De bescherming van persoonsgegevens
Acht Europese landen vergeleken

De bescherming van persoonsgegevens

Acht Europese landen vergeleken

Bart Custers (eindredactie)
Francien Dechesne
Ilina Georgieva
Simone van der Hof

Met medewerking van:
Alan M. Sears
Tommaso Tani

Sdu Uitgevers
Den Haag, 2017

Omslagontwerp: Villa Y

ISBN: 9789012400862

Sdu Uitgevers
Postbus 20025, 2500 EA Den Haag, tel. (070) 378 99 11
Nadere informatie over de uitgaven van Sdu Uitgevers vindt u op www.sdu.nl.

Inhoudsopgave

Samenvatting

Aanleiding en vraagstelling

De bescherming van persoonsgegevens wordt in de Europese Unie in belangrijke mate bepaald door wetgeving. De EU-richtlijn voor de bescherming van persoonsgegevens (richtlijn 95/46/EC), geldig tot 25 mei 2018 en de Algemene Verordening Gegevensbescherming van de EU (verordening 2016/679), geldig vanaf 25 mei 2018, bepalen de kaders voor rechten en plichten van enerzijds personen wier gegevens worden verzameld en verwerkt en anderzijds van personen, bedrijven en overheidsinstellingen die de persoonsgegevens verzamelen en verwerken. Hoe de feitelijke bescherming eruitziet is echter niet alleen afhankelijk van de wettelijke kaders, maar ook van de verdere invulling en interpretatie die daaraan wordt gegeven en de wijze waarop handhaving plaatsvindt. De wet- en regelgeving op het gebied van privacy en de bescherming van persoonsgegevens kent veel open normen. Als gevolg van verschillen in wetgevingsstelsels en culturele verschillen is de richtlijn voor de bescherming van persoonsgegevens in EU-lidstaten op verschillende manieren geïmplementeerd. Als gevolg van de open normen, in combinatie met culturele verschillen, wordt ook op verschillende manieren aan de wet- en regelgeving uitvoering gegeven. Hoewel de Algemene Verordening Gegevensbescherming dit verder zal harmoniseren, is het te verwachten dat in de praktijk verschillen blijven bestaan.

De verschillen in de mate van bescherming van persoonsgegevens roept de vraag op in welk land persoonsgegevens (en daarmee een belangrijk deel van iemands privacy) het beste zijn beschermd en hoe goed de bescherming van persoonsgegevens in Nederland is geregeld in vergelijking met andere landen. Is Nederland een achterhoedespeler, een middenmoter of een koploper op het vlak van privacybescherming? Een antwoord op deze vraag maakt het bovendien mogelijk aanvullende maatregelen ter bescherming van privacy en persoonsgegevens te nemen, als mocht blijken dat die bescherming in Nederland achterblijft bij andere EU-lidstaten. Dit leidt tot de centrale vraagstelling van dit onderzoek:

Wat is de positie van Nederland met betrekking tot de bescherming van de persoonsgegevens van de burgers in vergelijking met enkele andere landen binnen de Europese Unie?

Om te komen tot een antwoord op deze vraag zijn zes deelvragen geformuleerd:

1. Wat is de algemene situatie rondom de bescherming van persoonsgegevens?
2. Welk beleid wordt er vanuit de nationale overheid gevoerd om persoonsgegevens te beschermen?

3. Welke wet- en regelgeving is van toepassing op de bescherming van persoonsgegevens?
4. Op welke wijze zijn wetgeving en beleid op het terrein van bescherming van persoonsgegevens in de praktijk vormgegeven?
5. Hoe zijn toezicht en handhaving bij bescherming van persoonsgegevens georganiseerd?
6. Wanneer de acht onderzochte landen met elkaar worden vergeleken op bovengenoemde aspecten, wat is dan de positie van Nederland?

In dit onderzoek ligt de nadruk op de bescherming van persoonsgegevens (informationele privacy) en niet op de bescherming van privacy in brede zin. Hoewel een aanzienlijk deel van de onderzoeksvragen juridisch van aard is, is dit geen juridisch-dogmatisch of rechtspositivistisch onderzoek. De nadruk ligt veel meer op de vraag hoe de bescherming van persoonsgegevens voor burgers in de praktijk is vormgegeven en door burgers wordt beleefd. Uit eerder onderzoek blijkt namelijk dat de privacybeleving van burgers niet altijd overeenkomt met de doelstellingen van wet- en regelgeving. In dit onderzoek wordt geen normatief oordeel gegeven over waar Nederland zich zou moeten bevinden in de vergelijking met andere Europese landen, maar worden wel aanknopingspunten geboden hoe Nederland op bepaalde aspecten zou kunnen opschuiven in een bepaalde richting.

Methodologie

Bij een internationale vergelijking is ten eerste een keuze nodig op welke aspecten (de bescherming van persoonsgegevens) wordt vergeleken en is ten tweede een keuze nodig in de landen waarmee wordt vergeleken.

Vergelijkingsaspecten

Op basis van vooronderzoek is gekozen de bescherming van persoonsgegevens te vergelijking op vijf aspecten, weergegeven in de eerste vijf voornoemde deelvragen. De vergelijkingsaspecten zijn (1) de algemene situatie, (2) beleid, (3) wet- en regelgeving, (4) implementatie, en (5) toezicht en handhaving. Voor elk onderzocht land is middels deskresearch, een uitgebreide vragenlijst en expertbevragingen informatie verzameld op deze aspecten. Middels deskresearch zijn beschikbare literatuur en online gegevens (bijvoorbeeld websites en jaarverslagen van toezichthouders, overheden en burgerrechtenorganisaties) geraadpleegd. In dit onderzoek is geen survey gehouden onder EU-burgers, maar wel is aan de hand van secundaire analyses op en/of hergebruik van bestaande surveys (waaronder de CONSENT Survey, de Eurobarometer en de Oxford Internet Survey) informatie verzameld en de expertbevraging verrijkt. Informatie die niet beschikbaar was via deskresearch is via een uitgebreide vragenlijst uitgezet bij experts in de betreffende landen. Daarnaast is contact opgenomen met (medewerkers van) de toezichthoudende instanties op het gebied van privacy en gegevensbescherming in verschillende landen. Deze experts en toezichthouders hebben niet de integrale vragenlijst toegestuurd gekregen, maar slechts die vragen die niet of onvoldoende konden worden beantwoord middels deskresearch. Op aspecten waar na deskresearch en expertbevraging nog steeds weinig of geen informatie beschikbaar bleek voor bepaalde

landen, zijn de resultaten aangevuld met (nader) literatuuronderzoek, (nadere) media-analyses en aanvullende interviews. Voor aanvullende interviews zijn experts op het gebied van bescherming van persoonsgegevens, beleidsmakers, bedrijven die persoonsgegevens verwerken, toezichthouders en belangenorganisaties benaderd.
Uiteindelijk is het verzamelde materiaal geclusterd in 23 categorieën (labels). Voor de algemene situatie zijn dit internetgebruik, (gevoel van) controle, bewustzijn, vertrouwen, beschermingsmaatregelen, nationale politiek, media-aandacht, datalekken en burgerrechtenorganisaties. Voor beleid zijn dit nationaal beleid & Privacy Impact Assessments, privacy & bescherming van persoonsgegevens in beleid, maatschappelijk debat en informatiecampagnes. Voor wet- en regelgeving zijn dit implementatie van de EU-richtlijn, sectorale wetgeving en zelfregulering & gedragscodes. Voor implementatie zijn dit privacyfunctionarissen, beveiligingsmaatregelen en transparantie. Voor toezicht en handhaving zijn dit toezichthouders, taken & bevoegdheden, gebruik van bevoegdheden en reputatie.

Landenselectie
In dit onderzoek staat de positie van Nederland centraal. Daarnaast zijn de volgende landen in dit onderzoek betrokken: Duitsland, Zweden, het Verenigd Koninkrijk, Ierland, Frankrijk, Roemenië en Italië. Deze landen zijn geselecteerd opdat een spreiding aanwezig is op verschillende selectiecriteria. Daarbij gaat het om een strenge/soepele houding ten opzichte van privacybescherming, een vergelijkbare dan wel andere benadering van gegevensbescherming dan Nederland (culturele dimensies, rechtssysteem en monistische/dualistische benadering van internationaal recht), maturiteit op het gebied van privacybescherming (historie, met name toetreding tot de EU) en geografische spreiding (noord-zuid en oost-west). In totaal zijn voor acht Europese landen de vergelijkingsaspecten in kaart gebracht. Daarna zijn per vergelijkingsaspect alle landen vergeleken en is vastgesteld wat de positie van Nederland is ten opzichte van de andere landen.

Resultaten en conclusies
Wanneer de positie van Nederland wordt vergeleken met de andere onderzochte landen, kunnen de volgende conclusies worden getrokken:
- Nederlanders vertonen (m.b.t. de bescherming van hun persoonsgegevens) een hoge mate van bewustzijn en zelfredzaamheid. Tegelijkertijd is er een lage bezorgdheid/hoge mate van acceptatie en berusting.
- In Nederland is ruime aandacht voor de bescherming van persoonsgegevens in het politieke debat en in de media.
- Nederland loopt (met Duitsland) voorop met de meldplicht datalekken.
- De budgetten, invloed en bekendheid van burgerrechtenorganisaties in Nederland zijn beperkt.
- Nederland behoort tot de koplopers wat betreft Privacy Impact Assessments, maatschappelijk debat en informatiecampagnes.
- Op het gebied van wet- en regelgeving zijn de verschillen tussen de onderzochte landen niet groot.

- Het aantal privacyfunctionarissen lijkt in Nederland achter te blijven in vergelijking met andere landen.
- Voor de beveiliging van persoonsgegevens zijn er wel richtlijnen in Nederland, maar de toezichthouder biedt geen certificering of keurmerk zoals in andere landen.
- Transparantie is in alle onderzochte landen laag.
- Het budget en het aantal medewerkers van de Nederlandse toezichthouder loopt in de pas met andere landen.
- Boetebevoegdheden van de Nederlandse toezichthouder lopen Europees gezien in de pas.
- De Autoriteit Persoonsgegevens onderhoudt (op individueel niveau) nauwelijks een dialoog met degenen op wie toezicht wordt gehouden en doet nauwelijks aan klachten behandelen.
- De Nederlandse toezichthouder is goed bekend bij burgers.

Wanneer deze conclusies bij elkaar worden opgeteld, kan gesteld worden dat Nederland het goed doet als het gaat om de bescherming van persoonsgegevens. Binnen de groep met landen die in dit onderzoek zijn vergeleken, kan gesteld worden dat Duitsland in de meeste opzichten koploper is en dat met name Italië en Roemenië zich aan het andere uiteinde van het spectrum bevinden. Nederland doet het in de meeste opzichten bovengemiddeld goed. Zo is het goed gesteld met het bewustzijn en de zelfredzaamheid van Nederlanders, is er ruime aandacht voor de bescherming van persoonsgegevens in het politieke debat en de media, loopt Nederland voorop met de meldplicht datalekken, Privacy Impact Assessments, maatschappelijk debat en informatiecampagnes, lopen budgetten, aantallen medewerkers en boetebevoegdheden van toezichthouders goed in de pas en is de Nederlandse toezichthouder goed bekend bij burgers.
Ruimte voor verbetering in Nederland is mogelijk als het gaat om de budgetten, invloed en bekendheid van burgerrechtenorganisaties, het aantal privacyfunctionarissen in organisaties, certificering/keurmerken voor de beveiliging van persoonsgegevens, transparantie, klachtenafhandeling, dialoog tussen enerzijds toezichthouder en anderzijds degenen onder toezicht en burgerrechtenorganisaties. Daarbij dient echter te worden aangetekend dat transparantie in alle onderzochte landen laag is, dat de aankomende Algemene Verordening Gegevensbescherming (AVG) een aantal zaken zal verstevigen en dat door de Nederlandse overheden op allerlei andere onderwerpen reeds (verdere) verbeteringen in gang zijn gezet. Dit laatste bevestigt het proactieve optreden van Nederlandse overheden op het terrein van privacy en de bescherming van persoonsgegevens. Door deze opstelling is Nederland goed voorbereid op de Algemene Verordening Gegevensbescherming en is het aannemelijk dat Nederland ook in de toekomst (met name technologische) ontwikkelingen die gevolgen kunnen hebben voor de bescherming van persoonsgegevens goed zal weten te adresseren.

1. Inleiding

1.1 Aanleiding

Nederlanders maken zich steeds meer zorgen om hun privacy, blijkt uit peilingen.[1] Dit is onderdeel van een wereldwijde trend: overal maken mensen zich in toenemende mate zorgen om hun online privacy.[2] Verklaringen daarvoor zijn mogelijk te vinden in de technologische ontwikkelingen, waarbij steeds meer mensen steeds meer transacties online verrichten en in toenemende mate actief zijn op sociale media. Mensen geven aan weinig zicht te hebben op wie hun gegevens verwerkt en voor welke doeleinden.[3] Ook hebben ze het gevoel weinig controle te hebben over hun gegevens.[4] Omdat de technologische ontwikkelingen niet op nationaal maar op internationaal niveau plaatsvinden, heeft de EU al in 1995 de bescherming van persoonsgegevens geharmoniseerd via een Europese richtlijn, de zogeheten Data Protection Directive.[5] Deze richtlijn voorziet in spelregels voor het verwerken van persoonsgegevens. Europese richtlijnen moeten worden omgezet in nationale wetgeving binnen een bepaalde termijn, in dit geval drie jaar. Vijf landen, waaronder Nederland, hebben deze implementatietermijn niet gehaald.[6] Pas in 2001 werd in Nederland de richtlijn geïmplementeerd via de Wet bescherming persoonsgegevens (Wbp).
Omdat de richtlijn dateert van de periode waarin sociale media nog niet of nauwelijks bestonden (bijvoorbeeld Facebook is opgericht in 2004 en Twitter in 2006), leek de richtlijn inmiddels op onderdelen achterhaald. In een poging de bescherming van persoonsgegevens voor EU-burgers verder te bevorderen, kwam de EU in 2012 met

1 IPSOS (2014) Nederlander minder onverschillig over privacy, 11 maart 2014. http://site.ipsos-nederland.nl/politiekebarometer/Berichten/PersBericht_1264_Nederlander_minder_onverschillig_over_privacy.html.

2 Keulen, E. van (2016) Zorgen om privacy (infographic), 10 juni 2016. http://www.emerce.nl/research/zorgen-om-privacy.

3 Slechts 2 op de 10 EU-burgers geven aan geïnformeerd te zijn over welke gegevens over hen worden verzameld en wat daarmee gebeurt. Eurobarometer 431 (2015).

4 Slecht 15% van de EU-burgers geeft aan volledige controle te voelen over gegevens die ze online afstaan. 31% daarentegen geeft aan het gevoel te hebben helemaal geen controle hierover te hebben. 50% geeft aan gedeeltelijk controle te hebben hierover. Twee derde geeft aan zich zorgen te maken over het gebrek aan controle over hun persoonsgegevens. Eurobarometer 431 (2015).

5 Voluit: Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data European. Zie: Directive 95/46/EC of the European Parliament and the Council of 24th October 1995, *Pb*. L281/31, 23rd November 1995.

