.3.1 De Grondwet, Wpr en Wbp

De aandacht van de wetgever voor de bescherming van de persoonlijke levenssfeer van burgers was aanvankelijk fragmentarisch en zag vooral op de verhouding tussen de overheid en de burger. Zo werd in 1815 in de Grondwet het verbod opgenomen om zonder toestemming de woning van een ander te betreden. Dit zogenoemde huisrecht gold met name (ook) voor de overheid. Het zonder toestemming betreden van een woning werd alleen toegestaan als er een wettelijke grondslag voor was, zoals bij verdenking van strafbare feiten of in het belang van de nationale veiligheid. In 1848 volgde de opname van het briefgeheim in de Grondwet. Dit gebeurde omdat de overheid destijds – als enig uitvoerder van de Postwet – de post bezorgde. Met het opnemen van het briefgeheim werd beoogd te voorkomen dat nieuwsgierige ambtenaren ongestraft post van burgers zouden kunnen inzien. In 1983 werd de Grondwet aangevuld met het recht op bescherming van lichamelijke integriteit. Kenmerkend voor deze grondwetsartikelen is dat zij betrekking hebben op slechts één bepaald onderdeel van de persoonlijke levenssfeer en op de verhouding tussen overheid en burger. Naast deze specifieke grondwetsartikelen werd in 1983 ook een

© Noordhoff Uitgevers bv

algemeen recht op de bescherming van de persoonlijke levenssfeer opgenomen. Dit is artikel 10 van de Grondwet. De tekst hiervan luidt:

> ‘1 Ieder heeft, behoudens bij of krachtens wet te stellen beperkingen, recht op bescherming van zijn persoonlijke levenssfeer.
> 2 De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
> 3 De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.’

Het eerste lid van dit artikel is in feite een opdracht aan de overheid om de persoonlijke levenssfeer van burgers te eerbiedigen en te beschermen. De hiervoor beschreven specifieke grondwetsartikelen over de persoonlijke levenssfeer zijn daar uitwerkingen van. Op grond van het tweede en derde lid is de wetgever verplicht om dit grondrecht verder in wetten uit te werken. De totstandkoming van die nadere uitwerking verliep traag. De Wet persoonsregistraties (Wpr) kende een lange voorgeschiedenis en trad pas op 1 juli 1989 in werking. Van Europese invloed op de Wpr was nagenoeg geen sprake. Met de invoering in 2001 van de Wet bescherming persoonsgegevens (Wbp) veranderde dit.

Registratieplicht
Op grond van de Wpr werden private organisaties verplicht om een persoonsregistratie aan te melden bij de toezichthouder, de Registratiekamer. Publieke organisaties moesten een privacyreglement vaststellen en de toezichthouder daarover informeren. De Registratiekamer diende de naleving van de Wpr te controleren. In dat kader konden onderzoeken worden ingesteld en aanbevelingen gedaan. De Registratiekamer kon echter geen bestuursdwang toepassen of boetes opleggen.

Vervanging Wpr door Wbp
Als gevolg van de vervanging van de Wpr door de Wbp werden de regels gewijzigd. Er werd gekozen voor een andere benadering. In de Wbp werd niet meer – zoals in de Wpr – als uitgangspunt genomen het registeren van persoonsgegevens ongeacht de relevantie voor de persoonlijke levenssfeer. In de Wbp werd als uitgangspunt genomen het beschermen tegen onterechte inbreuken op de persoonlijke levenssfeer. Als gevolg van deze andere benadering hoefden er minder gegevens te worden gemeld bij het College bescherming persoonsgegevens (dit was onder de Wpr de Registratiekamer en is nu de Autoriteit Persoonsgegevens). Ook het ter inzage leggen van de melding werd afgeschaft. Naast deze versoepeling werden er ook regels aangescherpt. De persoonsgegevens mochten alleen worden verwerkt als die gebaseerd waren op één of meer van de zes in artikel 8 Wbp genoemde gronden en niet meer – zoals onder de Wpr – als er sprake was van een ‘rechtmatig doel’ en een ‘redelijk belang’. Ook diende de betrokkene eerder dan onder de Wpr over een gegevensverwerking te worden geïnformeerd. Nieuw was ook de invoering van het recht op verzet, de mogelijkheid een functionaris gegevensbescherming te benoemen, de bestuursdwang en de (bescheiden) boetes die konden worden opgelegd als de wet niet werd nageleefd. Met de invoering van de Wbp werd voldaan aan de Europese richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije

© Noordhoff Uitgevers bv

verkeer van die gegevens – afgekort Privacyrichtlijn 1995 – die in 1995 door de Europese Gemeenschap (afgekort: EG. Dit is nu de Europese Unie: afgekort EU) werd vastgesteld (Richtlijn 95/46/EG).

Om te voorkomen dat in de Wbp geformuleerde begrippen door nieuwe technische ontwikkelingen snel zouden verouderen, is geprobeerd de wet technologieneutraal te formuleren. Zo werd in de Wbp het in de Wpr gebruikte begrip 'persoonsregistratie' vervangen door het meer technologieonafhankelijke begrip 'gegevensverwerking'. Dat deze herformulering zinvol is, blijkt uit het volgende voorbeeld.

Cloud computing
Cloud computing is een nieuwe technische ontwikkeling waar steeds vaker gebruik van wordt gemaakt. Het is het via een netwerk beschikbaar stellen van hardware, software en/of gegevens. De gebruiker van de computer is geen eigenaar van de gebruikte hard- en software en weet ook niet door wie die wordt gebruikt. Het voordeel van werken in de 'cloud' is dat men niet verantwoordelijk is voor het onderhoud (kostenbesparend) en de gebruiker de (online) opgeslagen informatie – zoals bijvoorbeeld e-mailberichten – ook vanaf andere computers kan inzien. Het voorgaande maakt duidelijk dat het begrip 'persoonsregistratie' de praktijk van cloud computing niet goed dekt. Het begrip 'gegevensverwerking' past beter.

1.3.2 Van Privacyrichtlijn 1995 naar AVG en UAVG

EU-richtlijnen zijn gericht aan de lidstaten. Dit betekent dat een richtlijn voor een EU-lidstaat op grond van artikel 288 van het Verdrag betreffende de werking van de Europese Unie (VWEU) verbindend is ten aanzien van het te bereiken resultaat, maar dat het aan de nationale instanties van een lidstaat wordt overgelaten vorm en middelen te kiezen. Burgers kunnen in beginsel niet rechtstreeks een beroep op een richtlijn doen. Met de invoering van de Privacyrichtlijn 1995 kon (daarom) niet worden voorkomen dat gegevens in de EU op gefragmenteerde wijze werden beschermd. De lidstaten boden op het vlak van verwerking van persoonsgegevens uiteenlopende niveaus van bescherming. Dit werd als een belemmering ervaren voor het vrije verkeer van persoonsgegevens binnen de EU en zou tevens belemmerend zijn voor de (ontwikkeling van de) economische activiteiten. Tegen die achtergrond ontstond er behoefte aan meer uniformering van de regels en aan meer rechtsgelijkheid voor de burger. Op 25 mei 2018 werd de Privacyrichtlijn 1995 vervangen door de AVG. Naast het beschermen van persoonsgegevens heeft de verordening tot doel om binnen de EU het vrije verkeer van persoonsgegevens te bevorderen. Anders dan een richtlijn heeft een EU-verordening een algemene strekking. Zij is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in alle lidstaten (artikel 288 VWEU). Een verordening heeft dezelfde rechtskracht als de nationale wetgeving.

Indeling AVG
De AVG kent de volgende indeling:
Hoofdstuk I Algemene bepalingen
Hoofdstuk II Beginselen voor de verwerking van persoonsgegevens
Hoofdstuk III Rechten van betrokkenen
Hoofdstuk IV Verwerkingsverantwoordelijke en verwerker

© Noordhoff Uitgevers bv

Hoofdstuk V Doorgiften van persoonsgegevens aan derde landen of internationale organisaties
Hoofdstuk VI Onafhankelijke toezichthoudende autoriteiten
Hoofdstuk VII Samenwerking en coherentie
Hoofdstuk VIII Beroep, aansprakelijkheid en sancties
Hoofdstuk IX Bepalingen in verband met specifieke situaties op het gebied van gegevensverwerking
Hoofdstuk X Gedelegeerde handelingen en uitvoeringshandelingen
Hoofdstuk XI Slotbepalingen.

Verschillen AVG en Privacyrichtlijn 1995

De AVG verschilt niet alleen wat betreft wetgevingstechniek van de Privacyrichtlijn 1995: de AVG is omvangrijker en er zijn ook inhoudelijke verschillen. De AVG telt 99 artikelen en daarnaast 173 overwegingen. In de overwegingen wordt uitgelegd wat de bedoeling van de AVG is en welke keuzes daarbij zijn gemaakt. De Privacyrichtlijn 1995 telde 34 artikelen en 72 overwegingen. De AVG bouwt verder op wat met de Privacyrichtlijn 1995 begon. De inhoudelijke verschillen die er zijn, zijn enerzijds ontstaan omdat in de AVG jurisprudentie van het Hof van Justitie van de EU (HvJ EU) is verwerkt, en anderzijds omdat andere (beleids)keuzes zijn gemaakt. Belangrijke verschillen zijn:

- Organisaties moeten als het gaat om het beschermen van persoonsgegevens meer zelf regelen dan voorheen en worden daar vervolgens ook verantwoordelijk voor gehouden.
- Houdt men zich niet aan de AVG, dan loopt men het risico met veel hogere boetes geconfronteerd te worden dan de boetes die onder de Privacyrichtlijn 1995 mogelijk waren.
- Organisaties worden verplicht om voor bepaalde verwerkingen een Data Protection Impact Assessment (DPIA) uit te voeren. Daarin moet inzichtelijk gemaakt worden waarom een bepaalde verwerking wordt uitgevoerd en wat de risico's daarvan zijn met betrekking tot de gegevensbescherming.
- Persoonsgegevens mogen – als hoofdregel – in beginsel alleen verwerkt worden als betrokkene daar expliciet toestemming voor heeft gegeven. Uitzonderingen hierop zijn mogelijk.
- Veel organisaties worden verplicht een functionaris gegevensbescherming (FG) aan te stellen. In de Wbp en de Privacyrichtlijn 1995 bestond de mogelijkheid dit te doen, maar was er geen sprake van een verplichting.
- De rechten van burgers met betrekking tot hun persoonsgegevens zijn op diverse terreinen versterkt. Zo is onder meer toegevoegd het door het HvJ EU erkende recht om vergeten te worden.

European Data Protection Board (EDPB)

Behalve meer uniformering van regels en minder rechtsongelijkheid, heeft ook de toegenomen digitalisering bijgedragen aan de vervanging van de Privacyrichtlijn 1995 door de AVG. Overweging 6 AVG licht dit als volgt toe.

> 'Door de snelle technologische ontwikkelingen en globalisering zijn nieuwe uitdagingen voor de bescherming van persoonsgegevens ontstaan. De mate waarin persoonsgegevens worden verzameld en gedeeld, is significant gestegen. Dankzij de technologie kunnen bedrijven en overheid bij het uitvoeren van hun activiteiten meer dan ooit tevoren gebruikmaken van persoons-

© Noordhoff Uitgevers bv

gegevens. Natuurlijke personen maken hun persoonsgegevens steeds vaker wereldwijd bekend. Technologie heeft zowel de economie als het maatschappelijk leven ingrijpend veranderd en moet het vrije verkeer van persoonsgegevens binnen de Unie en de doorgifte aan derde landen en internationale organisaties verder vergemakkelijken en daarbij een hoge mate van bescherming van persoonsgegevens garanderen.'