6 De andere landen waren Frankrijk, Luxemburg, Duitsland en Ierland.

een voorstel voor nieuwe wetgeving naar buiten.[7] Na veel voorbereiding en debat werd uiteindelijk in april 2016 Verordening 2016/679 aangenomen, de Algemene Verordening Gegevensbescherming (AVG, of in het Engels: General Data Protection Regulation, GDPR).[8] Doordat de EU deze keer heeft gekozen voor een verordening (die rechtstreeks van toepassing is in alle lidstaten) in plaats van een richtlijn (die eerst in nationale wetgeving moet worden omgezet), is sprake van verdergaande harmonisering van de bescherming van persoonsgegevens. De verordening is vanaf 25 mei 2018 van toepassing, zodat burgers, bedrijven en overheden ruim de tijd krijgen zich voor te bereiden op de nieuwe spelregels en maatregelen kunnen nemen aan de nieuwe wetgeving te voldoen.
Wetgeving bepaalt in belangrijke mate in hoeverre burgers bescherming genieten. Op het vlak van de bescherming van persoonsgegevens geldt dit ook voor de richtlijn en de verordening. Deze bepalen de kaders voor rechten en plichten van enerzijds personen wier gegevens worden verzameld en verwerkt en anderzijds van bedrijven en overheidsinstellingen die de persoonsgegevens verzamelen en verwerken. Hoe de feitelijke bescherming eruitziet is echter niet alleen afhankelijk van de wettelijke kaders, maar ook van de verdere invulling en interpretatie die daaraan wordt gegeven en de wijze waarop handhaving plaatsvindt. De wet- en regelgeving op het gebied van privacy en de bescherming van persoonsgegevens kennen veel open normen.[9] Het voordeel hiervan is dat de regels langer bruikbaar blijven wanneer de technologie zich verder ontwikkelt en dat situaties, bijvoorbeeld in bepaalde sectoren, op maat kunnen worden beoordeeld en regels verder kunnen worden ingevuld en aangevuld.
Als gevolg van verschillen in wetgevingsstelsels en culturele verschillen is de richtlijn voor de bescherming van persoonsgegevens in EU-lidstaten op verschillende manieren geïmplementeerd. Als gevolg van de open normen, in combinatie met culturele verschillen, wordt ook op verschillende manieren aan de wet- en regelgeving uitvoering gegeven. In het ene land zijn de open normen veel verder ingevuld dan in het andere land. In sommige landen is de toezichthouder erg streng, in andere landen is er meer ruimte. Bepaalde landen richten zich op de minimale eisen die uit de regels voorvloeien, terwijl andere landen aanvullende regels opstellen.
In hun boek *Privacy on the Ground* vergelijken de Amerikaanse professoren Kenneth Bamberger en Deirdre Mulligan de verschillende manieren waarop landen invulling geven aan de regels voor de bescherming van privacy en de bescherming van persoonsgegevens.[10] Zij vergelijken Duitsland, Spanje, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten. Uit die vergelijking komt naar voren dat in Spanje privacy en de

7 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

8 http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

9 Zie bijvoorbeeld de memorie van toelichting op de Wet bescherming persoonsgegevens. *Kamerstukken II*, vergaderjaar 1997-1998, 25 892, nr. 3.

10 Mulligan, D.K. and Bamberger, K.A. (2015), *Privacy on the Ground in the United States and Europe*, MIT Press. Zie ook UNCTAD (2016) Data protection regulations and international data flows: Implications for trade and development. United Nation Conference on Trade and Development (UNCTAD), New York: UN.

bescherming van persoonsgegevens vooral wordt gezien als juridische tekst en een administratieve last, terwijl in Frankrijk en Duitsland actief werk wordt gemaakt van de regels: bedrijven en overheidsinstellingen worden expliciet verantwoordelijk gemaakt voor privacy. In het Verenigd Koninkrijk wordt, net als in de Verenigde Staten, privacy vooral gezien als een aspect waarop bedrijven kunnen concurreren en hun vertrouwen kunnen vergroten. In Duitsland en de VS bleken privacyprofessionals de stevigste aanpak te hebben op het vlak van privacymanagement. Privacy is steeds meer een strategisch onderwerp voor organisaties, waarbij het om meer gaat dan het voldoen aan de regels (compliance): privacy wordt in toenemende mate gezien als een sociale waarde en verantwoordelijkheid.[11] Hoewel de aankomende AVG de bescherming van persoonsgegevens verder zal harmoniseren binnen de EU, kent ook deze veel open normen en is niet te verwachten dat culturele verschillen helemaal zullen verdwijnen. Bovendien biedt de AVG, net als de richtlijn, minimumnormen waaraan moet worden voldaan. Er is ruimte voor nadere invulling en extra bescherming als landen daarvoor kiezen.

De verschillen in de mate van bescherming roept de vraag op in welk land privacy het beste is beschermd. Deze vraag kwam ook op in het Nederlandse parlement. Tijdens de behandeling van de begroting van het ministerie van Veiligheid en Justitie op 26 november 2014 werd in de Tweede Kamer door de leden Schouw (D66) en Oosenbrug (PvdA) een motie ingediend.[12] In deze motie wordt de regering verzocht een onderzoek te laten uitvoeren naar de positie van Nederland met betrekking tot de bescherming van de privacy van de burgers in objectieve vergelijking met andere landen binnen de Europese Unie. De kern van deze vraag is of Nederland een achterhoedespeler, een middenmoter of een koploper is op het vlak van privacybescherming. Impliciet lijkt ook in de vraag besloten te liggen dat Nederland mogelijk aanvullende maatregelen zou moeten nemen als mocht blijken dat de bescherming van privacy achterblijft van bij die in andere EU-lidstaten.

Deze motie uit 2014 is de directe aanleiding voor dit onderzoek. Het WODC, het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Veiligheid en Justitie, is gevraagd onderzoek te laten doen dat uitvoering geeft aan bovengenoemde motie. Om de reikwijdte van het onderzoek realistisch te houden, is daarbij de focus gelegd op de bescherming van persoonsgegevens en niet op (het recht op) privacy in den brede.[13] Teneinde te bevorderen dat het onderzoek tot een objectieve vergelijking leidt, heeft het WODC het onderzoek in twee delen geknipt. Eerst is een korte verkenning uitgevoerd naar indicatoren die bij de beoogde vergelijking kunnen worden gebruikt en naar een mogelijke selectie van landen die in het onderzoek zullen

11 Mulligan, D.K. and Bamberger, K.A. (2015), *Privacy on the Ground in the United States and Europe*, MIT Press. Zie ook Cannataci, J. (2016), Report of the Special Rapporteur on the right to privacy, 8 march 2016.

12 *Kamerstukken II* 2014-2015, 34 000 VI, nr. 50. Deze motie is op 27 november 2015 met een ruime meerderheid aangenomen.

13 Met andere woorden: de nadruk ligt dus op informationele privacy en niet op ruimtelijke, relationele of lichamelijke privacy. Zie Borking, J.J.F.M. (2010), *Privacyrecht is code. Over het gebruik van privacy enhancing technologies* (proefschrift, Universiteit Leiden). Deventer: Kluwer.

worden betrokken. Dit onderzoek is uitgevoerd door TNO en opgeleverd in 2015.[14] De resultaten van dit rapport van TNO zijn richtinggevend voor de opzet en uitvoering van het tweede deel (dit onderzoek). Het tweede deel betreft de eigenlijke vergelijking van een selectie van acht landen op de door TNO voorgestelde indicatoren met als doel een bepaling van de positie van Nederland in verhouding tot de andere landen. In opdracht van het WODC heeft eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden, dit tweede (deel van het) onderzoek uitgevoerd.[15] In dit rapport zijn de resultaten en bevindingen van dit onderzoek te lezen.
Dit hoofdstuk is verder als volgt opgebouwd. In paragraaf 1.2 worden de onderzoeksvragen uiteengezet. In paragraaf 1.3 wordt de onderzoeksaanpak beschreven. Daarbij wordt respectievelijk ingegaan op de afbakening, de landenselectie en de methodologie. In paragraaf 1.4 wordt de opbouw van dit rapport beschreven.

1.2 Onderzoeksvragen

De doelstelling van dit onderzoek is invulling te geven aan bovengenoemde motie. Volgens de indieners van deze motie is het van groot belang dat de bescherming van de privacy in Nederland op een hoog niveau staat en zou Nederland moeten streven om binnen de Europese Unie tot de koplopers te behoren waar het gaat om de bescherming van de privacy, aldus de tekst van de motie. Voor de indieners van de motie is evenwel onduidelijk waar Nederland op dit punt staat in vergelijking met andere landen binnen de Europese Unie. Om hierin meer duidelijkheid te krijgen, is onderzoek gewenst naar de positie van Nederland met betrekking tot de bescherming van de privacy van burgers in vergelijking tot andere landen binnen de Europese Unie.

Dit leidt tot de centrale vraagstelling van dit onderzoek:

Wat is de positie van Nederland met betrekking tot de bescherming van de persoonsgegevens van de burgers in vergelijking met enkele andere landen binnen de Europese Unie?

Om deze vraag te kunnen beantwoorden moeten enkele keuzes en praktische afbakeningen worden gemaakt. Allereerst wordt bij de bescherming van privacy, zoals hierboven reeds aangegeven, de nadruk gelegd op de bescherming van persoonsgegevens (informationele privacy). Ten tweede zijn keuzes nodig voor de aspecten waarop de bescherming van persoonsgegevens wordt vergeleken. Ten derde zijn keuzes nodig voor de landen waarmee wordt vergeleken.
Voor deze keuzes is het onderzoek van TNO (Roosendaal et al., 2015) richtinggevend geweest.[16] In het onderzoek van TNO is een raamwerk neergezet voor het bepalen van de relevante onderwerpen voor de vergelijking. Per onderwerp is een uitwerking gemaakt

14 Roosendaal, A., Ooms, M., Hoepman, J.H. (2015), *Een raamwerk van indicatoren voor de bescherming van persoonsgegevens. Nederland ten opzichte van andere landen*. Delft: TNO (WODC), 2015.

15 Onder de werktitel 'positie van NL aangaande de bescherming van persoonsgegevens van burgers in vergelijking met een aantal Europese lidstaten'.

16 Roosendaal, A., Ooms, M., Hoepman, J.H. (2015), *Een raamwerk van indicatoren voor de bescherming van persoonsgegevens. Nederland ten opzichte van andere landen*. Delft: TNO (WODC), 2015.

van het belang van het onderwerp en de wijze waarop dit onderwerp zich tot de overheid verhoudt. Omwille van het komen tot een kwalitatieve vergelijking is ervoor gekozen om ook enkele culturele aspecten mee te nemen en enkele onderwerpen of indicatoren waar de overheid niet of niet rechtstreeks invloed op heeft, maar die wel van belang zijn om een goed beeld van de bescherming van privacy in een land te verkrijgen. De behandelde onderwerpen betreffen achtereenvolgens een situatieschets van het land, indicatoren ten aanzien van beleid, wet- en regelgeving, de implementatie van beleid en regelgeving in de praktijk, en toezicht en handhaving.

Het raamwerk van Roosendaal et al. (2015) leidt tot de volgende deelvragen voor dit onderzoek.[17]

1. Wat is de algemene situatie rondom de bescherming van persoonsgegevens?

   Deze vraag leidt tot een situatieschets die weergeeft hoe de bescherming van persoonsgegevens is geregeld, welke rol de nationale politiek hierin heeft, wat de media-aandacht is hiervoor, of er sprake is van incidenten en welke rol burgerrechtenorganisaties spelen.

2. Welk beleid wordt er vanuit de nationale overheid gevoerd om persoonsgegevens te beschermen?

   Deze vraag betreft zowel beleid dat is gericht op de overheid zelf als beleid dat is gericht op burgers en private bedrijven en organisaties. Zowel bestaand beleid als beleidsvorming worden in kaart gebracht. Daarnaast wordt onderzocht wat de rol van de overheid in het maatschappelijk debat is en in hoeverre de overheid voorziet in voorlichting.

3. Welke wet- en regelgeving is van toepassing op de bescherming van persoonsgegevens?

   Op basis van richtlijn 95/46/EC is de wetgeving op het terrein van de bescherming van persoonsgegevens binnen de Europese Unie geharmoniseerd.[18] Inmiddels is de EU-verordening die deze richtlijn moet gaan vervangen aangenomen, zodat over enige tijd sprake is van nog verdergaande harmonisering.[19] Deze onderzoeksvraag inventariseert nationale wet- en regelgeving en brengt verschillen in kaart in de implementatie van de EU-richtlijn en de nadere invulling van regelgeving op lagere

17 Merk op dat Roosendaal et al. (2015) op zeer gedetailleerd niveau subvragen en deelaspecten weergeven. In dit onderzoek worden de onderzoeksvragen op het hoogste niveau gevolgd en op de lagere niveaus als richtinggevend beschouwd: afhankelijk van de specifieke situatie in een land en de beschikbaarheid van informatie wordt getracht ook antwoord te geven op zoveel mogelijk subvragen en deelaspecten. Echter, in sommige gevallen zal het niet mogelijk zijn elke subvraag voor elk land te beantwoorden.

18 Directive 95/46/EC of the European Parliament and the Council of 24th October 1995, [1995] OJ L281/31.

19 Voor meer achtergrond, zie bijvoorbeeld Kuner (2012) en Hornung (2012).

niveaus, waaronder sectorale wetgeving en (zelf)regulering. Waar relevant wordt de aankomende verordening betrokken in het onderzoek.

4. Op welke wijze zijn wetgeving en beleid op het terrein van bescherming van persoonsgegevens in de praktijk vormgegeven?

   Deze vraag ziet op de implementatie van wet- en regelgeving binnen organisaties. Daarbij wordt onderzocht in hoeverre sprake is van zelfregulering en gedragscodes, of sprake is van privacy officers, in hoeverre organisaties technische en organisatorische maatregelen hebben getroffen en in hoeverre zij transparantie betrachten.

5. Hoe zijn toezicht en handhaving bij bescherming van persoonsgegevens georganiseerd?

   Op grond van EU-richtlijn 95/46/EC zijn lidstaten verplicht een toezichthouder in te stellen op het terrein van bescherming van persoonsgegevens. Deze vraag geeft een beeld van de algemene kenmerken van de toezichthouder, de wijze waarop de toezichthouder zijn rol invult, in hoeverre de toezichthouder handhavend optreedt en welke opvattingen burgers en bedrijven hebben over de toezichthouder.

Deze deelvragen worden beantwoord voor acht landen, waaronder Nederland. De antwoorden op deze deelvragen zijn terug te vinden in de landenhoofdstukken (hoofdstuk 2 tot en met 9) van dit rapport. Voor een toelichting op de selectie van de landen wordt verwezen naar paragraaf 1.3.2. Door bovenstaande onderzoeksvragen voor elk van de acht landen (dus inclusief Nederland) te beantwoorden, wordt een beeld geschetst van de positie van verschillende lidstaten van de Europese Unie op het terrein van de bescherming van persoonsgegevens. Daarmee is de centrale vraag van dit onderzoek nog niet geheel beantwoord, aangezien de centrale vraag expliciet stelt wat de positie van Nederland is in vergelijking met andere landen binnen de EU. Om deze reden wordt een zesde onderzoeksvraag toegevoegd aan de vijf bovengenoemde onderzoeksvragen:

6. Wanneer de acht onderzochte landen met elkaar worden vergeleken op bovengenoemde aspecten, wat is dan de positie van Nederland?

   Bij deze vraag worden alle onderzochte landen per aspect gerangschikt. Daarmee wordt duidelijk wat de positie van Nederland is in vergelijking met de onderzochte landen. Zo kan blijken dat Nederland zich op bepaalde aspecten in het midden van het spectrum bevindt en op andere aspecten wellicht op een van de uiteinden van het spectrum.

Het antwoord op deze laatste deelvraag (en daarmee het antwoord op de centrale vraag van dit onderzoek) wordt gegeven in het conclusiehoofdstuk van dit rapport.

1.3 Onderzoeksaanpak

1.3.1 *Afbakening*

Dit onderzoek is een kwalitatief onderzoek. De acht landen die zijn geselecteerd vormen naar alle waarschijnlijkheid een representatief beeld van de verschillende posities die EU-lidstaten innemen ten opzichte van de bescherming van persoonsgegevens. Door deze representatieve selectie kan tevens een goed beeld worden verkregen van de positie van Nederland ten opzichte van andere landen in de Europese Unie. Echter, het aantal landen dat is betrokken in de vergelijking en de kwalitatieve aard van de aspecten waarop wordt vergeleken, staan geen kwantitatieve analyses van het verzamelde materiaal toe.

Hoewel een aanzienlijk deel van de onderzoeksvragen juridisch van aard is, is dit geen juridisch-dogmatisch onderzoek. Evenmin is de insteek van dit onderzoek zuiver rechtspositivistisch. Voor de bescherming van persoonsgegevens worden uiteraard wet- en regelgeving grondig geanalyseerd, maar steeds met de achterliggende gedachte dat de analyses antwoord moeten geven op de vraag hoe deze bescherming voor burgers in de praktijk is vormgegeven en door burgers wordt beleefd. Uit eerder onderzoek blijkt namelijk dat de privacybeleving van burgers niet altijd overeenkomt met de doelstellingen van wet- en regelgeving.[20] In dit onderzoek wordt geen uitgebreide survey opgezet om de beleving van burgers te onderzoeken, maar wordt wel gebruikgemaakt van eerdere EU-brede en nationale surveys die door anderen zijn uitgevoerd (zie paragraaf 1.3.3).

In dit onderzoek wordt geen normatief oordeel gegeven over waar Nederland zich zou moeten bevinden in de vergelijking met andere Europese landen. Wel worden aanknopingspunten geboden hoe Nederland op bepaalde aspecten zou kunnen verschuiven naar een andere plek op het spectrum. Daarmee kunnen de aanvragers van het onderzoek zelf ruimte nemen om voorstellen te doen over eventueel nieuwe wetgeving en/of beleid op het terrein van de bescherming van persoonsgegevens.

Zoals aangegeven in paragraaf 1.1, zal binnen afzienbare tijd (medio mei 2018) EU-richtlijn 95/46/EC worden vervangen door een EU-verordening die de bescherming van persoonsgegevens gaat reguleren. Aangezien de officiële publicatie van de EU-verordening reeds beschikbaar is, zal deze in het onderzoek worden betrokken waar relevant. Omdat de focus van dit onderzoek ligt op een vergelijking tussen verschillende landen, zal vooral nationale wet- en regelgeving centraal staan bij de landenanalyses.

In veel landen, ook in Nederland, bestaat sectorspecifieke wet- en regelgeving die de bescherming van persoonsgegevens nader invult. Voorbeelden van zulke sectoren zijn in Nederland de medische sector (bijvoorbeeld medisch beroepsgeheim in de Wet op de geneeskundige behandelingsovereenkomst), het strafrecht (bijvoorbeeld politie via

20 Regan, P.M. (2002), *Privacy and commercial use of personal data: policy developments in the US*, Rathenau Institute Privacy Conference, Amsterdam, Jan 2002; Custers, B., Van der Hof, S., Schermer, B., Appleby-Arnold, S., and Brockdorff, N. (2013), 'Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law', *SCRIPTed, Journal of Law, Technology and Society*, Volume 10, Issue 4, p. 435-457.

de Wet politiegegevens en justitie via de Wet justitiële en strafvorderlijke gegevens), nationale veiligheid (bijvoorbeeld via de Wet op de inlichtingen- en veiligheidsdiensten) en gemeenten (via de Wet basisregistraties personen).[21] In dit onderzoek wordt sectorspecifieke wet- en regelgeving wel in kaart gebracht (zie deelvraag 3), maar wordt niet dieper ingegaan op verschillen tussen landen op sectoraal niveau. Dat zou een extra dimensie toevoegen aan het onderzoek en de matrix van 5 aspecten x 8 landen aanzienlijk verder vergroten. Op verzoek van de opdrachtgever wordt, voor zover daarover informatie beschikbaar is gebleken, wel iets meer ingegaan op de regelingen voor de bescherming van persoonsgegevens in het strafrecht. Dit vergelijkingsaspect is met name uitgediept in hoofdstuk 10 (zie paragraaf 10.1.3). Reden voor deze bijzondere aandacht is dat de EU met het aannemen van de AVG tegelijk ook een richtlijn heeft aangenomen voor de bescherming van persoonsgegevens in het strafrecht, of beter gezegd: voor de bescherming van persoonsgegevens die door bevoegde autoriteiten worden verwerkt met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.[22] Deze richtlijn dienen EU-lidstaten te implementeren voor 6 mei 2018.
Dit onderzoek is uitgevoerd in de periode augustus 2016 tot en met mei 2017. Ontwikkelingen zijn meegenomen tot en met april 2017.

1.3.2 *Landenselectie*

De onderzoeksvragen 1 tot en met 5 in de vorige paragraaf worden beantwoord voor in totaal acht landen.[23] Naast Nederland, dat uiteindelijk zal worden gepositioneerd in vergelijking met andere Europese landen, worden de volgende landen in dit onderzoek betrokken: Frankrijk, Duitsland, het Verenigd Koninkrijk, Ierland, Roemenië, Italië en Zweden (zie figuur 1.1).

21 Zie paragraaf 2.3 voor meer details.

22 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

23 Roosendaal et al. (2015) geven aan dat minimaal zeven landen zouden moeten worden onderzocht, maar teneinde een vergelijking te kunnen maken met Nederland, zullen de onderzoeksvragen ook worden beantwoord voor Nederland.

Figuur 1.1 Landen die in dit onderzoek worden vergeleken: Frankrijk, Duitsland, het Verenigd Koninkrijk, Ierland, Roemenië, Italië en Zweden

De landenkeuze en bijbehorende onderbouwing is ingekaderd door Roosendaal et al. (2015). De selectiecriteria die zij hebben gehanteerd zijn:[24]

- spectrum van landen die bekend staan om strenge en soepele houding ten opzichte van privacybescherming;
- land met vergelijkbare benadering van gegevensbescherming als Nederland;
- land met andere benadering van gegevensbescherming dan Nederland;
- maturiteit van landen op het gebied van privacybescherming.

24 Roosendaal, A., Ooms, M., Hoepman, J.H. (2015), *Een raamwerk van indicatoren voor de bescherming van persoonsgegevens. Nederland ten opzichte van andere landen*. Delft: TNO (WODC), 2015.

In aanvulling op deze criteria is ervoor gezorgd dat zowel oude als nieuwe EU-lidstaten in het onderzoek zijn betrokken en dat zowel lidstaten uit Oost-, West-, Noord- en Zuid-Europa in het onderzoek zijn betrokken, opdat sprake is van een goede geografische spreiding. Uit het onderzoek van Roosendaal et al. (2015) wordt niet duidelijk hoe de door hen voorgestelde landen scoren op deze selectiecriteria en hoe deze selectie van landen derhalve een goede spreiding vertegenwoordigt op deze lijst van selectiecriteria.
In tabel 1.1 is weergegeven hoe de geselecteerde landen scoren op de genoemde criteria. De criteria zijn gescoord bij aanvang van het onderzoek op basis van de globaal beschikbare kennis. Tijdens het onderzoek is een veel uitgebreider beeld ontstaan van de onderzochte landen en bleek de initiële score redelijk te kloppen. Voor een uitgebreidere toelichting op de algemene situatie in de afzonderlijke landen wordt verwezen naar de eerste paragraaf van elk landenhoofdstuk (hoofdstukken 2 tot en met 9).
Op basis van de genoemde criteria komen Roosendaal et al. (2015) tot een longlist met de volgende landen: Frankrijk, Duitsland, het Verenigd Koninkrijk, Ierland, Roemenië (of een ander Oost-Europees land), Spanje/Italië/Portugal en Zweden.[25]
Alleen voor de keuze van een Oost-Europees en een Zuid-Europees land laten Roosendaal et al. (2015) enige keuzeruimte. Voor een Oost-Europees land is Roemenië gekozen. Roemenië is een geschikte keuze omdat het land pas in 2007, dus enkele jaren nadat andere lidstaten de richtlijn voor de bescherming van persoonsgegevens reeds hadden ingevoerd, lid is geworden van de Europese Unie. Roemenië heeft daardoor een volledig nieuw regelgevend kader voor bescherming van persoonsgegevens opgezet. Uiteraard geldt dit ook voor Bulgarije (toetreding in 2007) en Kroatië (toetreding in 2013), maar omdat de onderzoekers goede contacten hebben in Roemenië is aan dit land de voorkeur gegeven.
Voor een Zuid-Europees land wordt Spanje, Italië of Portugal voorgesteld door Roosendaal et al. (2015). Hoewel al deze landen geschikt zijn, is voor Italië gekozen als kandidaat voor een Zuid-Europees land. Italië heeft door de centrale ligging in Zuid-Europa met verschillende politieke aangelegenheden (vluchtelingenproblematiek, terrorismebestrijding, financiële crisis) te maken die dwingen tot uitwisseling van persoonsgegevens. Dit leidt tot een intensief politiek en maatschappelijk debat over de rol van privacy en de bescherming van persoonsgegevens. Bovendien beschikt eLaw ook in Italië over uitstekende contacten (zie volgende hoofdstuk).

25 Roosendaal, A., Ooms, M., Hoepman, J.H. (2015), *Een raamwerk van indicatoren voor de bescherming van persoonsgegevens. Nederland ten opzichte van andere landen*. Delft: TNO (WODC), 2015.

	Nederland	Duitsland	Zweden	Verenigd Koninkrijk	Ierland	Frankrijk	Roemenië	Italië
Streng/soepel[a]	Medium	Streng	Medium	Soepel	Medium	Soepel	Streng	Streng
Vergelijkbaar met Nederland[b]	n.v.t.	Ja	Ja	Nee	Nee	Nee	Nee	Nee
Rechtssysteem[c]	Civil Law (mengvorm)	Civil Law (Germaans)	Civil Law (Scandinavisch)	Common Law	Common Law	Civil Law (Napoleontisch)	Civil Law (Napoleontisch)	Civil Law (Napoleontisch)
Internationaal recht[d]	monistisch	dualistisch	dualistisch	dualistisch	dualistisch	monistisch	monistisch	dualistisch
Maturiteit[e]	Hoog	Hoog	Hoog	Medium	Medium	Hoog	Laag	Hoog
Oude/nieuwe lidstaat (jaar van toetreding)[f]	Oud (1958)	Oud (1958)	Medium (1995)	Medium (1973)	Medium (1973)	Oud (1958)	Nieuw (2007)	Oud (1958)
Geografische ligging	West	West	Noord	West	West	West	Oost	Zuid

Tabel 1.1 Overzicht van hoe de geselecteerde landen scoren op de selectiecriteria op basis van aannames voorafgaand aan het onderzoek

a Bij de inschatting van een strenge of soepele houding ten opzichte van privacybescherming is gebruikgemaakt van de privacy-index van Privacy International, een non-profitorganisatie uit het Verenigd Koninkrijk die periodiek een landenindex opstelt samen met het Electronic Privacy Information Center (EPIC) uit de Verenigde Staten. De laatste rapportage dateert van 2007. Hierin wordt het Verenigd Koninkrijk beschreven als een 'endemic surveillance society' (slechtst scorende categorie voor privacybescherming), Frankrijk als een 'extensive surveillance society', Ierland, Nederland en Zweden als landen met 'systemic faiure to uphold privacy safeguards' en Duitsland, Roemenië en Italië als landen met 'safeguards but weakened protection'. De laatste categorie is niet de best scorende categorie voor privacybescherming, maar er zijn vrijwel geen landen die hoger scoren dan deze categorie. Alleen Griekenland scoort hoger. Zie National Privacy Ranking 2007 – European Union and Leading Surveillance Societies (PDF). London: Privacy International. http://observatoriodeseguranca.org/files/phrcomp_sort.pdf.

b Voor deze globale inschatting is gebruikgemaakt van de theorie van organisatiepsycholoog Geert Hofstede, die op een aantal dimensies culturen onderscheidt. Deze dimensies zijn machtsafstand, individualisme, masculiniteit, onzekerheidsvermijding. Later zijn ook toegevoegd langetermijndenken en toegeeflijkheid. Op http://www.geerthofstede.nl/ zijn scores voor de eerste vier dimensies per land terug te vinden. Nederland en Duitsland scoren op drie van de vier dimensies vergelijkbaar (niet op masculiniteit), Nederland en Zweden scoren op bijna alle vier dimensies vergelijkbaar (onzekerheidsvermijding is in Nederland medium, in Zweden laag). Roemenië verschilt op alle vier de dimensies van Nederland. De overige landen verschillen op ongeveer de helft van de dimensies met Nederland. De indeling van Hofstede gaat over culturele verschillen, niet noodzakelijkerwijs ook over de benadering van privacy en gegevensbescherming. Maar ook daarvoor geldt dat Nederland, Duitsland en Zweden op elkaar lijken. Door verschillende rechtsstelsels zijn de verschillen met Ierland en het Verenigd Koninkrijk groter. Cultureel gezien zijn de verschillen op het vlak van privacy met Frankrijk, Italië en Roemenië ook groter.

c Het belangrijkste onderscheid in rechtssystemen is tussen common law en civil law (continentaal recht). In common law ligt bij wetsvorming de nadruk op gerechtelijke uitspraken terwijl in continentaal recht de nadruk bij rechtsvorming ligt op wetgeving die door de landelijke overheid wordt opgelegd. Het continentaal recht heeft zijn oorsprong in het Romeinse recht en wordt verder onderscheiden in Napoleontisch, Duits, Scandinavisch recht.

d In internationaal recht worden de termen monisme en dualisme gebruikt om de verhouding tussen internationaal en nationaal recht weer te geven. In een monistische opvatting vormen het internationale recht en het nationale recht één rechtssysteem. Internationaal recht is van een hogere orde en kan zonder verdere omzetting in nationaal recht direct worden toegepast. In een dualistische opvatting zijn de twee systemen afzonderlijke rechtssferen. Omzetting van internationaal recht in nationaal recht is dan nodig alvorens het kan worden toegepast. Zie voor welke landen monistisch danwel dualistisch zijn: Hoffmeister, F. (2002), International agreements in the legal order of the candidate countries. In: A. Ott and K. Inglis (Eds), *Handbook on European Enlargement*, The Hague: Asser Press, p. 209.

e Maturiteit is sterk gekoppeld aan de toetreding tot de EU en de bijbehorende wet- en regelgeving op het vlak van privacy en bescherming van persoonsgegevens. Zweden heeft een hoge maturiteit omdat dit het eerste land is dat een wet voor de bescherming van persoonsgegevens had (reeds in 1973, terwijl Zweden relatief laat tot de EU is toegetreden, in 1995).

f In 1958 werd de EEG opgericht. Nederland, Duitsland, Frankrijk en Italië behoren tot de oprichters.

1.3.3 *Methodologie*

Vragenlijst

Teneinde de situatie voor alle acht landen in kaart te brengen, is gebruikgemaakt van een uitgebreide vragenlijst die voor elk land moest worden beantwoord. Deze vragenlijst is gebaseerd op het vooronderzoek van TNO (Roosendaal et al., 2015) en terug te vinden in Appendix C. De antwoorden op de vragenlijst vormen de puzzelstukjes die het samen mogelijk maken op de centrale vraag van dit onderzoek antwoord te geven. Het gaat in totaal om 40 puzzelstukken (5 aspecten x 8 landen). Om de relevante informatie uit de verschillende landen adequaat te kunnen ontsluiten, is een uitgebreid Europees netwerk van experts op het terrein van bescherming van persoonsgegevens nodig, evenals goed zicht op nationale rechtsstelsels en voldoende talenkennis. Op basis van eerdere uitgevoerde Europese onderzoeksprojecten beschikten de onderzoekers over uitgebreide kennis over de situatie in andere landen en een netwerk van experts in die landen.

In dit onderzoek wordt geen survey onder burgers afgenomen en worden evenmin focusgroepen met burgers georganiseerd. Een survey onder burgers zou aanzienlijke aantallen respondenten moeten bevatten om representatief te zijn. Zulke aantallen waren niet haalbaar binnen een realistisch budget en de gewenste planning. Bovendien zou een dergelijke survey niet veel toevoegen aan reeds bestaande surveys (zie hierna). In deze surveys zijn reeds (zeer) grote aantallen respondenten betrokken. Focusgroepen met burgers zouden op vergelijkbare bezwaren stuiten: om te komen tot representatieve bevindingen zouden grotere groepen of grotere aantallen groepen moeten worden samengesteld, terwijl grotere groepen onwerkbaar worden en grotere aantallen groepen niet passen binnen een realistisch budget en de gewenste planning. Vandaar dat als alternatief gebruik is gemaakt van bestaande surveys voor het inventariseren van percepties van burgers betreffende de bescherming van persoonsgegevens. Dit bespaarde tijd en kosten, waardoor meer ruimte ontstond om diepgang in het onderzoek te creëren op de verschillende deelaspecten van bescherming van persoonsgegevens.

Zoals te zien is in Appendix C, zijn er op elk van de vijf vergelijkingsaspecten meerdere vragen gesteld in de vragenlijsten. Teneinde de antwoorden op deze vragen, gebaseerd op het onderzoek van Roosendaal et al., 2015, overzichtelijk te houden, zijn deze antwoorden uiteindelijk geclusterd in 23 categorieën (labels). Een overzicht van deze labels is te zien in Tabel 1.2.