In de AVG is – net als in de Privacyrichtlijn 1995 – gekozen voor een technologieneutrale benadering om omzeiling van de verordening te voorkomen. De bescherming van persoonsgegevens van natuurlijke personen mag niet afhankelijk zijn van de gebruikte technologieën (overweging 15 AVG). Het gevolg van deze benadering is dat de in de AVG opgenomen normen vaak in algemene termen zijn geformuleerd. Een voorbeeld daarvan geeft artikel 5 AVG. Dat artikel gaat over de beginselen voor de verwerking van persoonsgegevens. Daarin worden woorden gebruikt als 'behoorlijk' (onder a), 'gerechtvaardigde doeleinden' (onder b), 'toereikend' en 'passend' (onder e en f). Wat concreet met die woorden wordt bedoeld, wordt niet nader toegelicht. Dit betekent dat de eis dat persoonsgegevens 'behoorlijk' moeten zijn verwerkt en dat een 'passende beveiliging' moet zijn gewaarborgd, soms nadere uitleg behoeft. Niet ondenkbaar is ook dat men bijvoorbeeld in Finland een 'behoorlijke' verwerking van persoonsgegevens anders interpreteert dan in Spanje en dat een 'passende beveiliging' er in Letland anders uitziet dan in Roemenië.
Om ervoor te zorgen dat de AVG in de hele EU consequent wordt toegepast, is uitwisseling van informatie en onderlinge afstemming tussen de lidstaten van groot belang. In de AVG wordt hier rekening mee gehouden. Afdeling 3 van hoofdstuk 7 AVG geeft regels die betrekking hebben op het Europees Comité voor gegevensbescherming (artikel 68-76 AVG). Dit is de European Data Protection Board, afgekort EDPB. De kerntaak van de EDPB is te zorgen voor een consequente toepassing van de AVG. Dit gebeurt onder meer door het uitvaardigen van richtsnoeren, aanbevelingen en beste praktijken (artikel 70 AVG). De EDPB wordt gezien als de opvolger van de 'Artikel 29-groep' (vaak afgekort met: WP29) die functioneerde ten tijde van de Privacyrichtlijn 1995. De positie, de rol en de taken van de EDPB – en haar voorganger WP29 – worden in paragraaf 7.4 toegelicht.

Beperkte eigen invulling AVG door lidstaten
In de AVG wordt aan de EU-lidstaten ruimte geboden nationale regelgeving te maken op het terrein van het gegevensbeschermingsrecht, bijvoorbeeld als het gaat om arbeidsrecht en sociaal beschermingsrecht (overweging 52 AVG), zorg en volksgezondheid (overweging 52 en 53 AVG) of de informatievrijheid (artikel 85 AVG). De 'vrije beleidsruimte' is echter beperkt en mag niet in strijd zijn met de AVG. Van de 99 artikelen die de AVG telt, biedt ongeveer een vijfde daarvan lidstaten de mogelijkheid eigen (beleids)regels op te stellen.

Beleidsneutrale implementatie AVG in Nederland
Door Nederland is daar in beperkte mate gebruik van gemaakt. Er is gekozen voor een beleidsneutrale implementatie van de AVG. Dit betekent dat – daar waar de AVG dit toelaat – zo veel als mogelijk de bestaande regelgeving – die op de Privacyrichtlijn 1995 was gebaseerd – blijft bestaan. Dit is geregeld in de Uitvoeringswet AVG (UAVG). Deze wet vervangt de Wbp en is in 2018 in werking getreden.

© Noordhoff Uitgevers bv

Ter illustratie drie voorbeelden:

- Op grond van artikel 8 lid 1 AVG moet degene die de ouderlijke verantwoordelijkheid heeft voor een kind jonger dan 16 jaar toestemming geven voor bepaalde verwerkingen van de persoonsgegevens van het kind. Lidstaten kunnen er echter voor kiezen deze leeftijd te verlagen naar 13 jaar. Van deze afwijkingsmogelijkheid is door Nederland geen gebruik gemaakt. In Nederland werd en wordt de leeftijd van jonger dan 16 jaar gehanteerd.
- Op grond van artikel 9 lid 4 AVG kunnen de lidstaten bijkomende voorwaarden – waaronder beperkingen – handhaven of invoeren als het gaat om de verwerking van onder meer genetische gegevens. Van deze afwijkingsmogelijkheid heeft Nederland gebruikgemaakt in artikel 28 UAVG.
- Op grond van artikel 51 AVG bepalen de lidstaten zelf hoeveel onafhankelijke overheidsinstanties verantwoordelijk zijn voor het toezicht op de toepassing van de AVG. In Nederland is in artikel 6 UAVG gekozen voor één toezichthouder en dat is de Autoriteit Persoonsgegevens (AP) (www.autoriteitpersoonsgegevens.nl). Dit was voorheen het College bescherming persoonsgegevens (CBP).

Bij de behandeling van de UAVG stelde de Tweede Kamer vast dat met de inwerkingtreding van de AVG en de UAVG de discussie rond het gegevensbeschermingsrecht niet was afgerond en dat er op dit gebied nog vragen en wensen waren. Dit standpunt had tot resultaat dat in artikel 50 UAVG is bepaald dat de wet periodiek zal worden geëvalueerd. Dit biedt onder meer de mogelijkheid om te reageren op de effecten van de beleidsneutrale invoering van de UAVG en de wet zo nodig aan te passen.

Aanpassingswet AVG

Naast de intrekking van de Wbp en de invoering van UAVG dienden ook bepalingen in andere wetten aan de AVG te worden aangepast. Vaak ging het daarbij om bepalingen waarin werd verwezen naar de Wbp. In de aanpassing van de andere wetten is voorzien in de Aanpassingswet Algemene verordening gegevensbescherming (AAVG). De AAVG is ruim een maand na de inwerkingtreding van de UAVG op 11 juli 2018 gepubliceerd in het *Staatsblad* (*Stb*. 2018, 247). De wet treedt op een bij koninklijk besluit te bepalen tijdstip in werking. Dit tijdstip kan voor verschillende artikelen of onderdelen daarvan verschillend worden vastgesteld en kan terugwerkende kracht hebben.

Verdrag van Lissabon

De Privacyrichtlijn 1995 was gebaseerd op artikel 95 van het EG-Verdrag. In 2007 trad het Verdrag van Lissabon in werking. Dit verdrag heeft onder meer tot doel het democratisch gehalte en de transparantie in de EU te vergroten. Om dit te bereiken werden bestaande besluitvormingsprocedures aangepast. In het Verdrag van Lissabon werd tevens het EG-Verdrag vervangen door het Verdrag betreffende de werking van de Europese Unie (VWEU). De AVG is gebaseerd op artikel 16 VWEU. Dit artikel luidt:

> ‘1 Een ieder heeft recht op bescherming van zijn persoonsgegevens.
> 2 Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de

© Noordhoff Uitgevers bv

lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrije verkeer van die gegevens. Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten. De op basis van dit artikel vastgestelde voorschriften doen geen afbreuk aan de in artikel 39 van het Verdrag betreffende de Europese Unie bedoelde specifieke voorschriften.'

EU-Grondrechtenhandvest

Behalve in artikel 16 VWEU is de bescherming van persoonsgegevens ook vastgelegd in het EU-Grondrechtenhandvest. Dit document werd in 2000 opgesteld en kreeg met de inwerkingtreding van het Verdrag van Lissabon dezelfde rechtskracht als het EU-Verdrag en het VWEU. In uitspraken van het HvJ EU wordt regelmatig verwezen naar het EU-Grondrechtenhandvest. Voor het gegevensbeschermingsrecht zijn met name artikel 7 en 8 van het EU-Grondrechtenhandvest relevant. Deze luiden als volgt:

Artikel 7
'Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie

Artikel 8
1 Eenieder heeft recht op bescherming van zijn persoonsgegevens.
2 Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan.
3 Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd.'

Positie AVG binnen het EU-recht

Voor de EU zijn het EU-Verdrag, het VWEU en het EU-Grondrechtenhandvest de basisverdragen op basis waarvan wordt gehandeld. Dit betekent dat niet alleen bij het opstellen van richtlijnen of verordeningen, maar ook bij het sluiten van verdragen met landen buiten de EU steeds gekeken wordt hoe dit zich verhoudt tot de basisverdragen. Tegen die achtergrond is de AVG in het EU-recht een secundaire regeling. Dit standpunt werd onder meer door het HvJ EU ingenomen in ECLI:EU:C:2015:650 (*Schrems*). In die zaak concludeerde het Hof dat de bevoegdheid van de Europese Commissie (EC) om op grond van artikel 25 lid van de Privacyrichtlijn 1995 (nu: artikel 45 AVG) te beoordelen of een land buiten de EU een passend beschermingsniveau heeft voor de doorgifte van persoonsgegevens, de uitvoering is van een uitdrukkelijke verplichting van artikel 8 lid 1 EU-Grondrechtenhandvest. Voor een uitgebreidere toelichting op deze uitspraak wordt verwezen naar subparagraaf 3.3.2.

1.3.3 E-Privacyrichtlijn

De E-Privacyrichtlijn uit 2002 bevat regels op het gebied van telecommunicatie. De richtlijn vormde een specificatie van de Privacyrichtlijn 1995 en vulde die aan. In de richtlijn staan regels over de beveiliging van netwerken en het vertrouwelijke karakter van communicatie. In Nederland is de E-Privacyrichtlijn verwerkt in de Telecommunicatiewet. In die wet wordt onder meer het gebruik van cookies geregeld (artikel 11.7a Tw).

© Noordhoff Uitgevers bv

Cookies
In het gegevensbeschermingsrecht spelen cookies een belangrijke rol. Het zijn kleine tekst- of gegevensbestanden die bij een bezoek aan een website op de apparatuur van de bezoeker worden opgeslagen. Hierdoor kan worden bijgehouden wat de bezoeker op de website doet. Omdat deze informatie wordt opgeslagen, kan er bij een volgend bezoek aan de website gebruik van worden gemaakt. Onder 'apparatuur' wordt in dit verband verstaan: computers, tablets en mobiele telefoons. Bij al deze apparaten – in de Tw worden ze randapparaten genoemd – gaat het om het via een elektronisch communicatienetwerk opslaan van of toegang verkrijgen tot informatie in de apparatuur van de gebruiker.
Er zijn verschillende soorten cookies. Vaak wordt daarbij de volgende indeling in categorieën aangehouden:

- Functionele cookies zijn bestanden die noodzakelijk zijn voor het gebruik van de website. Zo worden bijvoorbeeld cookies gebruikt voor de webwinkel om bij te houden wat in de winkelwagen is geplaatst of de gebruikersvoorkeur voor een bepaalde taal.
- Analytische cookies worden onder meer gebruikt om bezoekersstatistieken van de website bij te houden. Hierdoor wordt beter inzicht verkregen in het functioneren van de website.
- Tracking cookies houden individueel surfgedrag van de bezoekers van de website bij en worden onder meer gebruikt om profielen op te stellen voor op de persoon van de bezoeker gerichte advertenties.

Sommige websites staan toe dat ook andere websites cookies plaatsen op de apparatuur van de gebruiker. Deze cookies van derden zijn in de regel tracking cookies. In subparagraaf 3.6.1 wordt verder ingegaan op het gebruik van cookies en het al dan niet geven van toestemming voor het gebruik daarvan.

De EU heeft het voornemen de E-Privacyrichtlijn te vervangen door de E-Privacyverordening. Daarmee wordt beter aangesloten bij de AVG. Het oorspronkelijke plan om de E-Privacyverordening samen met de AVG in te voeren, bleek niet haalbaar. Het is niet bekend wanneer de E-Privacyverordening zal worden ingevoerd.

1.3.4 Richtlijn gegevensbescherming politie en justitie (Richtlijn 2016/680)

Naast de AVG werd in mei 2018 ook de Richtlijn gegevensbescherming politie en justitie (Richtlijn 2016/680) van kracht. Deze richtlijn is van toepassing op persoonsgegevens die worden verwerkt 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 het vrije verkeer van die gegevens. De Richtlijn is een zelfstandige regeling en geen aanvulling op de AVG. Dit blijkt uit artikel 2 lid 2 onderdeel d AVG.
Richtlijn 2016/680 komt in de plaats van het Kaderbesluit 2008/977. Dit Kaderbesluit regelde de verwerking van persoonsgegevens in de EU op het terrein van politie en justitie. Doel daarvan was het creëren van een overkoepelende samenwerking bij politie en justitie om op EU-niveau bij de verwerking van persoonsgegevens een hoge mate van bescherming te waarborgen van natuurlijke personen. Anders dan in de AVG schrijft Richtlijn 2016/680 voor dat – voor zover mogelijk en relevant – de persoonsgegevens in categorieën worden onderscheiden, zoals verdachten, veroordeelden, slachtoffers en getuigen. De richtlijn geldt ook voor interne situaties

© Noordhoff Uitgevers bv

zonder dat er een grensoverschrijdend element aanwezig is. Dit is een afwijking ten opzichte van het Kaderbesluit.

1.3.5 Raad van Europa, EVRM en IVBPR

Zoals uit het voorgaande blijkt, was de aandacht voor de bescherming van de persoonlijke levenssfeer niet een uitsluitend Nederlandse aangelegenheid. Die aandacht was er al eerder op Europees niveau. In 1950 kwam het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) tot stand. Sinds 1954 is Nederland partij bij dit verdrag. Op grond van artikel 94 Gw heeft dit verdrag directe werking. Dit betekent dat de rechterlijke macht wetten moet toetsen aan het EVRM.

EVRM

Na de Tweede Wereldoorlog was er in Europa behoefte aan een organisatie die zich zou richten op het bevorderen van mensenrechten en democratie. Die organisatie werd de Raad van Europa (RvE). In het EVRM wordt de doelstelling van de RvE zichtbaar. Anders dan soms wordt gedacht, is het EVRM geen verdrag van de EU maar van de RvE (www.coe.int). Bij de RvE zijn 47 landen aangesloten. Naast de lidstaten van de EU zijn bijvoorbeeld ook Rusland, Turkije en landen in de Kaukasus lid. Het EVRM biedt burgers van de aangesloten landen de mogelijkheid om hun rechten die voortvloeien uit het EVRM te laten toetsen door een rechtelijke macht. Dit is het Europese Hof voor de Rechten van de Mens (EHRM) dat is gevestigd in Straatsburg (niet te verwarren met het HvJ EU dat gevestigd is in Luxemburg). Met name artikel 8 EVRM is van belang als het gaat over de bescherming van persoonsgegevens. Dit artikel luidt:

1 'Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2 Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.'

Uit de tekst van artikel 8 EVRM blijkt dat het niet uitsluitend gaat over privéleven, maar ook over familie- en gezinsleven (family life). Voor het onderwerp van dit boek is het element 'privéleven' het meest relevant.

In zaken waarin door burgers een beroep wordt gedaan op artikel 8 EVRM beoordeelt het EHRM eerst of het eerste lid van toepassing is; met andere woorden: is er in de voorliggende zaak sprake van een privéleven. Is het antwoord op die vraag positief, dan kijkt het EHRM naar het tweede lid. Is in het concrete geval een eventuele 'inmenging van enig openbaar gezag' in de persoonlijke levenssfeer toegestaan? Is er geen sprake van een privéleven dan is artikel 8 EVRM niet van toepassing. De strekking van artikel 8 EVRM is dat dit artikel de burger beschermt tegen ongerechtvaardigd overheidsingrijpen. Dit betekent dat als op grond van het eerste lid wordt geconcludeerd dat er sprake is van een inbreuk op het recht op respect voor het privéleven, dit alleen leidt tot een schending van artikel 8 EVRM als de inbreuk op dit recht niet toelaatbaar is. Dit blijkt onder meer uit de volgende zaken.

© Noordhoff Uitgevers bv

EHRM 16 december 1992, nr. 13710/88 Niemietz vs. Duitsland
Niemietz – een Duitse advocaat met een activistisch verleden – werd verdacht een dreigbrief te hebben verzonden. In het kader daarvan doorzocht de politie zijn kantoor. Daarbij werden ook dossiers van cliënten doorzocht. Er werd geen belastend materiaal gevonden en de zaak tegen Niemietz werd wegens gebrek aan bewijs geseponeerd. Bij de rechter beklaagde Niemietz zich over het huiszoekingsbevel. Dit was volgens hem onzorgvuldig geformuleerd. Hierdoor stond het aantal documenten dat door de politie was bekeken in geen verhouding tot de verdenking, mede gelet op de geheimhoudingsplicht die een advocaat heeft. Dit was een aantasting van het recht op respect voor zijn privéleven als bedoeld in artikel 8 EVRM. Duitsland was het niet eens met dit standpunt en betoogde dat een bedrijfsruimte geen privédomein is. Het EHRM vond de opvatting van Duitsland te restrictief. Respect voor het privéleven behelst ook het recht om relaties met andere mensen op te bouwen. Bezien vanuit dat standpunt was er geen reden om professionele activiteiten buiten het begrip privéleven te plaatsen omdat iemand via zijn werk bij uitstek relaties met de buitenwereld kan aangaan. Met deze uitspraak erkende het EHRM dat onder omstandigheden natuurlijke personen ook bij het uitoefenen van zakelijke activiteiten bescherming kunnen ontlenen aan artikel 8 EVRM. Omdat het huiszoekingsbevel meer inbreuk op het privéleven toestond dan de verdenking rechtvaardigde, was de klacht van Niemietz terecht.

EHRM 25 juni 1997, nr. 20605/92 Halford vs. Verenigd Koninkrijk
De telefoon van een Engelse werkneemster werd heimelijk op haar werkplek door de werkgever afgeluisterd. In deze zaak stelde het EHRM zich op het standpunt dat – net als in de zaak van Niemietz – het recht op privacy zich ook tot de werkplek kan uitstrekken. Omdat het Engelse recht geen bepalingen bevatte met betrekking tot het (heimelijk) afluisteren van telecommunicatie via het interne telecommunicatienetwerk kon niet gezegd worden dat de werkneemster de inbreuk op haar recht op privacy had kunnen voorzien. Daarnaast was er ook geen nationaal rechtsmiddel om tegen een eventuele schending van artikel 8 EVRM op te komen. Dit leverde volgens het EHRM een schending op van artikel 8 EVRM.

Hoewel uit de uitspraken van het EHRM blijkt dat het in het algemeen een ruime uitleg geeft van het recht op respect voor het privéleven, leidt dit niet altijd tot bescherming van persoonsgegevens. Niet bij elke verwerking van een persoonsgegeven is de persoonlijke levenssfeer in het geding, zoals blijkt uit de volgende zaak.

EHRM 4 januari 2007, nr. 39658/05 Smith vs. Verenigd Koninkrijk
In deze zaak werd de klacht van Smith over schending van artikel 8 EVRM door het EHRM niet-ontvankelijk verklaard. Smith beklaagde zich erover dat hij geen inzage kreeg in een zakelijk dossier, terwijl zijn naam uit hoofde van zijn professionele hoedanigheid in bepaalde documenten voorkwam. Het EHRM meende dat artikel 8 EVRM niet van toepassing was omdat het dossier uitsluitend zakelijke informatie bevatte en Smith al bekend was met de inhoud daarvan.

Uit artikel 8 lid 2 EVRM vloeit voort dat inmenging in het privéleven van burgers door overheden is toegestaan als dit wettelijk is geregeld en die inmenging om een aantal specifieke redenen – zoals nationale veiligheid of het

© Noordhoff Uitgevers bv

economisch welzijn van het land – noodzakelijk is. Er moet sprake zijn van een redelijke verhouding ('fair balance') tussen enerzijds het maatschappelijk belang dat de wetgeving dient en anderzijds de inbreuk die deze wetgeving maakt op het privéleven van burgers. In februari 2020 concludeerde de rechtbank Den Haag in de volgende zaak dat de redelijke verhouding ontbrak bij het door de overheid gebruikte Systeem Risico Indicatie (SyRI).

ECLI:NL:RBDHA:2020:865 NJCM c.s. vs. De Staat
Een aantal maatschappelijke organisaties waaronder het Nederlands Juristen Comité voor de Mensenrechten (NJCM) hebben deze zaak aangespannen omdat zij een 'halt' wilden toeroepen aan het gebruik van SyRI. Dit is een wettelijk instrument dat de overheid gebruikt voor de bestrijding van fraude op bijvoorbeeld het terrein van uitkeringen, toeslagen en belastingen. Met de inzet van SyRI worden bestanden waarover (overheids)instanties beschikken gestructureerd gekoppeld om samenhangende misstanden op het terrein van uitkeringen, toeslagen en belastingen te kunnen onderkennen en daarmee de pakkans te verhogen.
Uitgangspunt voor de rechtbank is dat de sociale zekerheid één van de pijlers van de Nederlandse maatschappij is en in belangrijke mate bijdraagt aan de welvaart in Nederland. In dat kader deelt de rechtbank het standpunt van de Staat dat nieuwe technologieën – waaronder de digitale mogelijkheden om bestanden te koppelen en met behulp van algoritmes data te analyseren – moeten worden benut om fraude te voorkomen en te bestrijden. De rechtbank meent echter dat de SyRI-wetegeving – die is vastgelegd in de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet Suwi) – in haar huidige vorm in strijd is met artikel 8 lid 2 EVRM. Het gebruik van SyRI is volgens de rechtbank onvoldoende inzichtelijk en controleerbaar. In dat kader verwijst de rechtbank naar het transparantiebeginsel, het doelbindingsbeginsel en het beginsel van dataminimalisatie van artikel 5 AVG. Hierdoor is er geen sprake van een 'fair balance'. Als gevolg daarvan verklaart de rechtbank artikel 65 Wet Suwi en hoofdstuk 5a van het Besluit Suwi onverbindend wegens strijd met artikel 8 lid 2 EVRM.

Verdrag van Straatsburg
Artikel 8 EVRM is in 1981 uitgewerkt in het Verdrag van Straatsburg, ook wel het Dataprotectieverdrag genoemd. Nederland is partij bij dit verdrag. Het verdrag – dat de basis legde voor de Europese privacybescherming – heeft betrekking op de geautomatiseerde verwerking van persoonsgegevens. De verwerking van persoonsgegevens moet eerlijk, rechtmatig, nauwkeurig en proportioneel zijn.

Internationaal verdrag inzake burgerrechten en politieke rechten (IVBPR)
Het IVBPR is een verdrag dat in 1966 tot stand kwam bij de Verenigde Naties. Het is gebaseerd op de Universele Verklaring van de Rechten van de Mens. Het verdrag is in 1969 door Nederland ondertekend en in 1978 geratificeerd. Artikel 17 IVBPR regelt het recht op privacy en luidt:

'1 Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privéleven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.
2 Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.'

© Noordhoff Uitgevers bv

Het EVRM geeft de burger in veel gevallen dezelfde bescherming als het IVBPR of meer. Hoewel het IVBPR op grond van artikel 94 Gw directe werking heeft, heeft het verdrag voor het gegevensbeschermingsrecht geen betekenis. De AVG biedt op het terrein van de verwerking van persoonsgegevens burgers meer en betere bescherming dan het IVBPR.

1.3.6 Organisatie voor Economische Samenwerking en Ontwikkeling (OESO)

De OESO (www.OECD.org) is een samenwerkingsverband van 35 (voornamelijk welvarende) landen om sociaal en economisch beleid te bespreken en te coördineren. Nederland was in 1961 een van de oprichters van de OESO. In 1980 wees de OESO voor het eerst op de gevaren voor de persoonlijke levenssfeer van het gebruik van persoonsgegevens. Dit standpunt werd uitgewerkt in een richtlijn die in 2013 werd geactualiseerd (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data). In deze richtlijn wordt een aantal principes geformuleerd voor de verwerking van persoonsgegevens. Deze principes sluiten aan bij de AVG. De richtlijnen van de OESO zijn gezaghebbend maar niet bindend. Burgers kunnen er geen rechten aan ontlenen.