Vergelijkingsaspecten	Labels
1. Algemene situatie	Internetgebruik, (gevoel van) controle, bewustzijn, vertrouwen, beschermingsmaatregelen, nationale politiek, media-aandacht, datalekken, burgerrechtenorganisaties
2. Beleid	Nationaal beleid & PIA's, privacy & bescherming van persoonsgegevens in beleid, maatschappelijk debat, informatiecampagnes

3. Wet- en regelgeving	Implementatie van de EU-richtlijn, sectorale wetgeving, zelfregulering & gedragscodes
4. Implementatie	Privacyfunctionarissen, beveiligingsmaatregelen, transparantie
5. Toezicht en handhaving	Toezichthouders, taken & bevoegdheden, gebruik van bevoegdheden, reputatie

Tabel 1.2 De 23 labels waarop landen in dit onderzoek zijn vergeleken binnen 5 vergelijkingsaspecten

Deskresearch

Als eerste stap hebben de onderzoekers voor elk land onderdelen van de vragenlijst zelf ingevuld op basis van deskresearch. Op basis van beschikbare literatuur en online gegevens (bijvoorbeeld websites en jaarverslagen van toezichthouders, overheden en burgerrechtenorganisaties) bleek een aanzienlijk deel van de benodigde informatie te vinden. Hoewel in dit onderzoek geen survey is gehouden onder EU-burgers, zijn delen van de vragenlijst wel beantwoord aan de hand van secundaire analyses op en/of hergebruik van bestaande surveys. Drie belangrijke bronnen die hierbij zijn gebruikt, zijn:

- CONSENT Survey[26]
  In dit onderzoek zijn aan respondenten 75 vragen over internetgebruik, online gedrag en percepties omtrent de bescherming van persoonsgegevens en online privacy voorgelegd. De nadruk lag op het gebruik van persoonsgegevens in sociale media. In totaal deden 8621 respondenten uit 26 verschillende EU-lidstaten mee.[27]
- Eurobarometer[28]
  In dit onderzoek in 27 EU-lidstaten zijn 26.574 Europeanen van 15 jaar en ouder ondervraagd op hun houding ten opzichte van bescherming van persoonsgegevens. Alle interviews zijn persoonlijk (face-to-face) afgenomen bij mensen thuis in hun eigen taal.
- Oxford Internet Survey[29]
  De Oxford Internet Survey (OxIS) is een serie surveys (meest recente publicatie in 2013)[30] over het internetgedrag in het Verenigd Koninkrijk. In de laatste survey zijn resultaten te vinden van in totaal 2657 respondenten. De survey is onder meer gericht op internetgebruik, privacy en gepercipieerd vertrouwen en risico's omtrent persoonsgegevens.

26 Brockdorff, N. (2012) *Quantitative Measurement of End-User Attitudes Towards Privacy*. Work Package 7 of Consent. http://www.consent.law.muni.cz/. Zie ook: https://consent.law.muni.cz/index.php.

27 Zie ook Custers, B., Van der Hof, S., Schermer, B. (2014), 'Privacy Expectations of Social Media Users. The Role of Informed Consent in Privacy Policies', *Policy & Internet*, Vol. 6, No. 3, p. 268-295.

28 Eurobarometer Survey 359 (2011). *Attitudes on Data Protection and Electronic Identity in the European Union*. Brussels, June. Zie ook: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

29 Dutton, W.H., and G. Blank (2013), *Cultures of the Internet. The Internet in Britain*, Oxford Internet Survey 2013. Zie ook: http://oxis.oii.ox.ac.uk/reports.

30 Eerdere versies verschenen in 2003, 2005, 2007, 2009 and 2011.

Het doel van de deskresearch is enerzijds algemene achtergrondinformatie te verzamelen en anderzijds om de informatie uit de expertbevraging (zie hierna) te verrijken. In het literatuuronderzoek zijn onder meer betrokken: Kamerbrieven, beleidsdocumenten, kabinetsvisies, parlementaire verslagen, regelgeving, rapporten en verslagen van eerder onderzoek en relevante wetenschappelijke publicaties.

Expertbevraging
De onderdelen van de vragenlijst die niet konden worden beantwoord aan de hand van deskresearch zijn vervolgens uitgezet bij experts in de betreffende landen. Op basis van eerdere samenwerkingsverbanden waarin de onderzoekers betrokken waren, is contact opgenomen met experts in de verschillende landen. Daarnaast is contact opgenomen met (medewerkers van) de toezichthoudende instanties op het gebied van privacy en gegevensbescherming in de verschillende landen. Deze experts en toezichthouders hebben niet de integrale vragenlijst toegestuurd gekregen, maar slechts die vragen die niet of onvoldoende konden worden beantwoord aan de hand van deskresearch. Deze aanpak leverde enerzijds ontbrekende informatie op en anderzijds een verificatie van de tot dusver gevonden resultaten. Een overzicht van de bevraagde experts en instanties is te vinden in Appendix B.

Aanvullend zoekwerk
Op aspecten waar na deskresearch en expertbevraging nog steeds weinig of geen informatie beschikbaar bleek voor bepaalde landen, zijn de resultaten aangevuld met (nader) literatuuronderzoek, (nadere) media-analyses en aanvullende interviews. Voor aanvullende interviews zijn experts op het gebied van bescherming van persoonsgegevens, beleidsmakers, bedrijven die persoonsgegevens verwerken, toezichthouders en belangenorganisaties benaderd. Voor zover deze experts inhoudelijke informatie hebben verschaft, zijn zij opgenomen in Appendix B. Daarnaast zijn de onderzoekers doorverwezen naar weer andere experts. Ook de begeleidingscommissie van dit onderzoek (zie het overzicht Appendix A) heeft actief bijgedragen aan het aanleveren van experts.

Analyses
Met behulp van bovenstaande methoden zijn alle puzzelstukken verzameld. Daarmee is het mogelijk voor elk land antwoord te geven op deelvragen 1 tot en met 5. De zesde deelvraag (waar Nederland zich bevindt ten opzichte van andere Europese landen) wordt beantwoord door vervolgens de matrix te 'kantelen' en per aspect de acht verschillende landen op een rij te zetten. Anders gezegd: eerst worden alle aspecten per land in kaart gebracht, daarna worden per aspect alle landen vergeleken. Waar mogelijk zijn kwantitatieve gegevens met elkaar vergeleken (bijvoorbeeld: 'hoeveel mensen weten van het bestaan van de toezichthouder?'), maar voor veel aspecten is een kwalitatieve vergelijking gemaakt (bijvoorbeeld: 'hoeveel aandacht is er in de media voor privacy en gegevensbescherming?'). Omdat de vergelijking op de vijf aspecten nog te grofmazig is, zijn bij elke vergelijking een aantal kernpunten als uitgangspunt genomen. Bij het vergelijken van de algemene situatie per land is, bijvoorbeeld, vergeleken op de kernpunten internetgebruik, (gevoel van) controle, bewustzijn, vertrouwen en beschermingsmaatregelen (zie tabel 1.2).

1.4 Opbouw van dit rapport

De opbouw van dit rapport volgt de hierboven beschreven aanpak. In de volgende acht hoofdstukken (hoofdstuk 2 tot en met 9) worden de acht onderzochte landen respectievelijk besproken. Deze reeks landenhoofdstukken start met Nederland. In elk van deze hoofdstukken komen de vijf aspecten uit onderzoeksvragen 1 tot en met 5 (zie paragraaf 1.2) aan bod: algemene situatie, beleid, wet- en regelgeving, implementatie en toezicht en handhaving.[31]
In de hoofdstukken 2 tot en met 9 wordt dus antwoord gegeven op onderzoeksvragen 1 tot en met 5. De zesde onderzoeksvraag (waar Nederland zich bevindt in het spectrum) wordt beantwoord in het laatste hoofdstuk (hoofdstuk 10) van dit onderzoeksrapport. In dat hoofdstuk worden de onderzochte landen per deelaspect op het spectrum gezet en de positie van Nederland in het bijzonder toegelicht. Tot slot worden aanknopingspunten beschreven hoe Nederland zou kunnen verschuiven op het spectrum (bijvoorbeeld meer naar het midden of meer naar een van de uitersten van het spectrum), mocht dat (politiek, juridisch en/of sociaal-maatschappelijk gezien) wenselijk zijn.

31 Merk op dat ook gekozen zou kunnen worden voor vijf hoofstukken met elk acht landenparagrafen. Ons inziens heeft het de voorkeur het beschikbare materiaal per land te rangschikken. De ervaring leert dat dit prettiger leest, herhaling en overlap voorkomt en ervoor zorgt dat informatie eenvoudig is terug te vinden.

2. Nederland

2.1 Algemene situatie

Dit onderzoek is gestart op verzoek van de Nederlandse overheid teneinde de bescherming van persoonsgegevens in Nederland te kunnen vergelijken met andere EU-lidstaten (zie hoofdstuk 1). Een dergelijke internationale vergelijking vereist uiteraard allereerst het in kaart brengen van de situatie en het niveau van bescherming van persoonsgegevens in Nederland. Vandaar dat we in dit hoofdstuk beginnen met het beantwoorden van de landspecifieke onderzoeksvragen (vragen één tot en met vijf, zie vorige hoofdstuk) voor Nederland.

Nederland kent een lange traditie van internationaal recht. Soms wordt zelfs gesteld dat de basis voor internationaal recht in Nederland is gelegd door Hugo de Groot.[1] In zijn beroemde boek *De iure belli ac pacis* ('over het recht in oorlog en vrede') bespreekt hij de juridische status van oorlog.[2] In latere eeuwen zijn ideeën en concepten uit dit boek gebruikt om internationale verdragen en conventies op te stellen. Nederland was een van de oprichters van de Verenigde Naties, de Europese Unie en vele van hun voorgangers, zoals de Volkenbond, de Europese Gemeenschap voor Kolen en Staal (EGKS) en de Europese Economische Gemeenschap (EEG). Verder is Nederland medeondertekenaar van alle relevante internationale mensenrechtenverdragen, waaronder de Universele Verklaring van de Rechten van de Mens, het Europees Verdrag voor de Rechten van de Mens en het Handvest van de grondrechten van de Europese Unie. In 2014 kreeg het Nederlandse College voor de Rechten van de Mens de A-status voor het volledig voldoen aan de zogeheten Paris Principles, een standaard voor de toestand en het functioneren van nationale overheidsinstituten voor het beschermen en bevorderen van mensenrechten. In Nederland is sprake van een gematigd monistisch stelsel, waarbij het internationale recht en het nationale recht grotendeels als één rechtssysteem worden gezien. Behoudens uitzonderingen[3] behoeven internationale verdragen geen omzetting naar nationaal recht om doorwerking te hebben. Hierdoor zijn mensenrechten uit internationale verdragen, waaronder het recht op privacy, stevig verankerd in Nederland.

---

1 Woods, T. (2012), *How the Catholic Church Built Western Civilization*. Regnery Publishing, Inc., pp. 5, 141–142.

2 Groot, H. de (1625), *De iure belli ac pacis*. Pariisis: Apud Nicalaum Buon.

3 Art. 93 en 94 Grondwet bepalen dat verbindende bepalingen uit internationale verdragen pas doorwerkend nadat ze bekend zijn gemaakt. Hieruit blijkt het gematigde karakter van het Nederlandse monistische stelsel.

Het recht op privacy is sinds 1983 opgenomen in de Nederlandse Grondwet.[4] Eerder waren wel aspecten van privacy zichtbaar, maar die werden toen nog niet als zodanig benoemd. Zo werd in de Nederlandse Grondwet van 1815 het huisrecht verankerd. In 1848 volgde de opname van het briefgeheim in de Grondwet. Bij de latere Grondwetsherziening van 1983 werd het recht op privacy als zelfstandig recht opgenomen en nader onderscheiden naar een algemeen recht op privacy (artikel 10 Grondwet) en verschillende meer specifieke privacyrechten, waaronder het recht op de bescherming van persoonsgegevens (artikel 10 Grondwet), lichamelijke integriteit/fysieke privacy (artikel 11 Grondwet), het huisrecht/ruimtelijke privacy (artikel 12 Grondwet) en het briefgeheim/communicatie privacy (artikel 13 Grondwet).

Internetgebruik

Nederlanders zijn actieve internetgebruikers en lijken zich erg bewust van het verwerken van persoonsgegevens, hoewel de bijkomende risico's als laag worden beschouwd.[5] Recent bevolkingsonderzoek laat zien dat 36% van de mensen tussen 1 en 2 uur per dag online is en dat 31% zelfs 3 tot 4 uur per dag online is.[6] Dit hoge internetgebruik kan verder worden geïllustreerd met het feit dat 95% van de Nederlanders online aankopen doet (EU-gemiddelde 87%), met slechts kleine verschillen tussen verschillende leeftijdscategorieën en een voorkeur voor het betalen (via betaalpas, creditcard of elektronisch geld) op het moment van bestellen.[7] Ongeveer 59% van de Nederlanders gebruikt ten minste één keer per week sociale media, hetgeen iets boven het EU-gemiddelde is.[8] Internetbankieren wordt gebruikt door 75% van de Nederlanders, waarmee Nederland behoort tot de top drie van EU-lidstaten (na Finland en Denemarken) en significant uitsteekt boven het EU-gemiddelde (43%).[9] De hoeveelheid aankopen van goederen en diensten via internet is vergelijkbaar met EU-gemiddelden.[10] De mate waarin Nederlanders online games spelen en de mate waarin ze telefoon- en videogesprekken voeren via internet is vergelijkbaar met EU-gemiddelden.[11] Echter, het gebruik van instant messaging en chat websites blijft aanzienlijk achter (43% vergeleken met het EU-gemiddelde van 53%).[12]

(Gevoel van) controle

Desgevraagd geven Nederlanders aan niet het gevoel te hebben controle te hebben over de gegevens die ze online verstrekken. Volgens recent bevolkingsonderzoek blijkt slechts 9% het gevoel te hebben hierover controle te hebben (het laagste van alle EU-lidstaten

4 https://www.nederlandrechtsstaat.nl/grondwet/artikel.html?artikel=10&categorie=&auteur=&trefwoord=&1=1##artikel10
5 Consent Country Report The Netherlands, (2012), p. 4.
6 Roosendaal, A., Nieuwenhuis, O., Ooms, M., Bouman-Eijs, A., en Huijboom, N. (2015), *Privacybeleving op het internet in Nederland*, Den Haag: TNO, p. 24.
7 Consent Country Report The Netherlands, (2012), p. 4.
8 Eurobarometer 431 (2015), p. 109.
9 Eurobarometer 431 (2015), p. 110.
10 Eurobarometer 431 (2015), p. 112.
11 Eurobarometer 431 (2015), p. 111.
12 Eurobarometer 431 (2015), p. 110.

na Duitsland), 59% voelt slechts gedeeltelijk controle en 30% voelt geen enkele controle.[13] Tegelijkertijd geven Nederlanders aan zich niet heel veel zorgen te maken over dit gebrek aan controle. Ongeveer 47% geeft aan zich hierover zorgen te maken (het laagste van alle EU-lidstaten na Estland en Zweden), vergeleken met een EU-gemiddelde van 67%.[14]
Het overgrote deel van de Nederlanders (86%) beschouwt het online verstrekken van persoonsgegevens als een toenemend onderdeel van het moderne leven. Dit is het op twee na hoogste in de EU (gemiddeld 71%), na Cyprus en Denemarken.[15] In tegenstelling tot het EU-gemiddelde lijkt deze opvatting in Nederland zelfs nog toe te nemen. Ongeveer 48% geeft aan dat het verstrekken van persoonsgegevens geen groot punt is (het hoogste binnen de EU na Denemarken en Litouwen).[16] Gevraagd naar het gebruik van persoonsgegevens voor gepersonaliseerde reclame en diensten geeft 4% aan dit erg comfortabel te vinden, 33% dit redelijk comfortabel te vinden, 39% dit redelijk oncomfortabel te vinden en 22% dit zeer oncomfortabel te vinden.[17]

Bewustzijn
In het algemeen vertonen Nederlanders een hoog niveau van bewustzijn als het gaat om het gebruik van persoonsgegevens door de eigenaren van websites. Wanneer deze gegevens door de eigenaren van websites worden gebuikt om gebruikers via e-mail te benaderen, is het niveau van bewustzijn en acceptatie onder Nederlanders erg hoog (bewustzijn 86%, acceptatie 80%).[18] Bewustzijn en acceptatie zijn vergelijkbaar hoog als het gaat om het gebruik van persoonsgegevens om de inhoud van websites en advertenties te personaliseren. Terwijl er een soort van evenwicht lijkt te zijn tussen bewustzijn van gebruikers en acceptatie van deze praktijk, zijn er echter substantieel lagere acceptatieniveaus wanneer het gaat om het diepgaand vergaren van persoonsgegevens, het verkopen van persoonsgegevens of het beschikbaar stellen van persoonsgegevens aan anderen. Zulke praktijken worden grotendeels als onacceptabel beschouwd (Nederland 75%, EU-gemiddelde 74%).[19] Daadwerkelijke ervaring met privacyinbreuken is relatief laag in Nederland, met een score van 2,92 (EU-gemiddelde 2,89) op een 7-puntsschaal (1 = nooit, 7 = zeer vaak).[20]
Als het gaat om privacy policies,[21] geeft 61% van de Nederlanders (hetgeen significant hoger ligt dan het EU-gemiddelde van 47%) aan ooit een website niet gebruikt te hebben vanwege ontevredenheid met het privacybeleid van die website. Echter, meer dan de