1.3.7 Overzicht van de ontwikkeling van het recht op privacy

De in dit hoofdstuk behandelde ontwikkeling van het recht op privacy en het gegevensbeschermingsrecht wordt in het volgende overzicht samengevat.

1815	Huisrecht opgenomen in artikel 170 van de Grondwet uit 1815. Dit is nu artikel 12 van de Grondwet.
1848	Briefgeheim opgenomen in artikel 154 van de Grondwet uit 1948. Dit is nu artikel 13 van de Grondwet.
1954	Nederland sluit zich aan bij het EVRM dat in 1950 tot stand is gekomen. Het verdrag is opgesteld door de Raad van Europa.
1978	Nederland ratificeert het IVBPR. In dit verdrag wordt onder meer aandacht besteed aan het recht op privacy.
1981	Nederland wordt partij bij het Verdrag van Straatsburg. Dit wordt ook wel het Dataprotectieverdrag genoemd. Het verdrag is opgesteld door de Raad van Europa en heeft een wereldwijde reikwijdte. In het verdrag wordt artikel 8 EVRM uitgewerkt. Het verdrag heeft betrekking op de geautomatiseerde verwerking van persoonsgegevens.
1983	In de Grondwet wordt het recht op lichamelijke integriteit (artikel 11) opgenomen en het recht op bescherming van de persoonlijke levenssfeer (artikel 10).
1989	De Wet persoonsregistraties treedt in werking. De Wpr is een uitwerking van artikel 10 van de Grondwet.
1995	De Privacyrichtlijn 1995 wordt door de EU vastgesteld. De lidstaten moeten deze richtlijn uiterlijk in oktober 1998 in hun wetgeving geïmplementeerd hebben. Nederland voldoet pas in 2001 aan deze verplichting.
2000	Opstelling EU-Grondrechtenhandvest. Dit document krijgt kracht van wet bij het Verdrag van Lissabon.
2001	De Wet bescherming persoonsgegevens treedt in werking en vervangt de Wpr. De Wbp is gebaseerd op de Privacyrichtlijn 1995.
2004	Aanpassing Telecommunicatiewet aan de E-Privacyrichtlijn 2002.
2007	Verdrag van Lissabon treedt in werking. Door dit verdrag veranderen onder meer de besluitvormingsprocedures in de EU. Het EG-Verdrag verdwijnt. Hiervoor in de plaats komt het VWEU. Met de inwerkingtreding van het Verdrag van Lissabon krijgt ook het EU-Grondrechtenhandvest kracht van wet.

© Noordhoff Uitgevers bv

2009	Het Kaderbesluit 2008/977 treedt in werking. Dit besluit regelde de verwerking van persoonsgegevens in de EU op het terrein van politie en justitie.
2013	Geactualiseerde richtlijn (uit 1980) van de OESO over de verwerking van persoonsgegevens. In de richtlijn worden alleen basisprincipes geformuleerd. Nederland is sinds 1961 betrokken bij de OESO. Burgers kunnen aan de richtlijn geen rechten ontlenen.
2016	De AVG wordt vastgesteld. Lidstaten krijgen tot mei 2018 de tijd hun wetgeving hierop aan te passen.
2018	De AVG en de UAVG treden in mei 2018 in werking. De Wbp wordt ingetrokken. Daarnaast treedt de Richtlijn gegevensverwerking politie en justitie in werking. De richtlijn vervangt het Kaderbesluit 2008/977. De richtlijn is geen aanvulling op de AVG, maar een zelfstandige regeling.

Het gegevensbeschermingsrecht zoals we dat nu in Nederland kennen, is in hoofdzaak Europees recht. Voor de EU is het beschermen van persoonsgegevens een fundamenteel recht. In landen buiten de EU wordt daar soms anders over gedacht. Zo is in de VS gekozen voor een andere benadering. Daar wordt de bescherming van persoonsgegevens geregeld in het consumentenrecht.

1.4 Persoonsgegevens

De AVG heeft als belangrijke doelstelling dat de persoonsgegevens van burgers goed worden beschermd. Wat zijn persoonsgegevens en wie kent die gegevens of kan daar – onder welke voorwaarden – over beschikken?

Art. 4 AVG verstaat onder persoonsgegevens:

> ‘alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene); als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online-identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon’.

Anonieme gegevens en identificatie
Uit de definitie blijkt dat er pas sprake is van een persoonsgegeven als de natuurlijk persoon identificeerbaar is. Anonieme gegevens zijn geen persoonsgegevens. Onder meer bij (wetenschappelijk) onderzoek of voor statistische doeleinden wordt gebruikgemaakt van anonieme gegevens. Anonieme gegevens die worden gecombineerd met andere gegevens als gevolg waarvan identificatie alsnog mogelijk is, vallen onder de reikwijdte van de AVG. Het zijn indirect identificeerbare persoonsgegevens. Een voorbeeld ter illustratie.

Stel dat aan een groep van 50 personen wordt gevraagd tot welke religie zij behoren. De groep bestaat uit 35 personen tussen 20 en 30 jaar, 14 personen tussen 30 en 40 jaar en 1 persoon die 50 jaar oud is. Stel dat de laatstgenoemde persoon, 17 van de 20- tot 30-jarigen en de helft van de 30- tot 40-jarigen aangeven protestant te zijn en de anderen aangeven niet religieus te zijn. Worden de antwoorden weergegeven zonder vermelding

© Noordhoff Uitgevers bv

van de leeftijd dan blijken van de 50 personen er 25 protestant te zijn. Wie protestant is, kan niet worden nagegaan. Worden de antwoorden daarentegen gecombineerd met de leeftijden, dan wordt duidelijk dat de persoon die 50 jaar is, aanhanger is van het protestantse geloof.

Om de mogelijkheid van identificatie te verkleinen bij onderzoeken zoals hiervoor beschreven, wordt vaak bij de weergave van de antwoorden een bepaalde bandbreedte aangehouden. Het College bescherming persoonsgegevens – de voorganger van de Autoriteit Persoonsgegevens – meldt hierover in 2002 als kader voor een gedragscode voor wetenschappelijk onderzoek en statistiek onder andere het volgende:

> 'Zo is, naar de huidige inzichten, bij een onderzoekbestand van een steekproef van minder dan 1% uit een algemene populatie of een selectie daaruit naar algemene kenmerken (bijvoorbeeld leeftijd, sekse, regio) de indirecte herleidbaarheid te verwaarlozen.'

Om te bepalen of een natuurlijk persoon identificeerbaar is, moet – volgens overweging 26 AVG – rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt om de natuurlijke persoon direct of indirect te identificeren. Met alle objectieve factoren, zoals de kosten en de tijd benodigd om iemand te identificeren, moet rekening worden gehouden. Bij het identificeren van een natuurlijk persoon gaat het er dus niet om of het met gebruik van bepaalde gegevens theoretisch mogelijk is iemand te identificeren, maar of dit in redelijkheid mogelijk is. Wat in dit verband redelijk is, is afhankelijk van de concrete omstandigheden. Zo mogen in de regel aan een groot onderzoeksinstituut hogere eisen worden gesteld dan aan een organisatie die over weinig mensen en middelen beschikt.

In de definitie van persoonsgegeven wordt een onderscheid gemaakt tussen directe en indirecte identificatie. Het combineren van naam, adres en geboortedatum geeft in de meeste gevallen een dermate uniek resultaat dat een natuurlijk persoon op basis van die gegevens met zekerheid of met een grote mate van waarschijnlijkheid kan worden geïdentificeerd. Er is sprake van directe identificatie. De identiteit van de betreffende persoon kan zonder veel omwegen eenduidig worden vastgesteld. Dit ligt anders wanneer de gegevens niet direct tot identificatie van een bepaalde persoon leiden maar via nadere stappen de gegevens in verband kunnen worden gebracht met een bepaalde persoon. In dat geval is er sprake van indirecte identificatie. Wat te doen als de gebruikelijke gegevens om iemand te identificeren zoals naam, adres en geboortedatum niet bekend zijn? Denk daarbij aan een verward persoon met geheugenverlies of een verdachte van een strafbaar feit die weigert deze gegevens te verstrekken. In dergelijke situaties zal men van andere gegevens gebruik moeten maken zoals foto's of vingerafdrukken om de identiteit te achterhalen.

Bijzondere categorieën persoonsgegevens

Niet elk gegeven over een persoon maakt in gelijke mate inbreuk op de persoonlijke levenssfeer. Een adres kan een persoonsgegeven zijn. Wordt bekend waar iemand woont, dan kan dat een inbreuk zijn op de persoonlijke levenssfeer, zeker als het een beroemd persoon betreft. Die inbreuk is echter van een heel andere orde dan gegevens over bijvoorbeeld iemands

© Noordhoff Uitgevers bv

gezondheid, religie of ras. Dit zijn gevoelige persoonsgegevens en de bescherming daarvan is apart geregeld in artikel 9 AVG. Overweging 51 AVG motiveert dit als volgt.

> 'Persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden'.

Betrokkene

In de AVG wordt een geïdentificeerd persoon omschreven als 'betrokkene'. Het is degene over wie de gegevens informatie bevatten. In de regel zullen de persoonsgegevens betrekking hebben op één persoon maar dat hoeft niet altijd het geval te zijn. Persoonsgegevens kunnen op meerdere personen betrekking hebben. Zo wonen ouders met hun minderjarige kinderen in de regel op hetzelfde adres en hebben mogelijk ook hetzelfde telefoonnummer. Is dat het geval, dan is eenieder voor zichzelf 'betrokkene'. Dat geldt ook voor de minderjarige kinderen. Elk individu heeft zijn of haar 'eigen' persoonsgegevens. Dat wil zeggen de persoonsgegevens waar het individu mee geïdentificeerd kan worden.

Relevante informatie met betrekking tot persoonsgegevens

Onder de woorden 'alle informatie' in de definitie van het begrip persoonsgegeven wordt ook subjectieve informatie verstaan, zoals meningen of beoordelingen. Dit blijkt uit de volgende uitspraak van het HvJ EU.

> **ECLI:EU:C:2017:994 Nowak**
> Peter Nowak diende in 2010 een verzoek in om inzage te krijgen in alle persoonsgegevens die de beroepsorganisatie voor accountants/belastingadviseurs (CAI) over hem had. Het CAI stuurde hem enige documenten, maar weigerde zijn schriftelijk examenwerk toe te sturen. Nowak beklaagde zich hierover bij de Ierse toezichthouder. De toezichthouder meende dat de gegevens van het examen geen persoonsgegevens vormden. Dit oordeel werd gedeeld door de rechtsprekende instanties. Uiteindelijk besloot de hoogste Ierse rechter om duidelijkheid te vragen aan het HvJ EU. Het Hof oordeelde dat de woorden 'alle informatie' in de definitie van persoonsgegevens ruim moeten worden uitgelegd. Dit betekent dat ook subjectieve informatie zoals meningen of beoordelingen onder het begrip persoonsgegevens kunnen vallen. De informatie moet wel over de betrokkene gaan. Dat was bij Nowak het geval. De door Nowak gegeven antwoorden gaven informatie over zijn kennis en kunde en konden van belang zijn voor een evaluatie. Datzelfde gold voor de opmerkingen die de examinator bij het gemaakte werk had gemaakt.

Soms wordt in het kader van een juridische procedure of een klachtprocedure door een buitenstaander een beoordeling gegeven over een zaak. Die beoordeling kan het karakter hebben van een juridische of medische analyse. Hoewel een dergelijke analyse betrekking heeft op (de zaak van) een bepaalde persoon, is er geen sprake van een persoonsgegeven, zoals blijkt uit de volgende uitspraken.