13 Eurobarometer 431 (2015), p. 10.
14 Eurobarometer 431 (2015), p. 13.
15 Eurobarometer 431 (2015), p. 29.
16 Eurobarometer 431 (2015), p. 32.
17 Eurobarometer 431 (2015), p. 40.
18 Consent Country Report The Netherlands, (2012), p. 4.
19 Consent Country Report The Netherlands, (2012), p. 4.
20 Consent Country Report The Netherlands, (2012), p. 4.
21 Strikt genomen is er een onderscheid tussen privacy policies (privacy beleid) en terms & conditions (algemene voorwaarden). De algemene voorwaarden zijn verplichtend voor beide partijen, terwijl beleid meer een belofte of voornemen inhoudt, maar niet afdwingbaar is. In de onderzoeken waarnaar wordt verwezen, lijken beide documenten als gelijkwaardig te worden behandeld, waarschijnlijk omdat gebruikers nauwelijks verschillen zien.

helft van de Nederlanders geeft aan nooit of zelden daadwerkelijk de algemene voorwaarden (51%) of het privacybeleid (61%) van een website te lezen. Als het privacybeleid al gelezen wordt, lezen Nederlanders zelden de hele tekst (Nederland 9%, EU-gemiddelde 11%). Niettemin zijn Nederlanders redelijk vol vertrouwen de tekst – als ze het lezen – grotendeels of helemaal te begrijpen (Nederland 72%, EU-gemiddelde 64%).
Het niveau van ervaring van Nederlanders wordt bevestigd door hun bewustzijn en gedrag omtrent hun omgang met technische details: 91% is zich bewust van cookies (EU-gemiddelde 65%), hoewel iets meer dan twee van de drie Nederlanders ze daadwerkelijk ooit uitschakelen (Nederland 72%, EU-gemiddelde 68%).[22] Ongeveer 50% van de Nederlanders heeft ooit gehoord van het bestaan van de toezichthouder op het terrein van bescherming van persoonsgegevens, de Autoriteit Persoonsgegevens. Hiermee behoort Nederland tot de top vijf van de EU-lidstaten (het gemiddelde is 37%).[23]

Vertrouwen
De mate waarin Nederlanders overheidsorganisaties en bedrijven vertrouwen als het gaat om de bescherming van persoonsgegevens verschilt behoorlijk voor verschillende sectoren. Vertrouwen is relatief hoog in de gezondheidszorg (81%, EU-gemiddelde 74%), overheidsinstellingen (82%, EU-gemiddelde 66%), banken en financiële instellingen (74%, EU-gemiddelde 56%) en EU-instellingen (63%, EU-gemiddelde 51%). Echter, vertrouwen is beduidend lager als het gaat om winkels (31%, EU-gemiddelde 40%), telecom- en internetproviders (37%, EU-gemiddelde 33%) en online bedrijven 18%, EU-gemiddelde 24%).[24]
In vergelijking met het EU-gemiddelde beschouwen Nederlanders de risico's verbonden aan het verstrekken van persoonsgegevens aan sociale media als relatief kleiner.[25] Ze nemen echter wel een toegenomen risico waar als het gaat om misbruik van gegevens (6,23 op een 7-puntsschaal, 1 = oneens en 7 = eens).[26] Specifieke risico's (met percentages boven de EU-gemiddelden) zien Nederlanders vooral bij gegevens die ze verstrekken op sociale media wanneer die worden gebruikt of gedeeld zonder dat ze daarvan weet hebben of daar toestemming voor hebben gegeven en wanneer die worden gebruikt om ze ongevraagd aanbiedingen te doen.[27] Meer 'persoonlijke' risico's zien Nederlanders niet: het percentage voor waargenomen risico's voor persoonlijke veiligheid als gevolg van het verstrekken van persoonsgegevens op sociale media is het op een na laagste van de EU met 14% (EU-gemiddelde 24%). Het waargenomen risico slachtoffer van fraude te worden, is het op twee na laagste van de EU met 23% (EU-gemiddelde 32%). Het waargenomen risico voor de persoonlijke reputatie is voor Nederlanders 17% (EU-gemiddelde 25%).
Hoewel 95% van de Nederlanders online aankopen doet, zegt slechts 8% van de Nederlanders die nooit iets via het internet koopt dat dit het gevolg is van het feit dat

22 Consent Country Report The Netherlands, (2012), p. 3.
23 Eurobarometer 431 (2015), p. 52.
24 Eurobarometer 431 (2015), p. 66.
25 Consent Country Report The Netherlands, (2012), p. 4.
26 Consent Country Report The Netherlands, (2012), p. 4.
27 Consent Country Report The Netherlands, (2012), p. 4.

ze geen vertrouwen hebben in online verkopers, hetgeen iets afwijkt van het EU-gemiddelde (15%).[28] De belangrijkste reden om af te zien van online aankopen is de afkeer van het verstrekken van persoonlijke informatie (financiële details en adressen), waarmee Nederlanders aanzienlijk boven het EU-gemiddelde scoren (35%, EU-gemiddelde 24%), hetgeen kan worden beschouwd als een probleem met vertrouwen en privacy. Ander onderzoek, uitgevoerd door de DDMA, de brancheorganisatie voor data driven marketing, laat zien dat Nederlanders in drie archetypen kunnen worden onderscheiden: 34% is pragmatisch, 28% is sceptisch en 38% maakt zich in het geheel niet druk.[29]

Beschermingsmaatregelen

Het aantal Nederlanders dat ooit heeft geprobeerd privacyinstellingen op hun sociale-mediaprofielen aan te passen is 71%, hetgeen het hoogste is binnen de EU (samen met het Verenigde Koninkrijk) en significant boven het EU-gemiddelde van 57%.[30] Niettemin is er onder Nederlanders het hoogste aandeel mensen dat het lastig vindt deze instellingen aan te passen (na Duitsland en België). Ongeveer 36% vindt dit lastig en 64% vindt dit eenvoudig.[31] Nederlanders die hun privacyinstellingen niet veranderen, geven aan erop te vertrouwen dat de website gepaste instellingen hanteert (26%), dat ze niet weten hoe de instellingen veranderd kunnen worden (21%), dat ze niet bezorgd zijn over hun persoonsgegevens online (28%), dat ze geen tijd hebben naar de mogelijkheden te kijken (8%) of dat ze niet weten dat deze instellingen aangepast kunnen worden (14%).[32] Vergelijkbare resultaten zijn te zien in een ander bevolkingsonderzoek, dat laat zien dat, om hun privacy te beschermen, 58% van de Nederlanders vaak of altijd de privacyinstellingen van hun persoonlijk profiel op sociale media aanpast (EU-gemiddelde 54%). Van de mensen die hun privacyinstellingen aanpassen, maakt 79% (in vergelijking met het EU-gemiddelde van 80%) deze instellingen strikter, zodat anderen minder informatie over hen te zien krijgen.[33] Nederlands onderzoek laat vergelijkbaar hoge cijfers zien: 89% heeft beschermende software geïnstalleerd en 68% heeft profielinstellingen aangepast.[34]

Op het niveau van specifieke technische maatregelen om persoonlijke internetbeveiliging te bewerkstelligen of te verbeteren, zijn onder Nederlanders sommige maatregelen (zoals het blokkeren van pop-ups, het aanvinken van opt-in- en opt-outopties en het blokkeren van bepaalde e-mailadressen) meer gebruikelijk dan andere (zoals controleren op spyware en het verwijderen van de zoekgeschiedenis). Nederlanders laten hier resultaten zien die duidelijk boven de EU-gemiddelden liggen.[35]

---

28 Consent Country Report The Netherlands, (2012), p. 4.

29 DDMA (2016), *Hoe Nederlanders denken over data en privacy*, Amsterdam: DDMA, p. 4.

30 Eurobarometer 431 (2015), p. 92.

31 Eurobarometer 431 (2015), p. 95.

32 Eurobarometer 431 (2015), p. 98.

33 Consent Country Report The Netherlands, (2012), p. 4.

34 Roosendaal, A., Nieuwenhuis, O., Ooms, M., Bouman-Eijs, A., en Huijboom, N. (2015), *Privacybeleving op het internet in Nederland*, Den Haag: TNO, p. 5.

35 Consent Country Report The Netherlands, (2012), p. 3.

Nationale politiek

Zowel in de Tweede Kamer als in de Eerste Kamer zijn privacy en de bescherming van persoonsgegevens regelmatig onderwerp of onderdeel van debat. Als het gaat om het afwegen tussen meer abstracte zaken als privacy en de bescherming van persoonsgegevens enerzijds en meer concrete, praktische zaken als het delen van gegevens, veiligheid, etc., lijkt de Tweede Kamer soms meer geneigd de concrete, praktische zaken voorrang te geven. Debatten over privacy versus veiligheid worden regelmatig in het voordeel van veiligheid beslecht.[36] Daarmee is echter niet gezegd dat privacy niet belangrijk is in de Tweede Kamer. Dit onderzoek, dat werd aangevraagd door leden van de Tweede Kamer (zie hoofdstuk 1), illustreert dit. Daarnaast eiste de Tweede Kamer van de minister van Veiligheid en Justitie middels periodieke rapportages op de hoogte te worden gehouden over de onderhandelingen over de Algemene Verordening Gegevensbescherming (AVG). Een ander typisch voorbeeld is de motie Franken uit 2011, herhaald in een motie in 2015 door andere parlementariërs, waarin de regering wordt verzocht een zogeheten Privacy Impact Assessment uit te voeren voor elk wetsvoorstel dat consequenties kan hebben voor het verwerken van persoonsgegevens.[37]

De Eerste Kamer, daarentegen, lijkt veel kritischer en stemde zelfs tegen enkele wetsvoorstellen die eerder waren goedgekeurd in de Tweede Kamer. Zo stemde de Eerste Kamer in 2011 tegen het wetsvoorstel voor het elektronisch patiëntendossier (Wet EPD) en tegen voorgestelde hervormingen bij de inlichtingen- en veiligheidsdiensten (Wet op de inlichtingen- en veiligheidsdiensten).

In de afgelopen jaren zijn veel wetsvoorstellen die betrekking hebben op of raken aan privacy en bescherming van persoonsgegevens besproken in de Tweede Kamer. Typische voorbeelden zijn de Meldplicht datalekken in 2016 (waarin ook de boetebevoegdheden van de Autoriteit Persoonsgegevens aanzienlijk werden verruimd), de versoepeling cookiewet in 2014, de verruiming preventief fouilleren in 2013 en de slimme energiemeters in 2010. Dit is slechts een kleine greep uit de voorgestelde wetgeving. Wetsvoorstellen die uitgebreid in de Eerste Kamer zijn besproken, zijn onder meer het (herziene wetsvoorstel) Wet elektronische patiëntendossiers in 2016 en de Wet verruimen cameratoezicht in 2014. Uiteraard worden alle wetsvoorstellen die door de Tweede Kamer worden goedgekeurd, doorgestuurd naar de Eerste Kamer. Daardoor zijn er veel debatten over privacy en de bescherming van persoonsgegevens. Aangezien de Eerste Kamer geen initiatiefrecht heeft om wetsvoorstellen te doen, beperken de debatten zich hier tot voorstellen die worden ontvangen vanuit de Tweede Kamer.

In beide Kamers van het parlement zijn veel verschillende politieke partijen vertegenwoordigd. De website www.privacybarometer.nl stelde een *score system* op voor de mate waarin politieke partijen privacy en de bescherming van persoonsgegevens in acht nemen. Volgens hun becijfering is de SP de enige politieke partij die privacy en de bescherming van persoonsgegevens serieus in acht neemt, al voegen ze er meteen aan toe dat het politieke programma van de SP geen enkel concreet plan of visie hiervoor

36 Voorbeelden zijn wetsvoorstellen met betrekking tot DNA, cameratoezicht, dataretentie, preventief fouilleren, identificatiemaatregelen, politiebevoegdheden en automatische kentekenherkenning.

37 *Kamerstukken II*, 2015, 34000 VII, nr. 21 (motie Segers/Oosenbrug).

geeft.[38] Een andere quickscan laat zien dat GroenLinks en D66 het meest gedetailleerd ingaan op privacy en per dossier (zoals zorg, rekeningrijden, IT) aangeven hoe ze de burger willen beschermen.[39]
Geen van de politieke partijen noemt expliciet nieuwe, meer gedetailleerde privacywetgeving of stevigere regulering in hun politieke programma's.[40] Dit suggereert dat ze voorstander zouden zijn van zelfregulering in plaats van overheidsregulering. Het kan echter ook het resultaat zijn van het feit dat de afgelopen jaren de focus lag op het voorbereiden van de Europese Algemene Verordening Gegevensbescherming (AVG, in het Engels General Data Protection Regulation, GDPR). Het aannemen van de AVG, de eis van de Tweede Kamer om periodiek te worden geïnformeerd over de voortgang van de onderhandelingen over de AVG en enkele maatregelen ter bescherming van persoonsgegevens voorafgaand aan de AVG (zoals meer bevoegdheden voor de Autoriteit Persoonsgegevens en wetgeving over de meldplicht datalekken), kunnen juist wijzen op een neiging naar stevigere regulering.
Nederland heeft een lange traditie op het gebied van mensenrechten (zie paragraaf 2.1). In 2013 lanceerde de Nederlandse overheid een nationaal actieplan voor mensenrechten.[41] Er is een actieve dialoog tussen de regering en het parlement enerzijds en burgerrechtenorganisaties anderzijds. In bepaalde gevallen, bij het voorbereiden van nieuwe wetgeving, raadpleegt de regering op actieve wijze mensenrechtenorganisaties.[42] Bovendien is er sprake van een actieve lobby door verschillende mensenrechtenorganisaties[43] om privacy en de bescherming van persoonsgegevens te verbeteren bij de overheid, waarbij onderwerpen regelmatig via de media worden geadresseerd. (Hierna volgt meer over burgerrechtenorganisaties die zich specifiek richten op privacy en de bescherming van persoonsgegevens.)
Het beleid van de huidige regering is min of meer dat wet- en regelgeving op het vlak van privacy en de bescherming van persoonsgegevens voorwaarden stellen waarmee rekening moet worden gehouden in wetgeving en beleid.[44] In de kabinetsreactie op het WRR-rapport iOverheid zet de regering eveneens in op de eigen verantwoordelijkheid van de burgers.[45] Het regeerakkoord van 2012 noemt expliciet dat de toezichthouder, de Autoriteit Persoonsgegevens, uitgerust moet worden met meer bevoegdheden tot het opleggen van boetes (hetgeen in 2016 is gerealiseerd met het aannemen van de Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid AP). Ook het

38 www.privacybarometer.nl.
39 Koning, B. de (2016), 'Welke partij heeft zijn beloftes over privacy het meest waargemaakt?', *De Correspondent*, 6 februari 2016.
40 D66 heeft sinds 1994 verzocht niet langer bevolkingsgegevens aan religieuze instellingen te verstrekken. In 2016 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties aangegeven dit te zullen regelen. Zie: www.kamerbrief-over-beeindiging-verstrekking-van-persoonsgegevens.pdf.
41 Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer, 'Aanbieding Nationaal Actieplan Mensenrechten', 10 december 2013.
42 *Kamerstukken II*, vergaderjaar 2015-2016, 32 761, nr. 102, p. 13.
43 Zie bijvoorbeeld de positie van Amnesty International in Nederland, http://jaarverslag.amnesty.nl/onze-werkwijze/amnesty-lobbyt/ en van Bits of Freedom, https://www.bof.nl/over-ons/.
44 Regeerakkoord (2012), Bruggen slaan, regeerakkoord VVD-PvdA, 29 oktober 2012, p. 22.
45 https://www.rijksoverheid.nl/documenten/kamerstukken/2011/10/25/kamerbrief-kabinetsreactie-wrr-rapport-ioverheid.

gebruik van zogeheten Privacy Impact Assessments (meer hierover in paragraaf 2.2) wordt als erg belangrijk beschouwd en wetgeving die inbreuken maakt op het recht op privacy zou horizonbepalingen moeten hebben en onderwerp van evaluaties moeten zijn.[46] Introductie van de Europese Algemene Verordening Gegevensbescherming (AVG) zal deze ontwikkelingen verder bevestigen.

Media-aandacht

In Nederland is er uitgebreide media-aandacht voor privacy en de bescherming van persoonsgegevens. Uiteraard is er aandacht voor internationale privacygerelateerde onderwerpen, zoals WikiLeaks en Snowden. Op nationaal niveau zijn privacy en de bescherming van persoonsgegevens belangrijke onderwerpen in het parlementaire debat, waardoor ze aandacht krijgen op tv en radio en in de kranten.[47] Sommige kranten, zoals De Telegraaf, lijken de laatste jaren steeds kritischer te staan tegenover *mass surveillance* en grootschalige opslag van gegevens. Privacy lijkt een kernwaarde in de meeste debatten te zijn, bijvoorbeeld in identiteitsmanagement.[48] Andere organisaties die regelmatig media-aandacht trekken op het vlak van privacy en de bescherming van persoonsgegevens zijn de toezichthouder (Autoriteit Persoonsgegevens, zie paragraaf 2.5)[49] en burgerrechtenorganisaties op het gebied van privacy en de bescherming van persoonsgegevens (zie hierna).[50] Ook opiniemakers en academici vragen aandacht voor deze onderwerpen via opiniestukken.[51]

Hoewel er geen breed maatschappelijk of nationaal debat is over privacy en de bescherming van persoonsgegevens, zijn er wel enkele initiatieven te noemen van nationale media tot het initiëren van een dergelijk debat. Een typisch voorbeeld is de Nationale Privacy Test, een tv-programma dat werd uitgezonden op 21 oktober 2016.[52] In dit programma werd kijkers een lijst met meerkeuzevragen voorgelegd, waaronder vragen over het gebruik van sociale media en veiligheidsvraagstukken. De testresultaten gaven het bewustzijnsniveau van de kijkers weer (d.w.z. of ze 'privacy-proof' waren). De Nationale Privacy Test was onderdeel van het zogeheten Privacyweken-initiatief van de nationale omroepen, waarin meer programma's over privacy en de bescherming

46 Regeerakkoord (2012), Bruggen slaan, regeerakkoord VVD-PvdA, 29 oktober 2012, p. 28.

47 Een typisch voorbeeld van deze media-aandacht is een verhaal waarin de sexvideo van een jonge vrouw op Facebook was gezet (zie http://nos.nl/op3/artikel/2129157-strijd-over-seksfilmpje-chantal-draait-opnieuw-om-privacy.html).

48 Andersson Elffers Felix (2013), Media-analyse identiteitsmanagement, Utrecht: AEF. http://www.aef.nl/aef-onderzoekt-identiteitsmanagement-in-europa.

49 Zie voor een overzicht https://autoriteitpersoonsgegevens.nl/nl/actueel.

50 Zie voor een overzicht de websites van deze burgerrechtenorganisaties.

51 Zie bijvoorbeeld Vries, J. de (2013), 'Blijf af van onze privacy', *Trouw*, 14 juni 2014, http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/3459001/2013/06/14/Blijf-af-van-onze-privacy.dhtml. Zie ook Custers, B.H.M. (2016), 'Etnisch profileren is wettelijk verboden en dat moet zo blijven', *Trouw*, 7 juni 2016, p. 17.

52 http://www.npo.nl/npo3/de-privacytest-hoe-privacybewust-ben-jij.

van persoonsgegevens werden uitgezonden op tv.[53] Een ander tv-programma was een openbaar hoorcollege van mr. dr. Bart Schermer van de Universiteit Leiden.[54]
Ook zijn er enkele journalisten die zich verder gespecialiseerd hebben in de onderwerpen privacy en bescherming van persoonsgegevens en aanverwante onderwerpen. Typische voorbeelden zijn privacyjournalisten Maurits Martijn en Dimitri Tokmetzis, die medepresentator waren van bovengenoemde Nationale Privacy Test en een populariserend boek over privacy schreven.[55] Een ander voorbeeld is journalist Brenno de Winter, die gespecialiseerd is in informatiebeveiliging en privacy en beveiligingsproblemen blootlegde bij de OV-chipkaart.[56] Soms nemen ook hackers deel aan het maatschappelijk debat. Een bekend voorbeeld is Rop Gonggrijp, die deelnam aan het debat over elektronische stemmachines.[57] Verder zijn er ook politici die zich proberen te onderscheiden door zich op privacy te richten. Een typisch voorbeeld is Sophie in 't Veld, Nederlands Europarlementariër, die zich richt op privacy en de bescherming van persoonsgegevens. Een ander voorbeeld is voormalig model Ancilla van der Leest, die als politica de Piratenpartij aanvoerde en daarbij privacyrechten als hoofdthema naar voren trachtte te schuiven.[58]
Een ander belangrijk mediamoment in deze context zijn de jaarlijkse Big Brother Awards. Deze prijzen worden uitgereikt aan organisaties en personen binnen de overheid en de private sector die het meest hebben gedaan om de persoonlijke privacy te bedreigen. Deze prijzen bestaan in meerdere landen, waaronder Duitsland en de Verenigde Staten.[59] De Nederlandse variant wordt georganiseerd door burgerrechtenorganisatie Bits of Freedom.[60] Categorieën zijn onder meer prijzen toegekend door het publiek en prijzen toegekend door deskundigen. Recentelijk is ook een prijs geïntroduceerd voor een positieve bijdrage aan privacy en de bescherming van persoonsgegevens. Door de bank genomen is de houding van de media ten opzichte van privacy en de bescherming van persoonsgegevens kritisch. Problemen worden aan de kaak gesteld en zorgen worden geadresseerd. Wetsvoorstellen, beleid en praktijken van zowel overheden als bedrijven worden bekritiseerd. Daarmee dragen de media aanzienlijk bij aan het creëren van bewustzijn bij een breed publiek. Het opperen van oplossingen voor de geschetste problemen is echter zeldzaam.[61] Er zijn aanwijzingen dat dit mensen verward achterlaat: hoewel mensen bezorgd zijn over hun privacy, vertonen ze geen gedrag dat deze zorgen weerspiegelt (de zogeheten privacyparadox).[62]

---

53 http://www.metronieuws.nl/nieuws/showbizz/2016/10/privacyweken-op-npo3-veel-heftiger-dan-ik-dacht.
54 http://www.universiteitvannederland.nl/hoogleraar/bart-schermer/.
55 Martijn, M., en Tokmetzis, D. (2016), *Je hebt wel iets te verbergen*. Amsterdam: De Correspondent BV.
56 https://nl.wikipedia.org/wiki/Brenno_de_Winter.
57 http://wijvertrouwenstemcomputersniet.nl/Wij_vertrouwen_stemcomputers_niet.
58 Van der Leest (2014), 'We zijn allemaal naakt, Joop.nl, 3 september 2014. Zie http://www.joop.nl/opinies/we-zijn-allemaal-naakt.
59 https://en.wikipedia.org/wiki/Big_Brother_Awards
60 https://bigbrotherawards.nl/.
61 Hulshof, M., en Veen, M. van der (2017), 21 ideeën voor een beter internet, *de Volkskrant*, 17 juni 2017. http://www.volkskrant.nl/media/21-ideeen-voor-een-beter-internet~a4501135/.
62 Norberg, P.A., Horne, D.R., and Horne, D.A. (2007), 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors', *Journal of Consumer Affairs*, Vol. 41, No.1, p. 100-126.

Datalekken

Burgerrechtenorganisatie Bits of Freedom hield een overzicht bij van datalekken in Nederland van 2009 tot 2013.[63] Dit is een lange lijst van ziekenhuizen, telecomaanbieders, luchtvaartmaatschappijen en andere bedrijven bij wie persoonsgegevens werden gelekt. In sommige gevallen werden gegevens van duizenden personen gelekt, in andere gevallen werden gegevens van honderdduizenden personen gelekt. Melden van zulke datalekken was echter niet verplicht in Nederland, tot januari 2016. Sinds die datum moeten datalekken worden gemeld bij de toezichthouder (Autoriteit Persoonsgegevens). In de eerste week van 2016 werden 20 datalekken gerapporteerd. In april 2016 waren inmiddels meer dan duizend meldingen ontvangen.[64] In september stond de teller boven de 3.600 datalekken. Op dat moment had 44% van alle Nederlandse gemeenten (172 van de 390) reeds een datalek gemeld. Aan het eind van 2016 liet de Autoriteit Persoonsgegevens (AP) in een persbericht weten dat ze in 2016 in totaal bijna 5.500 meldingen van datalekken had ontvangen.[65] Uit het jaarverslag 2016 van de AP blijkt dat er 5.693 datalekken werden gemeld.[66] De top drie van sectoren met de meeste datalekken bestond uit gezondheid & welzijn, financiële dienstverlening en openbaar bestuur. Voor het eerste kwartaal van 2017 zijn 2.317 datalekken gemeld.[67]

Een van de grootste datalekken betrof een medewerker van Netbeheer Nederland, een bedrijf dat het energienetwerk beheert, die gegevens had gestolen van 2 miljoen Nederlandse huishoudens.[68] Een ander voorbeeld is het UWV, waar gegevens van 11.000 mensen die op zoek waren naar een nieuwe baan werden gelekt.[69] Het snel toenemende aantal meldingen van datalekken impliceert dat datalekken niet langer nieuws zijn. Sommige deskundigen hebben al gesteld dat daardoor een van de veronderstelde mechanismen achter de meldplicht datalekken (namelijk dat *naming & shaming*-organisaties zou dwingen hun beveiliging te verbeteren) slechts beperkt effect zal hebben.[70] Bovendien lijkt het nieuws over datalekken weinig reacties los te maken onder de bevolking. Er zijn in elk geval geen protesten of publieke reacties van woede geweest.

Burgerrechtenorganisaties

In Nederland zijn verschillende burgerrechtenorganisaties actief in het veld van privacy en de bescherming van persoonsgegevens. Het meest bekend zijn Bits of Freedom en Privacy First. Bits of Freedom noemt zichzelf de meest toonaangevende Nederlandse digitale burgerrechtenbeweging.[71] Haar focus ligt bij informationele zelfbeschikking.

63 https://www.bof.nl/category/zwartboek-datalekken/.

64 https://informatiebeveiliging.nl/nieuws/autoriteit-persoonsgegevens-1-000-datalek-meldingen/.

65 http://nos.nl/artikel/2150430-5500-datalekken-gemeld-bij-waakhond.html.

66 AP (2017), *Jaarverslag 2016*, Den Haag: AP, p. 7. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2016.pdf.

67 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/overzicht_meldingen_datalekken_q1_2017.pdf.

68 https://informatiebeveiliging.nl/nieuws/grootste-datalek-energiecontracten-ooit-in-nederland/.

69 https://informatiebeveiliging.nl/nieuws/uwv-lekt-gegevens-van-11-000-werkzoekenden/.

70 ZIe ook: Schneier, B. (2009), 'State Data Breach Notification Laws: Have They Helped?', *Information Security*, January 2009.

71 https://www.bof.nl/home/english-bits-of-freedom/.

Haar belangrijkste doel is een internet dat open is voor iedereen, waar iedereen informatie kan blijven delen en waar privécommunicatie ook privé blijft. Bits of Freedom bestaat sinds 2000 en is medeoprichter van European Digital Rights (EDRi). Ze is wellicht het meest bekend vanwege het organiseren van de jaarlijkse Big Brother Awards (zie hiervoor), maar ze organiseert ook voorlichtingsbijeenkomsten onder de naam privacy cafés en ontwikkelde een *Internet freedom toolbox* waarmee persoonsgegevens veilig en privé blijven.[72] Verder is ze actief in lobbyen, het politieke debat en rechtszaken. Bits of Freedom is gevestigd in Amsterdam en is een non-profitorganisatie die wordt gefinancierd met particuliere donaties. In de periode 2006-2009 werden haar activiteiten opgeschort vanwege een gebrek aan financiën.[73]

Privacy First stelt dat het recht op privacy onder grote druk staat en verdedigd moet worden.[74] Haar doel is om van Nederland een gidsland te maken als het aankomt op de bescherming van privacy. De nadruk ligt op vier punten: privacy als startpunt voor innovatie, zorgen dat mensen echt vrije keuzes hebben, Nederland tot gidsland voor privacy maken en zorgen dat overheden en bedrijven verantwoordelijkheid nemen voor privacy.[75] Privacy First organiseert voorlichtingscampagnes,[76] maar voert ook rechtszaken, hoewel meestal in samenwerking met andere organisaties.[77] In 2015 klaagde Privacy First de Nederlandse overheid aan voor de opslag van vingerafdrukken in paspoorten. Hoewel Privacy First deze rechtszaak verloor in de rechtszaal, schortte de regering deze praktijk toch op.[78] Andere rechtszaken betreffen onder meer het verstrekken van gegevens door Nederlandse inlichtingen- en veiligheidsdiensten aan andere landen, kentekenparkeren en dataretentie. Privacy First is gevestigd in Amsterdam en is een non-profitorganisatie die wordt gefinancierd door particuliere donaties. Haar jaarlijks budget was ongeveer 80.000 euro in 2015.[79] Sinds 2015 reikt Privacy First ook jaarlijkse prijzen uit, de zogeheten Nationale Privacy Innovatie Awards, voor privacyvriendelijke oplossingen.[80] Tot dusver hebben deze awards minder media-aandacht getrokken dan de Big Brother Awards.

Wellicht minder bekend bij het grote publiek is de Vereniging Privacy Recht (VPR), een vereniging die een platform biedt voor het bevorderen van de kwaliteit van wetgeving op het terrein van privacy en de bescherming van persoonsgegevens.[81] Deze vereniging heeft als leden onder meer praktijkjuristen, privacy consultants en academici. Afgezien van het verder ontwikkelen van privacyrecht tracht de vereniging een gesprekspartner te zijn voor de toezichthouders en beleidsmakers. Haar activiteiten bestaan onder meer uit het organiseren van een jaarlijks congres, bijeenkomsten en seminars. Het voeren

72 https://www.bof.nl/ons-werk/onze-successen/.
73 http://webwereld.nl/security/31687-bits-of-freedom-stopt-per-1-september.
74 https://www.privacyfirst.nl/.
75 Privacy First (2015), Visie op privacy 2.0, visiedocument, Amsterdam: Privacy First. Zie: https://www.privacyfirst.nl/index.php?option=com_k2&view=item&layout=item&id=117&Itemid=156.
76 https://www.privacyfirst.nl/campagnes.html.
77 https://www.privacyfirst.nl/rechtszaken.html.
78 Privacy First (2016), *Jaarverslag 2015*, Amsterdam: Privacy First, juni 2016, p. 2.
79 Privacy First (2016), *Jaarverslag 2015*, Amsterdam: Privacy First, juni 2016, p. 25.
80 https://www.privacyfirst.nl/solutions/evenementen/item/1044-winnaars-iir-nationale-privacy-innovatie-awards-2016.html.
81 https://verenigingprivacyrecht.nl/.

van rechtszaken is geen onderdeel van haar activiteiten. De vereniging is gevestigd in Rotterdam. Het is een non-profitorganisatie en lidmaatschap staat open voor iedereen behalve personen die verbonden zijn aan toezichthouders op het gebied van privacy en bescherming van persoonsgegevens en beleidsmakers. Het lidmaatschap bedraagt 75 euro per jaar.[82]
De Nederlandse afdeling van de International Commission of Jurists (ICJ) heet het NJCM (Nederlands Juristen Comité voor de Mensenrechten) en is opgericht in 1974.[83] De ICJ is een non-gouvernementele organisatie die zich toelegt op het verzekeren van respect voor internationale mensenrechtenstandaarden via het recht. Er zijn nationale afdelingen en geassocieerde organisaties in meer dan 70 landen. De Nederlandse afdeling, het NJCM, publiceert commentaar op voorgenomen wetgeving en overheidsbeleid, schrijft en coördineert schaduwrapporten en voert een lobby bij politici, journalisten, beleidsmakers en maatschappelijke organisaties. Het NJCM publiceert ook een tijdschrift en een bulletin en organiseert seminars. De focus ligt op mensenrechten, niet op privacy en de bescherming van persoonsgegevens in het bijzonder, maar deze rechten liggen wel binnen zijn werkterrein. Het NJCM is een non-profitorganisatie die een jaarlijks budget had van ongeveer 131.000 euro in 2015.[84] De organisatie is gevestigd in Leiden.
Gesteld kan worden dat Bits of Freedom en Privacy First meer de nadruk leggen op een activistische benadering en het voeren van rechtszaken, terwijl de VPR en het NJCM meer de nadruk leggen op het organiseren en het faciliteren van het debat. Alle spelen ze een rol in het beïnvloeden van overheidsbeleid en in bepaalde gevallen raadpleegt de regering hen bij voorgestelde of voorgenomen wetgeving. Bits of Freedom is de meest bekende organisatie in dit domein (18% van de Nederlanders heeft van haar gehoord), gevolgd door Privacy First (13% van de Nederlanders heeft van haar gehoord).[85]

2.2 Beleid

Nationaal beleid, Privacy Impact Assessments
In de vorige paragraaf is het algemene beleid van de overheid op het terrein van privacy en bescherming van persoonsgegevens aan bod gekomen. Sectorspecifieke wetgeving en bijbehorend beleid is aanwezig in veel domeinen. Bijvoorbeeld in de strafrechtsketen is er specifieke wet- en regelgeving (zie paragraaf 2.3) die aan de meer algemene Wet bescherming persoonsgegevens derogeert. Ook in de medische sector is er specifieke wetgeving die het medisch beroepsgeheim regelt. Sectorspecifieke regelgeving is ook aanwezig voor de overheid, sociale zaken en sociale zekerheid. Het beleid in deze domeinen is doorgaans strikter, omdat het bijzondere (meer gevoelige) categorieën gegevens betreft. Ook is in sommige gevallen sprake van een verplichte relatie tussen burger en overheid, waardoor regels meer gedetailleerd zijn uitgewerkt.