> **ECLI:EU:C:2014:2081 IND**
> In deze zaak legden Nederlandse rechters het HvJ EU de prejudiciële vraag voor over het recht op inzage in de minuten die ten grondslag liggen aan de

© Noordhoff Uitgevers bv

beslissing op een asielaanvraag. Onder een 'minuut' wordt in dit verband verstaan een vastgesteld en goedgekeurd concept van een geschrift. De 'minuten' waar het in deze zaak om ging, bevatten onder meer een juridische analyse van de situatie van de asielaanvrager. De inzage in deze 'minuten' wordt sinds 2009 standaard geweigerd door de Nederlandse overheid. Dit tot frustratie van asieljuristen. De zaak spitste zich toe op de vraag of de juridische analyse een persoonsgegeven is. Volgens het Hof is een juridische analyse een uitleg van de wet en zegt dit op zich niets over de persoon van de betrokkene. Het is daarom geen informatie over de persoon. Dit standpunt vindt ook steun als men kijkt naar de bedoeling van de Privacyrichtlijn 1995. Die heeft onder meer tot doel burgers de mogelijkheid te geven te controleren of hun persoonsgegevens juist en rechtmatig worden verwerkt. De juridische analyse heeft daar geen betrekking op. De in de juridische analyse vermelde persoonsgegevens van de aanvrager van de verblijfsvergunning zijn persoonsgegevens. Omdat die persoonsgegevens uit de juridische analyse zijn verstrekt, is aan het inzageverzoek voldaan.

ECLI:NL:HR:2018:365 Waterlandziekenhuis
In deze zaak ging het om de beroepsaansprakelijkheid van een arts. Na de bevalling – door middel van een keizersnede waarbij een verlostang werd gebruikt -– bleek de baby een hoge dwarslaesie te hebben. De arts en het ziekenhuis werden hiervoor aansprakelijk gesteld. In het kader van die procedure wilde de moeder van de baby inzage hebben in een notitie met bevindingen die was opgesteld door een door de arts en het ziekenhuis geraadpleegde radioloog. Dit verzoek was door het hof geweigerd. Volgens de Hoge Raad was dit terecht. Onder verwijzing naar het hiervoor vermelde oordeel van het HvJ EU concludeerde de Hoge Raad dat wat geldt voor een juridische analyse ook geldt voor een medische analyse.

Objectgegevens en bedrijfsgegevens
Gegevens over objecten kunnen iets zeggen over de eigenaar en zouden in dat geval persoonsgegevens kunnen zijn. Zo kan de verkoper van een woning het vervelend vinden als iedereen op een website kan lezen hoe vaak en hoeveel de prijs van de woning is verlaagd. Dergelijke informatie zou het gedrag van een potentiële koper in voor de verkoper ongunstige zin kunnen beïnvloeden. In ECLI:NL:GHAMS:2013:5224 (*Street View*) bevestigde het Hof Amsterdam in hoger beroep de uitspraak van de voorzieningenrechter waarbij een gebod tot verwijdering van persoonsgegevens van de website van Google Maps of Google Street View werd afgewezen. Het ging om afbeeldingen van objecten en niet om een identificeerbaar persoon.
In ECLI:NL:RBZWO:2004:AO6018 (*inzage MKZ-dossier*) werd in de nasleep van de mond- en klauwzweer crisis een verzoek van de eigenaar van een besmet bedrijf om inzage in een rapport van de Rijksdienst voor de keuring van Vee en Vlees afgewezen omdat volgens de voorzieningenrechter de betreffende gegevens niet als persoonsgegevens konden worden aangemerkt. De gegevens hadden betrekking op dieren; het waren bedrijfsgegevens.

1.4.1 IP-adres

Met de komst van het internet rees de vraag of een in 1989 bedacht internetprotocoladres – afgekort IP-adres – een persoonsgegeven is. Het is een voorbeeld van een ontwikkeling waar het recht niet onmiddellijk een antwoord op had. Sommigen meenden dat er geen sprake was van een persoonsgegeven, anderen – waaronder de voorganger van de Autoriteit Persoonsgegevens – meenden dat dit in de regel wel het geval is.

© Noordhoff Uitgevers bv

Computers hebben een IP-adres nodig om met elkaar te kunnen communiceren. Bij bedrijven en organisaties is het IP-adres in de regel gekoppeld aan het bedrijf of de organisatie. Bij particulieren die hun computer privé gebruiken, bepaalt de internetprovider het IP-adres. Via het IP-adres zijn bijdragen op het internet in beginsel te herleiden tot een natuurlijk persoon. Dat is niet altijd eenvoudig. Allereest is er de koppeling van het IP-adres aan een rechtspersoon. Bij een rechtspersoon kunnen meerdere medewerkers van het IP-adres gebruikmaken. Bij computers die privé worden gebruikt, is er de kans dat huisgenoten van degene van wie de computer is die ook gebruiken. Daarnaast bestaat er de mogelijkheid gebruik te maken van dynamische IP-adressen. In dat geval krijgt de gebruiker een IP-adres niet op basis van een abonnement of in het kader van een dienstbetrekking, maar voor de duur van de verbinding. Een voorbeeld van dynamische IP-adressen zijn de IP-adressen die worden toegewezen aan computers in een internetcafé waar de klanten zich voor het gebruik van een computer niet hoeven te legitimeren. Het is tegen de achtergrond van de hiervoor gegeven voorbeelden dat degenen die menen dat een IP-adres geen persoonsgegeven is, vaak aanvoeren dat het om technische en organisatorische redenen niet mogelijk is de gebruiker te identificeren. In ECLI:EU:C:2016:779 (*Breyer*) heeft het HvJ EU geconcludeerd dat IP-adressen in beginsel persoonsgegevens zijn. Dit geldt ook voor dynamische IP-adressen waarvan de gebruiker van de computer zich niet heeft geïdentificeerd als met behulp van extra – zo nodig bij derden verkregen – informatie identificatie mogelijk is. Dit is alleen anders als het inwinnen van de extra informatie bij wet verboden of praktisch ondoenlijk is.

De hiervoor vermelde uitspraak was gebaseerd op de Privacyrichtlijn 1995. Anders dan in die richtlijn kan op grond van de AVG identificatie ook plaats vinden met behulp van een online-identificator. Een IP-adres is een online-identificator zoals blijkt uit de volgende omschrijving uit overweging 26 AVG:

> 'Natuurlijke personen kunnen worden gekoppeld aan online-identificatoren via hun apparatuur, applicaties, instrumenten en protocollen, zoals internetprotocol (IP)-adressen, identificatiecookies of andere identificatoren zoals radiofrequentie-identificatietags. Dit kan sporen achterlaten die, met name wanneer zij met unieke identificatoren en andere door de servers ontvangen informatie worden gecombineerd, kunnen wordt gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen.'

Net als in de Privacyrichtlijn 1995 geldt echter ook in de AVG dat als het onevenredig veel moeite of middelen vergt om de identiteit van een persoon te achterhalen, dit achterwege kan blijven (overweging 26 AVG). Het risico dat de identiteit van een persoon kan worden achterhaald, wordt onder die omstandigheden verwaarloosbaar klein geacht.

1.4.2 Gegevens van overleden personen

Gegevens van personen die zijn overleden, zijn geen persoonsgegevens in de zin van de AVG (overweging 27 AVG). Dit was ook het geval in de Wbp. Als het verwerken van persoonsgegevens van overleden personen de persoonlijke levenssfeer van nog levende personen raakt, dan kan de AVG van toepassing zijn zoals blijkt uit de volgende zaak.

© Noordhoff Uitgevers bv

ECLI:NL:RBAMS:2003:AN9893 Child Survivors
De Stichting Digitaal Monument Joodse Gemeenschap in Nederland (hierna: de stichting) heeft tot doel het levend houden van de herinnering aan Joden die de Sjoa in Nederland hebben meegemaakt en hen en hun nakomelingen in staat te stellen hun wortels te (her)vinden, alsook de gegevens in de archieven aan te vullen met hun herinneringen en privédocumenten. Om dit doel te bereiken worden de gegevens gedigitaliseerd en gedeeltelijk op de website geplaatst. Eiseres is de enige dochter van Joodse ouders. Haar oudere broer, een nichtje en zijzelf zijn de enige nog in leven zijnde 'Child Survivors' van de Sjoa in hun familie. Eiseres wil de stichting verbieden gegevens op de website te plaatsen van haar familie met betrekking tot haar grootouders van vaders- en moederszijde en hun nabestaanden en degenen met wie zij gehuwd zijn. Eiseres beroept zich daarbij onder meer op de Wbp en haar recht op privacy. Op de website zal over eiseres alleen worden vermeld dat zij een 'overlevend kind' is. Eiseres krijgt geen gelijk. De voorzieningenrechter overweegt onder meer het volgende: 'De Wbp is slechts van toepassing op gegevens die betrekking hebben op identificeerbare natuurlijke personen die nog in leven zijn. Een identificeerbare persoon is blijkens de wetgeschiedenis een persoon wiens identiteit zonder onevenredige inspanning kan worden vastgesteld. Uit de enkele vermelding 'overlevend kind' uit het gezin van haar wel op de website te vermelden vader kan haast onmogelijk – laat staan zonder onevenredige inspanning – worden afgeleid dat eiseres de dochter is van die in 1942 in Auschwitz vermoorde vader. Eiseres is dan ook geen identificeerbare persoon in de zin van de Wbp'.

Op grond van overweging 27 AVG kunnen EU-lidstaten met betrekking tot de verwerking van persoonsgegevens van overleden personen eigen regels stellen. Verplicht is dit niet. Nederland heeft in de UAVG geen gebruik gemaakt van de mogelijkheid regels te stellen met betrekking tot de verwerking van persoonsgegevens van overledenen. Dit laatste betekent niet dat in andere wetten geen rekening wordt gehouden met de persoonsgegevens en de privacy van overleden personen. Dit is onder meer het geval als het gaat om inzage in het medisch dossier, het portretrecht en het gebruik van de naam van de overledene.

Inzage medisch dossier overledene
Medische gegevens over een persoon zijn persoonsgegevens. Op grond van artikel 7:457 BW geldt als hoofdregel dat een hulpverlener zonder toestemming van de patiënt anderen – met uitzondering van andere hulpverleners die de patiënt behandelen – geen inzage geeft in een medisch dossier. Dit is het medisch beroepsgeheim. De ratio van deze bepaling is te voorkomen dat zieken ervan worden weerhouden geneeskundige hulp in te roepen uit vrees dat wat door de geneeskundige wordt geconstateerd, openbaar wordt. Die vrees kan ook bestaan wanneer de geheimhouding niet blijft gelden na het overlijden van de patiënt. De geheimhoudingsplicht weegt daarom zwaar en kan alleen om zwaarwegende redenen doorbroken worden. Dit is bijvoorbeeld het geval als alleen in het medisch dossier de antwoorden te vinden zijn op bepaalde vragen over de overledene. Dit standpunt vloeit voort uit ECLI:NL:HR:2001:AB1201 (*inzage medisch dossier*) waarin de broer van een overledene inzage vroeg in het medisch dossier van de overledene. Deze had zijn buurvrouw tot enig erfgenaam benoemd. De broer die om inzage verzocht, betwijfelde of de erflater bij het opmaken van zijn testament zijn wil had kunnen bepalen. Uit de informatie

© Noordhoff Uitgevers bv

van de notaris bleek echter dat de overledene wist wat hij deed toen hij zijn buurvrouw tot erfgenaam benoemde. De broer kreeg geen inzage in het medisch dossier.

In ECLI:NL:RBDOR:2007:BB9778 (*De grote rivieren*) verzocht een familielid van de overledene in kort geding om inzage in de correspondentie die de overledene – die zich van het leven had beroofd – met zijn behandelaar had gevoerd. Daarbij beriep het familielid zich op de Wob. De voorzieningenrechter merkte hier onder meer het volgende over op.