82 https://verenigingprivacyrecht.nl/lid-worden/.
83 http://www.njcm.nl/site/njcm/vereniging/vereniging.
84 NJCM (2016), *Financieel jaarverslag 2015*, Leiden: NJCM. Zie: http://www.njcm.nl/site/njcm/vereniging/vereniging.
85 Roosendaal, A., Nieuwenhuis, O., Ooms, M., Bouman-Eijs, A., en Huijboom, N. (2015), *Privacybeleving op het internet in Nederland*, Den Haag: TNO, p. 39.

Privacy Impact Assessments (PIA's) worden steeds belangrijker in Nederland, al zijn ze nog niet wettelijk verplicht. Zoals aangeven in de vorige paragraaf dienden parlementsleden in 2011 en 2015 moties in met het verzoek een Privacy Impact Assessment uit te voeren voor wetsvoorstellen die consequenties hebben voor het verwerken van persoonsgegevens.[86] De regering heeft deze motie aangenomen. Als resultaat daarvan werd in 2013 de eerste Privacy Impact Assessment uitgevoerd door de Nederlandse overheid, voor een wetsvoorstel voor de opslag van kentekengegevens met een technologie die bekend staat als Automated Number Plate Recognition (ANPR).[87] Later datzelfde jaar kwam de Nederlandse regering met een voorstel voor een gestandaardiseerd model voor het uitvoeren van Privacy Impact Assessments, een model dat sinds 1 september 2013 verplicht is voor de rijksoverheid.[88] Dit model zet aan tot meer bewustwording van mogelijke privacyrisico's, maar is niet erg gebruikersvriendelijk. Een ander bezwaar van dit model is dat er geen instrumenten worden geboden om risico's op gesystematiseerde wijze in kaart te brengen en ook niet om een inschatting te maken van de waarschijnlijkheid dat bepaalde geïdentificeerde risico's zich daadwerkelijk voordoen en wat vervolgens de impact is als deze risico's zich daadwerkelijk voordoen.[89] Daarmee is het model vooral een *compliance check*, een toets om na te gaan of aan de wetgeving wordt voldaan, aldus de Autoriteit Persoonsgegevens die advies uitbracht over het model.[90] Het standaardmodel lijkt niet vaak gebruikt te worden: latere Privacy Impact Assessments ontwikkelen gewoon weer hun eigen aanpak.[91] Het model voor Privacy Impact Assessments van de rijksdienst is geëvalueerd en wordt op dit moment opnieuw geijkt.[92] Uit de evaluatie blijkt dat er ruimte voor verbetering is omtrent praktische toepasbaarheid, volledigheid, begrijpelijkheid en bruikbaarheid, en gebruikersvriendelijkheid. Anderen hebben modellen ontwikkeld die meer praktisch zijn, zoals het model van NOREA, de vereniging van IT-professionals.[93] Dit model bevat een uitgebreide checklist die beter garandeert dat de risicoanalyse ook echt volledig is. De Autoriteit Persoonsgegevens heeft zelf geen model ontwikkeld voor het uitvoeren

86 *Kamerstukken II*, 2015, 34 000 VII, nr. 21 (motie Segers/Oosenbrug).

87 *Kamerstukken II*, 2012-2013, 33 542, nr. 3, bijlage 6.

88 https://www.rijksoverheid.nl/documenten/publicaties/2013/06/24/toetsmodel-privacy-impact-assessment-pia-rijksdienst.

89 Een kwalitatief goede PIA brengt niet alleen risico's in kaart, maar maakt ook een inschatting van de kans en impact van deze geïdentificeerde risico's; zie Wright, D., en Hert, P. de (2012), *Privacy Impact Assessment*. Heidelberg: Springer. Verder is het doorgaans ook wenselijk, als risico's eenmaal inzichtelijk zijn gemaakt, om tevens maatregelen te nemen die de risico's kunnen vermijden of verkleinen.

90 Brief van het CBP aan de minister van BZK, 4 dec 2012 (Advies – concept Toetsmodel Privacy Impact Assessment). Zie https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-impact-assessment-pia.

91 Zie bijvooreeld Koops, B.J., Roosendaal, A., Kosta, E., Lieshout, M. van, en Oldhoff, E. (2016), *Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX*, Delft: TNO. Zie https://www.rijksoverheid.nl/documenten/rapporten/2016/02/12/privacy-impact-assessment-wet-op-de-inlichtingen-en-veiligheidsdiensten-20xx.

92 Versmissen, J.A.G. Terstegge, J.H.J., Siemers, K.M., en Tran, T.H. (2016), *Evaluatie Toetsmodel PIA Rijksdienst*. Utrecht: Privacy Management Partners.

93 http://www.norea.nl/Norea/Actueel/Nieuws/PIA+nieuwe+versie.aspx.

van Privacy Impact Assessments, maar biedt wel informatie op de website, waaronder de richtlijnen van de Artikel 29 Werkgroep.[94]

Privacy en de bescherming van persoonsgegevens in nieuw beleid

In het parlement zijn er geen debatten die speciaal gewijd zijn aan nieuwe technologische ontwikkelingen zoals big data, het Internet of Things (IoT) of de quantified self (het vastleggen van persoonsgegevens uit het dagelijks leven, zoals voeding, luchtkwaliteit, stemmingen, bloeddruk en sportprestaties, met wearables, draagbare apparaten als smartwatches en smartphones).[95] Niettemin spelen deze onderwerpen wel een rol bij andere debatten, bijvoorbeeld over de economie en bij justitie. De regering heeft weliswaar nog geen integrale beleidsvisie ontwikkeld omtrent deze nieuwe technologische ontwikkelingen, maar heeft wel al onderzoeksinstituten van de overheid onderzoek laten uitvoeren naar deze onderwerpen en op verschillende onderdelen al kabinetsstandpunten en beleidsvisies geformuleerd waarin uitgangspunten voor een bredere visievorming zijn terug te vinden.[96] De meeste aandacht is tot dusver uitgegaan naar de ontwikkelingen omtrent big data. Zo heeft de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) een uitgebreid onderzoeksprogramma opgestart naar big data. Recente voorbeelden van WRR-rapporten zijn onder meer een overzichtsstudie[97] en rapporten naar meer specifieke onderwerpen zoals data en veiligheid,[98] internationale rechtsvergelijking naar big data,[99] big data en fraudebestrijding,[100] big data voor inlichtingen- en veiligheidsdiensten[101] en big data in de gezondheidszorg.[102] De Nederlandse regering heeft op deze onderzoeken gereageerd en aangegeven dat big data veel kansen en mogelijkheden biedt die de regering verder wil verkennen, inclusief bijkomende risico's en hoe die risico's geadresseerd zouden moeten worden.[103] Het ministerie van Onderwijs,

94 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/privacy-impact-assessment-pia.

95 In 2014 diende SP-senator Gerkens in de Eerste Kamer een motie in die de regering verzocht het Rathenau Instituut te laten onderzoeken of een ethische commissie noodzakelijk is in de voortschrijdende digitaliserende samenleving. Zie *Kamerstukken I*, vergaderjaar 2014-2015, CVIII, E. Dit rapport is inmiddels beschikbaar; zie: Kool, L., Timmer, J., Royakkers, L. en Van Est, R. (2017), *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*. Den Haag: Rathenau Instituut. Zie https://www.rathenau.nl/nl/file/2797/Opwaarderen_Rathenau_Instituut.pdf.

96 Zie bijvoorbeeld Van der Leij, J.B.J. (2015), *Privacyrecht en slachtoffers. Een studie naar de grondslagen en juridische kaders van privacy van slachtoffers*. (WODC) Den Haag: Boom Uitgevers; Malsch, M., Dijkman, N. & Akkermans, A. (2015), *Het zichtbare slachtoffer. Privacy van slachtoffers binnen het strafproces*. (WODC/NSCR/VU) Boom Uitgeverij.

97 Sloot, B. van der, Broeders, D., & Schrijvers, E. (2016), *Exploring the Boundaries of Big Data*. Amsterdam: Amsterdam University Press.

98 WRR (2016), *Big data in een vrije en veilige samenleving*. Amsterdam: Amsterdam University Press.

99 Sloot, B. van der, Schendel, S. van (2016), *International and comparative legal study on Big Data*. The Hague: WRR.

100 Olsthoorn, P. (2016), *Big data voor fraudebestrijding*. The Hague: WRR.

101 Schendel, S. van (2016), *Het gebruik van Big Data door de mivd en aivd*. The Hague: WRR.

102 Ottes, L. (2016), *Big Data in de zorg*. The Hague: WRR.

103 Ministerie van Veiligheid en Justitie (2016), Kabinetsstandpunt over het WRR-rapport Big Data in een vrije en veilige samenleving, brief van de minister van veiligheid en justitie aan de Tweede Kamer, 11 november 2016.

Cultuur en Wetenschap heeft onderzoek laten uitvoeren naar big data in onderwijs en wetenschap.[104] In een officiële reactie geeft de regering aan dat deze ontwikkelingen kansen bieden, maar ook risico's met zich meebrengen en dat verdere ontwikkelingen nauwgezet zullen worden gevolgd.[105] Het ministerie van Economische Zaken richtte in 2015 een expertgroep op die een rapport heeft opgesteld over big data en innovatie.[106] In een kabinetsreactie heeft de regering laten weten dit rapport te zullen gebruiken voor verdere discussie over dit onderwerp.[107]
Onderzoek naar het Internet of Things is verzocht door de Cyber Security Raad en opgestart door het WODC, het Wetenschappelijk Onderzoek- en Documentatie Centrum van het ministerie van Veiligheid en Justitie.[108] Wat betreft de 'quantified self'-beweging heeft datzelfde WODC onderzoek opgestart naar toepassingen van de quantified self in de context van justitie.[109] De voordelen en risico's (waaronder risico's voor de privacy en de bescherming van persoonsgegevens) van andere technologieën, zoals nanotechnologie,[110] bitcoins[111] en drones[112], worden ook nauwgezet gevolgd door de overheid. In sommige gevallen ligt er reeds een kabinetsvisie of -standpunt, zoals in het geval van nanotechnologie[113] en drones[114].
De Nederlandse overheid heeft ook belangstelling getoond voor het gebruik van het principe van Privacy by Design en heeft een actieplan voor de privacy laten opstellen.[115] Ondanks het voornemen meer gebruik te maken van Privacy by Design is het niet duidelijk waar en hoe deze plannen zijn geïmplementeerd. Bovendien lijkt het niet standaard onderdeel uit te maken van overheidsbeleid. Onderzoek naar factoren die het gebruik van Privacy by Design in Nederland kunnen bevorderen of juist hinderen, hebben vooralsnog niet geleid tot een toename in het gebruik van Privacy by Design.[116]

---

104 Bongers, F., Jager, C.J., & Velde, R. te (2015), *Big data in onderwijs en wetenschap*. Utrecht: Dialogic.
105 Ministerie van Onderwijs, Cultuur en Wetenschap (2016), Big data in onderwijs, cultuur en wetenschap, brief van de minister van Onderwijs, Cultuur en Wetenschap aan de Tweede Kamer, 28 juni 2016.
106 Expertgroep EZ (2016). *Licht op de digitale schaduw. Verantwoord innoveren met big data*, Den Haag: ministerie van economische zaken.
107 Ministerie van Economische Zaken (2016), Aanbieding rapport expertgroep big data en privacy, brief van de minister van Economische Zaken aan de Tweede Kamer, 4 oktober 2016.
108 https://www.wodc.nl/onderzoeksdatabase/2734-kansen-en-bedreigingen-internet-of-things.aspx.
109 https://www.wodc.nl/onderzoeksdatabase/2716a-quantified-self-toepassingsmogelijkheden-in-justitiele-context.aspx?cp=44&cs=6778.
110 Schulze Greiving, V., Kulve, H. te, Konrad, K., Kuhlman, S., Pinkse, P. (2016), *Nanotechnologie in dienst van veiligheid en justitie*. Twente: Universiteit Twente, Department of Science, Technology and Policy Studies (STePS).
111 Oerlemans, J.J., Custers, B.H.M., Pool, R.L.D., & Cornelisse, R. (2016), *Cybercrime en witwassen. Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*. Den Haag: Boom Juridische Uitgevers.
112 Custers, B.H.M., Oerlemans, J.J., Vergouw, S.J. (2015), *Het gebruik van drones. Een verkennend onderzoek naar onbemande luchtvaartuigen*. Meppel: Boom Lemma Uitgevers.
113 https://www.rijksoverheid.nl/documenten/rapporten/2006/11/16/kabinetsvisie-nanotechnologie.
114 *Kamerstukken II*, vergaderjaar 2014-2015, 30 806, nr. 28.
115 Roosendaal, A., Lieshout, M. van, Cuijpers, C., & Leenes, R. (2014), *Actieplan privacy*. Den Haag: TNO.
116 Lieshout, M. van, Kool, L., Bodea, G., Schlechter, J., & Schoonhoven, B. van (2012), *Stimulerende en remmende factoren van Privacy by Design in Nederland*. Delft: TNO.

Verder is sinds 2014 een zogeheten Digicommissaris aangesteld.[117] Dit is een regeringscommissaris belast met een speciale taak namens de regering. De Nationale Commissaris Digitale Overheid heeft als taak de overheidsbrede digitale basisinfrastructuur van Nederland robuust en toekomstbestendig te maken, de sturing hierop te versterken met een passend governance- en financieringsarrangement en om een stevige overheidsbrede agenda op te stellen om het gebruik van de digitale dienstverlening aantrekkelijker te maken en verder te laten toenemen.[118] Uit een recente evaluatie blijkt dat deze, mede door het complexe werkveld, nog veel werk te doen heeft.[119]

Maatschappelijk debat

De Nederlandse overheid lijkt een actieve benadering te kiezen in het privacydebat. Soms lijkt het echter lastig uitgangspunten voor privacy en de bescherming van persoonsgegevens te vertalen in concrete maatregelen die kunnen worden genomen. Concepten als *Privacy by Design* en *Privacy Impact Assessments* zijn niet (of niet voldoende) gestandaardiseerd en worden niet of niet altijd meegenomen wanneer nieuwe wetgeving of nieuw beleid wordt ontwikkeld.[120] In veel discussies wordt weliswaar het belang van privacy en de bescherming van persoonsgegevens onderstreept, maar vaak is er geen sprake van een diepgaand debat, verdere opvolging en concrete maatregelen. Zoals besproken in de vorige paragraaf is er tot op zekere hoogte sprake van een dialoog tussen de overheid en burgerrechtenorganisaties, maar dit heeft het probleem niet opgelost. In 2015 heeft zich een zogeheten privacycoalitie gevormd tussen verschillende personen en organisaties vanuit burgerrechten, journalistiek, strafrecht en wetenschap.[121] De overheid is een dialoog gestart met deze coalitie over onder meer onderwerpen als de opslag van gegevens[122] en big data[123] en lijkt voornemens te zijn deze dialoog voort te zetten.

Bij het opstellen van nieuw beleid en nieuwe wetgeving maakt de Nederlandse overheid in toenemende mate gebruik van internetconsultaties waarbij burgers en bedrijven kunnen reageren op de voorstellen.[124] Middels de internetconsultaties die zijn gestart in 2008 beoogt de overheid burgers, bedrijven en andere organisaties informatie te verschaffen over wetsvoorstellen en mensen uit te nodigen hierop te reageren. De achterliggende gedachte is dat hiermee de beleids- en wetsvoorstellen verder kunnen worden verbeterd en het draagvlak kan worden vergroot. Mensen moeten zich registreren alvorens ze kunnen reageren, maar kunnen ervoor kiezen dat hun reactie niet zichtbaar is voor anderen en dus niet openbaar is. De naam en woonplaats van de

117 https://www.digicommissaris.nl/.

118 *Kamerstukken II*, vergaderjaar 2013-2014, 26643, nr. 314.

119 Veld, P., Meijer, A., Schurink, M (2017), *De Digidelta: samen versnellen. Evaluatie van de nationale commissaris digitale overheid*. Den Haag: ABDTopconsult. Zie https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-evaluatie-nationaal-commissaris-digitale-overheid.