> 'Niet valt in te zien dat datgene dat iemand bij leven tot zijn persoonlijke levenssfeer rekende en niet over zichzelf buiten die persoonlijke levenssfeer kenbaar wilde hebben, na overlijden niet langer tot diens persoonlijke levenssfeer zou blijven behoren en niet langer zou behoeven te worden gerespecteerd. Dit geldt des te sterker voor medische gegevens, die bij uitstek een privacygevoelig karakter hebben. De omstandigheid dat de Wbp niet ziet op bescherming van persoonsgegevens na overlijden en daardoor het begrip "persoonlijke levenssfeer" zich in die wet beperkt tot levende personen, maakt niet dat het begrip "persoonlijke levenssfeer" in de WOB op diezelfde wijze moet worden uitgelegd. Ook het betoog van verweerder dat uit de betekenis van het woord "levenssfeer" in het dagelijks taalgebruik voortvloeit dat die sfeer een in leven zijnde persoon betreft, acht de voorzieningenrechter niet overtuigend'.

Portretten van overledenen

Wordt iemand herkenbaar afgebeeld, dan is er sprake van een portret. Dit is een persoonsgegeven. Een portret in de zin van de Auteurswet (Aw) kan een foto zijn maar ook een schilderij of een tekening. Essentieel voor een portret is dat men herkenbaar is. Dit betekent dat er zelfs sprake van een 'portret' kan zijn als het gaat om een lookalike van een bekend persoon in een reclame, oordeelde de rechter in ECLI:NL:RBAMS:2017:6395 (*Max Verstappen vs. Picnic*).

De geportretteerde bezit portretrecht. Dit is geregeld in artikel 19-22 Aw. Het portretrecht is een persoonlijk recht. Dit betekent dat alleen de geportretteerde of diens nabestaanden dit recht kunnen uitoefenen. Op grond van artikel 20 Aw is het in beginsel niet toegestaan een portret van een overledene gedurende tien jaar na diens overlijden te publiceren. Is een portret zonder opdracht van de geportretteerde gemaakt, dan is het de maker daarvan (de auteur) niet toegestaan dit openbaar te maken als een redelijk belang van de geportretteerde zich daartegen verzet (artikel 21 Aw). Een redelijk belang kan zowel betrekking hebben op persoonlijke (privacy) als op commerciële belangen. In ECLI:NL:RBAMS:2012:BY2573 (*Nicole van den Hurk*) verzocht de vader van Nicole van den Hurk in kort geding de uitzending 'Praten met de doden' van RTL Nederland over zijn vermoorde dochter te verbieden. De vader meende dat met het programma zijn dochter werd misbruikt voor een amusementsprogramma, terwijl daar geen enkel belang mee was gediend en men de doden diende te respecteren. Het verzoek werd door de rechter afgewezen, onder meer op grond van de volgende overwegingen:

> 'De voorzieningenrechter van de rechtbank weegt bij de vraag of het recht op bescherming van de privacy van de vader of het recht op vrije meningsuiting van RTL Nederland zwaarder weegt, de wederzijdse belangen van partijen af

© Noordhoff Uitgevers bv

en heeft alle relevante omstandigheden van het geval meegenomen. Voorts oordeelt de voorzieningenrechter dat artikel 21 Auteurswet de vader van Nicole geen absoluut recht verschaft zich tegen iedere verspreiding van portretten van Nicole te verzetten. Op grond hiervan wijst de voorzieningenrechter de vordering van de vader af. Hij heeft geen redelijk belang om de uitzending tegen te houden. Er is geen sprake van schending van zijn privacy, nu noch zijn naam, noch hijzelf in beeld komt in de uitzending. Meegewogen wordt ook dat onderhavige onopgeloste moord de laatste jaren veel in de publiciteit is geweest'.

Het gebruik van de naam van de overledene

In de praktijk komt het regelmatig voor dat organisaties de naam van een overledene willen gebruiken. Het gaat dan vaak om een beroemde overledene die men met de naamgeving wil eren. Ook veel straatnamen dragen de naam van een overledene. In ECLI:NL:GHAMS:2015:3034 (*weduwe Kopland/stichting Het Kopland*) overweegt het Hof Amsterdam hier het volgende over.

'Vernoeming van een instelling naar een bekende persoon is een delicate kwestie die dientengevolge omkleed dient te zijn met duidelijke zorgvuldigheidsnormen die bij dit delicate proces in acht moeten worden genomen. Bij de vernoeming, met name kort na het overlijden van de betreffende persoon, dient rekening te worden gehouden met vanzelfsprekende en te respecteren gevoelens van de nabestaanden. Tevens dient rekening gehouden te worden met het beheer van het morele en immateriële aspect van de nalatenschap van de overledene. De directe nabestaanden komt naar algemeen maatschappelijke opvattingen een rol toe waar het gaat om het beheer van de geestelijke nalatenschap en het beheer van de integriteit en reputatie van de overledene. De nabestaanden zijn het best geëquipeerd om te beoordelen of ook naar de vermoedelijke wens en opvatting van de overledene een bepaald gebruik van zijn of haar goodwill en reputatie past in het patroon van normen, waarden en handelswijze bij het leven van de overledene. De hier geformuleerde zorgvuldigheidsnormen brengen mee dat de nabestaanden om instemming moeten worden gevraagd voor het gebruik van de naam van de overledene'.

E-mails van overledenen

Voor onder andere erfgenamen kan het van belang zijn e-mails van overledenen in te zien. Voorstelbaar is dat de overledene of degene met wie de overledene heeft gecommuniceerd niet de intentie hebben gehad dat hun e-mailverkeer openbaar wordt gemaakt. Hoe hier in de praktijk mee wordt omgegaan, is in de regel afhankelijk van de algemene voorwaarden van de aanbieder van de online-e-maildienst. Bij geschillen over inzage in de e-mails van de overledene zal in de regel geen beroep kunnen worden gedaan op de AVG omdat alleen een betrokkene recht op inzage heeft (artikel 15 AVG). Voorstelbaar is dat wel een beroep mogelijk is op het erfrecht en het EVRM. Heeft de gevraagde informatie niet alleen betrekking op persoonsgegevens van de overledene maar ook op die van anderen, dan dient ook met hun belangen rekening te worden gehouden. Dit kan door hen bijvoorbeeld de informatie te verstrekken die alleen op hen betrekking heeft. Deze conclusie vloeit voort uit de overweging van de Hoge Raad in ECLI:NL:HR:2007:AZ4663 (*Dexia*) waarin onder meer werd ingegaan op de vraag wat moet worden verstaan onder het recht van een betrokkene op 'volledige inzage'. Dat inzagerecht moet volgens de Hoge Raad ruim wor-

© Noordhoff Uitgevers bv

den uitgelegd. Daarbij kan echter wel rekening gehouden worden met de rechten van derden. De Hoge Raad formuleert dit als volgt:

> 'Wel kan Dexia bij het verstekken van de gegevens rekening houden met de belangen van derden, zij het dat dit op proportionele wijze dient te geschieden. Zo kunnen bij de verstrekking van kopieën van bescheiden bijvoorbeeld daarin aanwezige passages die betrekking hebben op derden worden afgeschermd, indien de belangen van die derden zulks vergen.'

Gaat het om inzage in de mailbox van een overleden werknemer, dan ligt de zaak anders. Zakelijke correspondentie van de overledene kan door de werkgever vertrouwelijk worden ingezien. Verdedigbaar is dat in dat geval het belang van de werkgever zwaarder moet wegen dan de rechten van de overledene. Aangenomen mag worden dat de zakelijke correspondentie die door de overledene is gevoerd in het belang van de werkgever was en namens die werkgever. Tegen die achtergrond is het niet bezwaarlijk als de werkgever inzage krijgt in de zakelijke correspondentie. Normaliter zou die informatie bij leven van de werknemer op enig moment ook met de werkgever zijn gedeeld. In overweging 63 AVG wordt over het inzagerecht van een betrokkene het volgende opgemerkt:

> '(...) Elke betrokkene dient dan ook het recht te hebben, te weten en te worden meegedeeld voor welke doeleinden de persoonsgegevens worden verwerkt (...). Dat recht mag geen afbreuk doen aan de rechten van anderen, met inbegrip van het zakengeheim of de intellectuele eigendom en met name aan het auteursrecht dat de software beschermt. Die overwegingen mogen er echter niet toe leiden dat de betrokken alle informatie wordt onthouden. (...).'

1.5 Bescherming persoonlijke levenssfeer in de praktijk

Als burgers menen dat hun persoonlijke levenssfeer wordt geschonden, kunnen zij zich tot de rechter wenden. Als zij dat doen, is dat om de onrechtmatigheid van de inbreuk door de rechter te laten vaststellen en om verdere inbreuken op hun persoonlijke levenssfeer te voorkomen. Soms wordt ook om schadevergoeding verzocht. Dat gebeurt in de regel op grond van artikel 6:106 of 6:162 BW. Sinds de invoering van de AVG kan dit ook op grond van artikel 82 AVG.
De situaties waarin de inbreuken op de persoonlijke levenssfeer plaatsvinden, zijn zeer verschillend. Wordt er geprocedeerd over een inbreuk op de persoonlijke levenssfeer, dan wordt het recht op privacy van de klagende burger door de rechter afgewogen tegen de rechten van anderen. Een aantal voorbeelden.

1.5.1 Botsing grondrechten

Volgens overweging 4 AVG moet de verwerking van persoonsgegevens ten dienste staan van de mens.

> 'Het recht op bescherming van persoonsgegevens heeft geen absolute werking, maar moet worden beschouwd in relatie tot de functie ervan in de samenleving en moet conform het evenredigheidsbeginsel tegen andere grondrechten worden afgewogen.'

© Noordhoff Uitgevers bv

Wordt er door bekende personen geprocedeerd over inbreuken op de persoonlijke levenssfeer, dan is een informatiemedium vaak de gedaagde partij. In de rechtszaal is er in dat geval al snel sprake van botsing van grondrechten. Welk recht moet het zwaarst wegen: het recht op eerbiediging van de persoonlijke levenssfeer of het recht op vrije meningsuiting? Volgens de Hoge Raad in ECLI:NL:HR:2013:851 (*publicatie portret verdachte*) moet per geval worden bekeken welk recht moet wijken als er sprake is van een botsing van grondrechten. In de betreffende zaak publiceerde dagblad *Het Parool* een herkenbare foto van iemand die verdacht werd van een moord. De verdachte had bezwaar tegen het publiceren van de foto, meende dat hierdoor zijn persoonlijke levenssfeer werd geschonden en eiste een immateriele schadevergoeding. Als verweer voerde *Het Parool* haar (grondwettelijk) recht op vrije meningsuiting aan en het feit dat de verdachte in het verleden aan diverse uitzendingen in de media had meegewerkt. Dit verweer hielp *Het Parool* niet. Het recht op vrije meningsuiting van *Het Parool* moest van de rechter wijken voor het recht op privacy van de verdachte. De verdachte was geen publiek figuur en toen hij meewerkte aan de uitzendingen in de media was hij nog geen verdachte van een moord. *Het Parool* kon zich daar volgens de rechter dan ook niet op beroepen. Aan de verdachte werd een schadevergoeding toegekend omdat zijn persoonlijke levenssfeer was geschonden.

Anders dan in de zaak van *Het Parool* liep het in ECLI:NL:HR:2013:CA2788 (*Johan Cruijff vs. Tirion*) af met Johan Cruijff. Ook in die zaak ging het om de vraag welk grondrecht moest wijken: het recht op privacy van Cruijff of het recht op vrije meningsuiting van een uitgever. Deze wilde een fotoboek over Cruijff uitgeven over zijn jaren als voetballer. Het recht op privacy van Cruijff moest in dit geval wijken voor het recht op vrije meningsuiting van de uitgever. De Hoge Raad ging in deze zaak onder meer in op inbreuken op de persoonlijke levenssfeer van bekende personen en merkte daar het volgende over op:

> '(….) een geportretteerde zich kan verzetten tegen het zonder zijn toestemming openbaar maken van zijn (niet in opdracht vervaardigd) portret voor zover hij daarbij een redelijk belang heeft waarvoor het recht van meningsuiting en informatievrijheid in de gegeven omstandigheden moet wijken. In een zodanig geval is openbaarmaking van het portret in beginsel onrechtmatig en geldt als uitgangspunt dat publicatie kan worden verboden. Niet geldt als uitgangspunt dat voor openbaarmaking steeds voorafgaande toestemming van de geportretteerde is vereist. (…….) het portretrecht is een persoonlijkheidsrecht waaraan in de regel een zwaarwegend gewicht zal toekomen. Dit geldt vooral ten aanzien van geportretteerden die geen publieke bekendheid genieten, in die zin dat zij openbaarmaking van hun portret in beginsel niet behoeven te dulden. Ten aanzien van personen die door hun beroepsuitoefening bekendheid genieten, geldt evenwel dat de openbaarmaking van foto's die deze beroepsuitoefening betreffen en zijn gemaakt in voor het algemeen publiek toegankelijke plaatsen, tot op zekere hoogte inherent is aan hun beroepsuitoefening en de daarmee gemoeide bekendheid en belangstelling van het publiek. Indien de openbaarmaking de beroepsuitoefening van een daardoor bekende geportretteerde betreft, komt derhalve in de regel groot gewicht toe aan factoren als algemene nieuwswaarde en informatie aan het publiek in verhouding tot diens enkele verzet tegen openbaarmaking (….)'.

© Noordhoff Uitgevers bv

Conclusie van het vorenstaande is dat als men een bekend persoon is – en daar zelf ook aan heeft bijgedragen – men soms (enige) inbreuken op de persoonlijke levenssfeer voor lief zal moeten nemen. Het is de prijs van de bekendheid.

1.5.2 Privacy en arbeidsrelaties

Naarmate mensen meer met elkaar te maken hebben, zal het risico op inbreuken op de persoonlijke levenssfeer toenemen. Dat er in arbeidsrelaties regelmatig – al dan niet opzettelijke – inbreuken op de persoonlijke levenssfeer voorkomen, verbaast daarom niet. Hoofdregel is dat een goed werkgever de persoonlijke levenssfeer van werknemers respecteert. Van die hoofdregel kan echter worden afgeweken als er voor de werkgever redelijke en objectieve redenen zijn om – al dan niet tijdelijk – in te breken op de persoonlijke levenssfeer van werknemers of die te beperken. Een werkgever die zonder zwaarwegende argumenten de privacy van werknemers schendt, pleegt wanprestatie.
Voorbeelden van situaties waarbij zich inbreuken op de persoonlijke levenssfeer kunnen voordoen zijn:

Sollicitaties
Alvorens iemand in dienst te nemen, willen werkgevers weten of degene die solliciteert geschikt is voor de functie. Dit betekent dat er informatie over de sollicitant wordt verzameld. In dat verband wordt ook vaak op het internet naar informatie gezocht. Dat is toegestaan als de sollicitant daarover tevoren wordt geïnformeerd. Bedacht moet worden dat informatie op het internet niet altijd betrouwbaar is en soms ook sterk verouderd. Tegen die achtergrond is het onjuist om op basis van die informatie iemand te selecteren. Vindt de werkgever op het internet berichten over de sollicitant die relevant zijn, dan moet de werkgever dit de sollicitant melden en hem of haar de gelegenheid geven hierop te reageren.
Een werkgever mag een sollicitant niet vragen naar zijn of haar gezondheid. Wel is het zo dat als een sollicitant tijdens een sollicitatiegesprek een ziekte verzwijgt en dat na indiensttreding duidelijk wordt, dit voor de werkgever aanleiding kan zijn de arbeidsrelatie te beëindigen.

Screening

In sommige gevallen worden sollicitanten gescreend. Dit gebeurt door referenties op te vragen of door een uitgebreider onderzoek in te stellen. De sollicitant moet hier tevoren over worden geïnformeerd. Is er sprake van een uitgebreid onderzoek, dan kan ook gekeken worden naar de financiële en gezinssituatie van de sollicitant. Afhankelijk van de functie kan deze informatie voor de werkgever relevant zijn. Zo is het voorstelbaar dat als men solliciteert naar een leidinggevende financiële functie, de sollicitant te maken krijgt met een screening waarbij ook gekeken wordt naar de situatie in de persoonlijke levenssfeer en naar zaken met betrekking tot integriteit.
De gegevens van afgewezen sollicitanten moeten worden vernietigd.

© Noordhoff Uitgevers bv

Kledingvoorschriften
Als een werkgever in de bouw de werknemers verplicht op de bouwplaats een helm te dragen, is dat geen aantasting van de persoonlijke levenssfeer. Het dragen van een helm is een veiligheidsmaatregel en een goed werkgever is verplicht te zorgen voor de veiligheid van zijn personeel. Ook de arts die in het ziekenhuis een witte jas draagt, zal dit in de regel niet ervaren als een inbreuk op de persoonlijke levenssfeer. Het is nu eenmaal gebruikelijk dat artsen in een ziekenhuis witte kleding dragen. Anders lag dit voor een stewardess bij KLM in ECLI:NL:RBHAA:2010:BO2066 (*niet voldoen aan kledingvoorschriften*). Haar arbeidsovereenkomst werd door de rechter ontbonden omdat zij – in strijd met de kledingvoorschriften van KLM – zichtbare tatoeages had, te veel ringen, piercings en te kort haar. Dat uiterlijk paste niet bij de uitstraling die KLM tegenover het publiek wilde hebben en was om die reden verboden. De rechter oordeelde dat een werkgever bevoegd is voorschriften te geven over het uiterlijk van het personeel. Deze bevoegdheid is wel aan grenzen gebonden, namelijk de eisen van redelijkheid en billijkheid. De rechter erkende dat door het verbod van KLM een zekere inbreuk wordt gemaakt op de vrijheid die een werknemer heeft om zelf voor een bepaald uiterlijk te kiezen, maar die inbreuk oordeelde de rechter in dit geval niet in strijd met de eisen van redelijkheid en billijkheid. Wie kiest voor het beroep van stewardess, accepteert daarmee ook dat tijdens het werk een uniform moet worden gedragen en dat strenge regels aan het uiterlijk worden gesteld.

Neutrale uitstraling bedrijf

Is het voor een bedrijf belangrijk om neutraliteit uit te stralen, dan kan het bedrijf een beleid voeren waarin het werknemers verboden wordt zichtbare tekenen van politieke, filosofische of religieuze overtuigingen te dragen. Dit concludeerde het HvJ EU in ECLI:EU:C:2017:203 (*Achbita*) in antwoord op een prejudiciële vraag van het Belgische Hof van Cassatie. De zaak had betrekking op een receptioniste die haar werkgever meedeelde het voornemen te hebben tijdens werkuren de islamitische hoofddoek te dragen. Omdat zij bij haar voornemen bleef, werd zij ontslagen. De wens van de werkgever om naar klanten neutraliteit uit te stralen, houdt volgens het Hof verband met de vrijheid van ondernemerschap die in artikel 16 van het EU-Grondrechtenhandvest wordt erkend. Van directe discriminatie was geen sprake. Het verbod mag volgens het Hof echter niet verdergaan dan strikt noodzakelijk is. Dit kan betekenen dat als het verbod ook geldt voor werknemers die geen contact met klanten onderhouden, er sprake kan zijn van indirecte discriminatie.

Nevenactiviteiten
Wat een werknemer in zijn of haar vrije tijd doet, behoort tot de persoonlijke levenssfeer van de werknemer. Een werkgever heeft daar niets mee te maken. Dit wordt anders in het geval dat – als gevolg van nevenactiviteiten – het werk van de werknemer bij de werkgever eronder gaat leiden of als de nevenactiviteiten concurrerend of schadelijk voor de werkgever zijn. Zo werd in ECLI:NL:RBLIM:2017:782 (*ontdekking niet toegestane nevenactivitei-*

© Noordhoff Uitgevers bv

ten) een glazenwasser die bij een glazenwasserij werkte op staande voet ontslagen nadat de werkgever via Facebook had ontdekt dat de werknemer een eigen glazenwasserij was gestart. De werknemer had de werkgever niet om toestemming gevraagd en in zijn arbeidsovereenkomst was het verbod opgenomen om (gelijksoortige) werkzaamheden te verrichten. In ECLI:NL:RBARN:2012:BV9483 (*belediging werkgever*) werd de arbeidsovereenkomst van een medewerker van Blokker door de rechter ontbonden. De medewerker had zich op Facebook zeer beledigend uitgelaten over de werkgever. De rechter meende dat deze uitlating niets te maken had met de vrijheid van meningsuiting. Het feit dat de werknemer excuses had aangeboden en het beledigende bericht had verwijderd, was volgens de rechter 'mosterd na de maaltijd'. Het standpunt van de werknemer dat Facebook tot het privédomein van de werknemer behoort, deelde de rechter niet, omdat dit begrip bij Facebook betrekkelijk is en dat geldt volgens de rechter ook voor het begrip 'vrienden'. Een ontslagvergoeding werd niet toegekend.

Uit de voornoemde uitspraken kan worden geconcludeerd dat – anders dan vaak wordt gedacht – uitingen op Facebook niet in alle gevallen tot het privédomein van de werknemer worden gerekend.

Cameratoezicht

Werkgevers controleren het werk van werknemers. Dat is logisch, want kenmerk van een arbeidsovereenkomst is de gezagsverhouding tussen werkgever en werknemer (artikel 7:660 BW). Een werkgever is bevoegd te controleren of dat wat is opgedragen ook juist wordt uitgevoerd. Ten behoeve van die controlerende taak plaatsen werkgevers op de werkvloer soms camera's. Zij mogen dit alleen doen als dit noodzakelijk is. De persoonlijke levenssfeer van werknemers hoeft – ook op de werkvloer – niet onnodig beperkt te worden. Wil een werkgever camera's plaatsen, dan moet worden voldaan aan de eisen die de AP daaraan stelt. Dit betekent onder meer dat de werknemers over het gebruik van de camera's vooraf moeten worden geïnformeerd en ook waarom dit gebeurt. Daarnaast moeten er afspraken worden gemaakt over de bewaartermijn van de beelden en de mogelijkheid de beelden te bekijken. Camera's in bijvoorbeeld douches of toiletten zijn niet toegestaan. Het is een te grote inbreuk op de persoonlijke levenssfeer. Dit betekent niet dat een werkgever ruimtes voor de privacy van de werknemer nooit zou mogen betreden; dat mag als daar zwaarwegende argumenten voor zijn. Het gebruik van verborgen camera's waar medewerkers geen weet van hebben, is evenmin toegestaan. Zouden die beelden gebruikt worden om een bepaald gedrag van een werknemer aan te tonen, dan is dat onrechtmatig verkregen bewijs. Wat geldt voor camera's geldt ook voor geluidsopnames. Is bewijsmateriaal onrechtmatig verkregen, dan betekent dit niet dat een rechter daar in een procedure geen bewijskracht aan kan toekennen als het voldoende betrouwbaar is. Die situatie deed zich voor in de volgende zaak.

ECLI:NL:RBMNE:2017:6075 Controle met verborgen camera

Een werknemer werd wegens diefstal van goederen op staande voet ontslagen. Het bewijs van de diefstal kwam van een verborgen camera die de werkgever had geplaatst nadat hij vermoede dat er gestolen werd uit het magazijn. Vervolgens is door een recherchebureau in opdracht van de werkgever een onderzoek ingesteld. De werknemer heeft erkend goederen te hebben gestolen. Bij de rechter verweert de werknemer zich onder meer met het standpunt

© Noordhoff Uitgevers bv

dat het bewijs voor de diefstal door het gebruik van een verborgen camera onrechtmatig is verkregen en in strijd is met de Wbp. De rechter is het daar niet mee eens. Gelet op de concrete omstandigheden konden de camerabeelden als bewijs worden gebruikt.

Controle op e-mails en internetverkeer
Wat geldt voor het cameratoezicht, geldt in feite ook voor controle op e-mails en internetverkeer. Controle is toegestaan, mits voldaan wordt aan de eisen die de AVG daaraan stelt. De beperking van de persoonlijke levenssfeer moet voor de werkgever noodzakelijk zijn en de mate waarin dit gebeurt proportioneel. Voorstelbaar is dat de werkgever steekproefsgewijs het internetverkeer met speciale software laat onderzoeken. Zijn er reële vermoedens van misbruik, dan kan nader onderzoek worden ingesteld. In ECLI:NL:RBAMS:2017:6700 (*controle zoekgeschiedenis medewerker*) werd een werkneemster op staande voet ontslagen. Via de kassa van de winkel kon zij verbinding krijgen met het internet. Hierdoor verwaarloosde zij de klanten. Hoewel de werkgever haar herhaaldelijk had gewaarschuwd, bleef zij het internet stelselmatig onder werktijd gebruiken. Uit de door de werkgever bekeken zoekgeschiedenis op de kassa bleek dat de medewerkster ruim een half uur op het internet allerlei sites had bezocht. De rechter accepteerde het ontslag op staande voet. Een transactievergoeding werd niet toegekend.

Controle op alcohol, drugs en medicijnen
Gegevens over het gebruik van alcohol, drugs en medicijnen zijn gegevens die de persoonlijke levenssfeer van de werknemer raken. De werkgever heeft daar geen inzage in en werknemers hoeven er niet aan mee te werken als de werkgever de werknemer op het gebruik van alcohol, drugs of medicijnen wil controleren. Dit is anders als die controle berust op een wettelijke bevoegdheid. Dit is geregeld in het Besluit alcohol, drugs en geneesmiddelen in het verkeer. Op basis van dat besluit mogen schippers, loodsen, piloten en spoorwegmachinisten onder bepaalde voorwaarden door opsporingsambtenaren worden gecontroleerd op het gebruik van alcohol, drugs en medicijnen. In andere gevallen is dat niet toegestaan. Op dit punt is de AP streng. Gebleken is dat werkgevers hier moeite mee hebben. Voor werkgevers kan het belangrijk zijn om – bijvoorbeeld uit veiligheidsoverwegingen – werknemers te mogen controleren op alcohol-, drugs- of medicijngebruik. Bij de behandeling van het wetsvoorstel UAVG is er door de Raad van State op gewezen dat artikel 9 en 88 AVG lidstaten de ruimte bieden om nadere regels vast te stellen die betrekking hebben op de verwerking van persoonsgegevens van werknemers in het kader van de arbeidsverhouding. In reactie hierop is door de regering gesteld dat – gegeven het beleidsneutrale karakter van de UAVG – er vooralsnog geen gebruik wordt gemaakt van de nieuwe mogelijkheid die de AVG biedt. De regering sluit echter niet uit dat dit in de toekomst anders zal zijn.

Controle zieke medewerkers
In ons arbeidsrecht is het niet aan de werkgevers om te bepalen of een zieke werknemer de bedongen arbeid kan verrichten. Het is de bedrijfsarts die daar een medisch oordeel over geeft en de werkgever vervolgens adviseert. In de praktijk schakelen werkgevers soms derden in om te controleren of de werknemer ziek is. Dit is een vergaande inbreuk in de persoonlijke levenssfeer van de werknemer. Een dergelijke inbreuk is alleen bij zeer

© Noordhoff Uitgevers bv

zwaarwegende omstandigheden verdedigbaar. Zijn die omstandigheden er niet of kan gekozen worden voor een alternatief met minder impact op de persoonlijke levenssfeer van de werknemer, dan is het niet toegestaan. Een voorbeeld.

ECLI:NL:RBROT:2017:434 Controle arbeidsongeschiktheid
Een werknemer met een fysieke functie was arbeidsongeschikt voor zijn werk bij een havenbedrijf. Samen met zijn echtgenote exploiteerde de werknemer een eigen botenverhuurbedrijf. De werkgever wist dit. Op enig moment ontvangt de werkgever anonieme signalen van derden die voor de werkgever aanleiding vormen om te twijfelen over de (mate van) arbeidsongeschiktheid van de werknemer. De werknemer zou in zijn eigen bedrijf bepaalde fysieke werkzaamheden verrichten op grond waarvan hij in staat moet worden geacht ook de bedongen arbeid bij het havenbedrijf te verrichten. Hierop schakelt de werkgever een bedrijfsrecherchebureau in om onderzoek te doen. Op basis van dit onderzoek verzoekt de werkgever de kantonrechter de arbeidsovereenkomst te ontbinden. Dit verzoek wordt afgewezen. De rechter neemt het de werkgever kwalijk in een geval als dit geen contact met de bedrijfsarts te hebben opgenomen, bijvoorbeeld om een herkeuring te vragen. Het inschakelen van het bedrijfsrecherchebureau – op basis van signalen van derden en zonder eerst nader onderzoek te doen – gaat de rechter te ver. Zo werd de werknemer en zijn gezin gedurende drie weken bijna dagelijks en ook in het weekend door twee medewerkers geobserveerd en daar werden camerabeelden van gemaakt. Dit had impact op de werknemer en zijn echtgenote en heeft bij hen gevoelens van onveiligheid losgemaakt. Omdat de werknemer geen vertrouwen meer had in zijn werkgever, werd de arbeidsovereenkomst op verzoek van de werknemer ontbonden. Aan de werknemer werd een vergoeding van €55.000 bruto toegekend.

Schending privacy door werknemer
Niet alleen werkgevers, maar ook werknemers behoren op het werk de persoonlijke levenssfeer van anderen te respecteren. Dat gebeurt niet altijd. Zo komt het in de praktijk regelmatig voor dat werknemers op hun laptop documenten van hun werk mee naar huis nemen om er verder aan te werken. Daar zijn privacyrisico's aan verbonden omdat de documenten persoonsgegevens kunnen bevatten. Zo blijkt onder meer uit het Jaarverslag 2018 van de AP dat er regelmatig laptops of usb-sticks met persoonsgegevens verloren of gestolen worden.
Kent een werkgever een (door werknemers gekend) privacybeleid, dan kan het voor de werknemer vervelende gevolgen hebben als die zich daar niet aan houdt. Zo werd in ECLI:NL:RBAMS:2015:5487 (*niet naleven privacybeleid*) een medewerkster van een ziekenhuis ontslagen omdat zij – in strijd met het privacybeleid van het ziekenhuis – medische gegevens van haar halfbroer had opgevraagd.

© Noordhoff Uitgevers bv

Vragen

1.1 Via het WOZ-waardeloket van het Kadaster (www.kadaster.nl) kan iedereen gratis nagaan hoeveel de WOZ-waarde van een woning bedraagt.

a Is de WOZ-waarde een persoonsgegeven? Motiveer.

b Tegen betaling van een vergoeding kan men bij het Kadaster ook informatie verkrijgen over de koopsom van een woning en de hypotheek die er eventueel op rust. Is deze informatie een persoonsgegeven? Motiveer.

c Hoe verhoudt de onder a en b bedoelde informatie zich met het recht op privacy van de burger?

1.2 Postcodes kunnen inzicht geven in de welvaart of demografische samenstelling van een bepaalde woonwijk. Er zijn bedrijven en organisaties die deze informatie gebruiken.

a Is een postcode een persoonsgegeven?

b Is een postcode informatie die de identiteit van een natuurlijk persoon kan vaststellen?

1.3 Het Handelsregister wordt bijgehouden door de Kamer van Koophandel (www.kvk.nl). Het is een openbaar register. Dit vloeit voort uit de Handelsregisterwet 2007 (Hrgw 2007).

a Welke persoonsgegevens zijn te vinden in het Handelsregister?

b Op welke wijze wordt in het Handelsregister rekening gehouden met de bescherming van persoonsgegevens?

1.4 Tijdens de officiële opening van het studiejaar wordt er een foto gemaakt van het aanwezige publiek. Het is de bedoeling de foto te publiceren in het blad van de universiteit. Op de foto is onder meer Jeroen te zien in een innige omhelzing met een vrouw die niet zijn vriendin of een familielid is.

a Is de foto een persoonsgegeven?

b Kan Jeroen het publiceren van de foto tegenhouden? Motiveer.

1.5 Een begrafenisonderneming wil de dienstverlening uitbreiden. In dat kader wordt aan de nabestaanden gevraagd of er een vingerafdruk van de overledene mag worden afgenomen. Die vingerdruk kan vervolgens verwerkt worden in een sieraad. De nabestaanden ontvangen op die manier een zeer persoonlijk aandenken van de overledene.

a Is een vingerafdruk een persoonsgegeven?

b Is wat de begrafenisonderneming aanbiedt, toegestaan op grond van de AVG?

c Is het toegestaan een foto van de overledene te maken en die te gebruiken in een rouwadvertentie?

© Noordhoff Uitgevers bv

1.6 Biedt artikel 91 AVG EU-lidstaten de mogelijkheid voor kerkgenootschappen uitzonderingen te maken met betrekking tot het gegevensbeschermingsrecht?

1.7 In 2019 heeft de Socialistische Partij tijdens de verkiezingen voor het Europees Parlement gebruikgemaakt van een filmpje waarin een acteur eurocommissaris Frans Timmermans speelt. De acteur lijkt sprekend op de eurocommissaris. In het filmpje – dat onder meer is te zien op YouTube – wordt kritiek geuit op het beleid van de EU. De acteur wordt in het filmpje Hans Brusselmans genoemd.

a Is de naam Hans Brusselmans in dit geval een persoonsgegeven?
b Is er sprake van een inbreuk op de privacy van Frans Timmermans? Motiveer.
c Is de AVG van toepassing?

1.8 Mevrouw Van Zwieten wil haar borsten laten verkleinen. Zij geeft aan na de operatie alleen in een kamer te willen liggen om te herstellen. Vóór en na de operatie worden er door de kliniek foto's gemaakt van de borsten van mevrouw Van Zwieten. De kliniek wil deze foto's voor marketingdoeleinden in een brochure opnemen.

a Hoe wordt in het recht de wens van mevrouw Van Zwieten omschreven om alleen in een kamer te liggen?
b Zijn de foto's van de borsten van mevrouw Van Zwieten persoonsgegevens? Motiveer.

1.9 Het BIG-register (BIG staat voor: beroepen in de individuele gezondheidszorg) is een openbaar register (www.bigregister.nl).

a Welke beroepen staan daarin vermeld?
b Is een beroep een persoonsgegeven in de zin van de AVG? Motiveer.
c Welke persoonsgegevens zijn te vinden in het BIG-register?

1.10 In een parkeergarage worden genummerde parkeerplaatsen verhuurd aan bedrijven en particulieren. Om een parkeerplaats te huren, wordt een huurcontract getekend waarin de naam en het adres van de huurder worden vermeld. In de parkeergarage hangt een lijst met nummers van parkeerplaatsen die verhuurd of nog niet verhuurd zijn.

a Is het nummer van een parkeerplaats een persoonsgegeven?
b Is in dit geval het kentekennummer van een auto een persoonsgegeven?

1.11 Bij het verlaten van de winkel controleert een medewerker van de beveiliging de inhoud van de tassen van de werknemers.

a Is er sprake van een inbreuk op de persoonlijke levenssfeer van de werknemers? Motiveer.
b Is de tassencontrole toegestaan op grond van de AVG? Motiveer.

© Noordhoff Uitgevers bv