120 De rijksoverheid heeft een gestandaardiseerde model voor Privacy Impact Assessments ontworpen, maar dit is niet op bedrijven gericht. Zie verder de discussie eerder in deze paragraaf over dit model, dat inmiddels geëvalueerd is en wordt herijkt.

121 https://visieopprivacy.nl/.

122 http://nos.nl/artikel/2028170-privacycoalitie-stop-op-wetgeving-dataopslag.html.

123 *Kamerstukken II* 2014-2015, 32 761, nr. 83, blz. 4.

124 www.overheidsconsultatie.nl.

persoon die reageert worden gepubliceerd, samen met het commentaar, tenzij de betreffende persoon daartegen bezwaar maakt. Internetconsultaties zijn een aanvulling op het bestaande consultatieproces voor wetgeving (en veel beleid), waarbij overheidsinstellingen die geraakt worden door de voorstellen vooraf worden geraadpleegd. Hoewel de overheid regelmatig gebruikmaakt van internetconsultaties en ervan overtuigd is dat dit nuttig is, hebben veel consultaties hetzelfde format en is het vaak dezelfde groep mensen die reageert. Er is geen eenduidig overheidsbeleid voor internetconsultaties en ministeries kunnen in beginsel zelf beslissen of ze wel of niet een internetconsultaties organiseren, wie ze daarbij consulteren en hoe dat gebeurt.[125] Dit laat onverlet dat bepaalde instanties moeten worden geconsulteerd. Bij de bescherming van persoonsgegevens is er een wettelijke plicht de AP om advies te vragen.

Informatiecampagnes

In de afgelopen jaren heeft de rijksoverheid verschillende internetcampagnes gevoerd teneinde burgers verder te informeren over privacy en de bescherming van persoonsgegevens en het bewustzijn verder te vergroten. In 2008 startte de overheid de website www.mijnoverheid.nl waarop burgers zaken met de overheid online kunnen regelen. In 2015 waren er 1,6 miljoen burgers met een account. Wanneer burgers inloggen, krijgen ze toegang tot hun persoonsgegevens, bijvoorbeeld tot gegevens uit de Basisregistratie Personen (BRP), voertuiggegevens bij de Dienst Wegverkeer (RDW) en perceel- of eigendomsgegevens van hun huis bij het Kadaster.[126]

In oktober 2016 lanceerde de overheid de campagne Alert Online, bedoeld om de kennis en vaardigheden van burgers over cybercrime te verbeteren.[127] Dit is niet de eerste campagne met dit doel, maar deze campagne is in het bijzonder gericht op ransomware[128] en adviseert om regelmatig back-ups te maken, software te updaten en nooit bijlagen en links te openen in e-mails.[129] In de campagne is bijzondere aandacht voor de bescherming van persoonsgegevens.[130]

In 2014 werd de campagne Veilig internetten gestart.[131] Deze campagne bestond vooral uit een website (www.veiliginternetten.nl) met praktische adviezen over wat wel en niet te doen om veilig te zijn op het internet. De website verschaft alleen informatie, het is geen helpdesk. Speciale aandachtsgebieden in de campagne zijn basisbeveiliging, draadloos internet, sociale media, internetbankieren, online winkelen, privacy en kin-

125 Sandee, R. (2014), 'Het zwarte gat van de internetconsultatie', *SC Online*, 28 oktober 2014. Zie: http://www.sconline.nl/achtergrond/het-zwarte-gat-van-de-internetconsultatie.

126 https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/wat-is-mijnoverheid.

127 https://www.rijksoverheid.nl/actueel/nieuws/2016/10/03/nederlanders-niet-voorbereid-op-cybercrime.

128 Zie voor meer over ransomware Custers B.H.M., J.J. Oerlemans & Pool R.L.D. (2016), 'Ransomware, cryptoware en het witwassen van losgeld in Bitcoins', *Strafblad* 14(2): 87-95 of J.J. Oerlemans, Custers B.H.M., Pool R.L.D. & Cornelisse R. (2016), *Cybercrime en witwassen. Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*. Onderzoek en beleid WODC nr. 319. Meppel: Boom Criminologie.

129 https://www.alertonline.nl/.

130 https://www.alertonline.nl/experts/bescherming-persoonsgegevens.

131 https://www.rijksoverheid.nl/actueel/nieuws/2014/10/27/burgers-beter-geinformeerd-over-veilig-internetten.

deren online.[132] Binnen het aandachtsgebied privacy ligt de nadruk op het beschermen van persoonsgegevens, sociale media, identiteitsfraude, digitale sporen en het delen van bestanden.[133]
In 2013 lanceerde de overheid een campagne over identiteitsfraude.[134] Deze campagne verspreidde digitaal informatiemateriaal naar gemeentes (aangezien die paspoorten en identiteitsbewijzen uitgeven) om burgers te informeren over wat wel en niet te doen met kopieën van hun identiteitsdocumten, inclusief het uitwissen van hun burgerservicenummer op de kopieën. In 2014 startte de Nederlandse overheid ook met de zogenoemde KopieID app, een app die burgers de mogelijkheid biedt een veilige kopie van hun identiteitsdocumenten te maken op hun mobiele telefoon. De app maakt het mogelijk het burgerservicenummer te verwijderen en een watermerk aan te brengen op de digitale kopie van het identiteitsdocument, zodat de herkomst van de kopieën traceerbaar is in geval van misbruik door fraudeurs.[135]

2.3 Wet- en regelgeving

Implementatie van de EU-richtlijn
De eerste wet in Nederland die zich specifiek richtte op de bescherming van persoonsgegevens was de Wet persoonsregistraties (Wpr), die van kracht werd in 1989. De handhaving van deze wet was in handen van de toenmalige Registratiekamer, de eerste toezichthouder in het domein van privacy en de bescherming van persoonsgegevens en voorloper van het College bescherming persoonsgegevens (CBP). In 2016 werd het CBP omgedoopt tot de Autoriteit Persoonsgegevens (zie volgende paragraaf).
In Nederland is de Europese richtlijn voor de bescherming van persoonsgegevens (EU-richtlijn 95/46/EC) in nationale wetgeving geïmplementeerd door de introductie van de Wet bescherming persoonsgegevens (Wbp), die van kracht is sinds 1 september 2001.[136] Een belangrijk verschil tussen de Wbp en diens voorloper, de Wpr, is dat de Wpr was gebaseerd op het begrip persoonsregistraties, terwijl de Wbp is gebaseerd op het begrip persoonsgegevens. De Wbp implementeert de zogeheten *principles for the fair processing of personal data* (beginselen voor een eerlijke verwerking van persoonsgegevens)[137], biedt een limitatieve opsomming van rechtvaardigingsgronden waarop

132 https://veiliginternetten.nl/themes/.
133 https://veiliginternetten.nl/themes/privacy/.
134 https://www.rijksoverheid.nl/actueel/nieuws/2013/01/15/campagne-tegen-identiteitsfraude.
135 https://www.rijksoverheid.nl/actueel/nieuws/2014/11/04/kopieid-app-maakt-misbruik-met-kopie-identiteitsbewijs-moeilijker.
136 Zie http://wetten.overheid.nl/BWBR0011468/2016-01-01. De deadline van drie jaar voor het implementeren van deze Europese richtlijn was toen al lang verstreken, op 24 oktober 1998. In januari 2001 besloot de Europese Commissie vijf lidstaten voor de rechter te dagen (Frankrijk, Luxemburg, Nederland, Duitsland en Ierland) omdat ze niet op tijd waren met de implementatie van deze richtlijn.
137 Deze beginselen zijn: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. Zie voor meer achtergrondinformatie https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2.

persoonsgegevens kunnen worden verwerkt en regelt het bestaan en de taken van de toezichthouder op het gebied van de bescherming van persoonsgegevens.[138]
Volgens de Autoriteit Persoonsgegevens zijn de belangrijkste bepalingen in de Wbp:[139]

- Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt.
- Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn.
- Degene van wie persoonsgegevens worden verwerkt, moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt en van het doel van de gegevensverwerking.
- De gegevensverwerking moet op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.[140]

De Wbp is sinds de introductie ervan in 2001 verschillende keren herzien. In 2012 werden de administratieve lasten voor gegevensbeheerders verlicht.[141] Voorafgaand onderzoek is niet langer verplicht voor het vragen van toestemming voor het verwerken van persoonsgegevens wanneer zo'n voorafgaand onderzoek al is uitgevoerd voor een andere gegevensverwerker en is goedgekeurd door de toezichthouder.[142] Het verstrekken van persoonsgegevens naar landen buiten de EU (*third country data transfers*) zonder een adequaat beschermingsniveau is niet langer onderworpen aan goedkeuring door het ministerie van Veiligheid en Justitie wanneer gebruik wordt gemaakt van een standaardovereenkomst van de Europese Commissie. Verder wordt van privacyfunctionarissen niet langer verwacht dat ze een jaarverslag opstellen over hun activiteiten en bevindingen. In 2012 werden de maximale bedragen voor een bestuurlijke dwangsom (in geval van niet voldoen aan de meldplicht) ook verhoogd.
De Wbp implementeert de EU-richtlijn voor de bescherming van persoonsgegevens op een minimumniveau: hoewel het de Nederlandse wetgever vrijstond de richtlijn verder uit te werken en aan te vullen bij de implementatie in nationale wetgeving, zijn er geen extra bepalingen opgenomen, afgezien van een belangrijke uitzondering. In 2016 werd een herziening van de Wbp van kracht waarin het melden van datalekken verplicht werd (art. 34a Wbp). In diezelfde herziening werden boetes ingevoerd en

138 Deze zaken waren in de Wpr ook reeds geregeld.
139 https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens.
140 In beginsel geldt voor deze gegevens een 'nee, tenzij…'-regime: deze persoonsgegevens mogen niet worden verwerkt, behoudens in bepaalde uitzonderingsgevallen. Zie ook de memorie van toelichting bij de Wbp, *Kamerstukken II*, vergaderjaar 1997-1998, 25 892, nr. 3.
141 Wijziging Wbp in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen, *Staatsblad*, jaargang 2012, nr. 33. Zie ook https://autoriteitpersoonsgegevens.nl/nl/nieuws/wijziging-van-de-wet-bescherming-persoonsgegevens.
142 https://autoriteitpersoonsgegevens.nl/nl/nieuws/wijziging-van-de-wet-bescherming-persoonsgegevens.

uitgebreid tot meer verschillende soorten overtredingen (art. 66 Wbp).[143] Volgens de bepalingen voor de meldplicht datalekken moeten gegevensbeheerders elk datalek betreffende diefstal, verlies of misbruik van persoonsgegevens melden. De Autoriteit Persoonsgegevens moet worden geïnformeerd en in bepaalde gevallen moeten ook de betrokkenen wiens persoonsgegevens het betreft worden geïnformeerd. De toezichthouder heeft een speciaal loket geopend voor het melden van datalekken.[144] De maximale boetes zijn aanzienlijk hoger dan de bestuurlijke dwangsommen die voorheen de enige financiële sanctiemogelijkheid waren. Voorafgaand aan deze herziening van de Wbp waren de maximale bedragen 4.500 euro, nu zijn de maximale boetes 820.000 euro (zie voor meer details paragraaf 2.5).

Sectorale wetgeving

Op het terrein van de bescherming van persoonsgegevens bestaat voor specifieke sectoren ook specifieke wet- en regelgeving in Nederland. In bepaalde situaties kan de burger zich niet onttrekken aan het prijsgegeven van zijn persoonsgegevens, bijvoorbeeld in basisregistraties of belastingzaken. In zulke gevallen heeft de burger een 'verplichte' relatie met de overheid. Soms heeft een burger beperktere rechten met betrekking tot persoonsgegevens in bepaalde sectoren, bijvoorbeeld bij politiegegevens en strafrechtelijke gegevens. In andere gevallen heeft een burger juist extra rechten, bijvoorbeeld op extra vertrouwelijkheid in de medische sector.

In het strafrecht is er de Wet politiegegevens (Wpg)[145] die de verwerking van persoonsgegevens in het kader van de uitvoering van de politietaak regelt en de Wet justitiële en strafvorderlijke gegevens (Wjsg)[146] die de verwerking van justitiële gegevens[147] door de minister van Veiligheid en Justitie en van strafvorderlijke gegevens[148] door het Openbaar Ministerie regelt.[149] Dit kan persoonsgegevens van criminelen betreffen, maar ook persoonsgegevens van verdachten, getuigen, etc. Afgezien van de nationale politie richt de Wpg zich ook op bijzondere opsporingsdiensten, de Koninklijke Marechaussee en de Rijksrecherche. De Wpg is ook van toepassing op politietaken van

143 Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp), *Staatsblad*, jaargang 2015, nr. 230. Zie ook: https://www.rijksoverheid.nl/actueel/nieuws/2015/07/10/meldplicht-datalekken-en-uitbreiding-boetebevoegdheid-cbp-1-januari-2016-van-kracht.

144 https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

145 http://wetten.overheid.nl/BWBR0022463/2016-01-01.

146 http://wetten.overheid.nl/BWBR0014194/2016-01-01.

147 Justitiële gegevens zijn persoonsgegevens en gegevens over een rechtspersoon inzake de toepassing van het strafrecht of de strafvordering. Het gaat kortweg om gegevens over beslissingen in strafzaken.

148 Strafvorderlijke gegevens zijn persoonsgegevens of gegevens over een rechtspersoon die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het Openbaar Ministerie in een strafdossier of langs geautomatiseerde weg verwerkt. Het gaat kortweg om gegevens over lopende strafzaken.

149 De inhoud van het werk van de rechter valt niet onder de toezichthoudende taak van de AP, maar verder is op de verwerking van persoonsgegevens die de rechtbanken verwerken de Wbp van toepassing. Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-justitie/justitie.

het ministerie van Veiligheid en Justitie, zoals bij het uitvoeren van het vreemdelingenrecht. De Wpg wordt verder aangevuld en ingevuld door het Besluit politiegegevens.[150] Dit besluit regelt onder meer aan welke organisaties de politie persoonsgegevens (in deze context aangeduid als politiegegevens) mag verstrekken. De Wjsg bepaalt welke persoonsgegevens (en gegevens betreffende rechtspersonen) de minister van Veiligheid en Justitie en het Openbaar Ministerie mogen opslaan en hoelang. Als zodanig regelt het ook de bewaartermijnen van strafdossiers door de overheid. Persoonsgegevens mogen onder meer worden verwerkt voor het verstrekken van Verklaringen Omtrent Gedrag (VOG). In aanvulling op de Wjsg is er het Besluit justitiële en strafvorderlijke gegevens[151] dat verdere invulling geeft aan de Wjsg. Het toezicht op zowel de Wpg als de Wjsg ligt bij de Autoriteit Persoonsgegevens.

Ook verschillende andere wetten derogeren aan de Wbp, waaronder de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002),[152] de Wet basisregistratie personen (Brp)[153] en de Kieswet.[154] De Brp regelt de persoonsgegevens van Nederlandse burgers (de bevolkingsadministratie) en het toezicht hierop ligt eveneens bij de Autoriteit Persoonsgegevens. Het toezicht op de Wiv 2002 en de Kieswet is neergelegd bij andere toezichthouders.[155]

In de medische sector regelt de Wbp het verwerken van persoonsgegevens, maar daarenboven is ook de Wet op de geneeskundige behandelingsovereenkomst (WGBO) van toepassing. De WGBO is onderdeel van Boek 7 van het Burgerlijk Wetboek en regelt de relatie tussen geneeskundige hulpverlener en patiënt en regelt onder meer het medisch beroepsgeheim en privacy- en toegangsrechten voor patiënten en hun medische dossiers.[156] De WGBO verduidelijkt de rechtspositie van een patiënt, in het bijzonder in gevallen waarin geen of slechts weinig afspraken zijn gemaakt tussen de arts en de patiënt. Op grond van de WGBO heeft de patiënt recht op toegang tot zijn of haar medisch dossier (artikel 456) en is toestemming van de patiënt nodig voordat een behandeling kan worden gestart (artikel 450).[157] Als een patiënt aangeeft dat hij niet wenst te worden geïnformeerd over zijn medische toestand, kan een arts afzien van het verschaffen van informatie, tenzij de nadelen voor de patiënt als te aanzienlijk worden beschouwd.[158] In bepaalde situaties kan het artsen zijn toegestaan hun medisch beroepsgeheim te doorbreken, bijvoorbeeld wanneer een patiënt hiervoor toestemming

150 http://wetten.overheid.nl/BWBR0023086/2015-07-01.

151 http://wetten.overheid.nl/BWBR0016544/2015-07-01.

152 http://wetten.overheid.nl/BWBR0013409/2013-01-01.

153 http://wetten.overheid.nl/BWBR0033715/2015-09-01.

154 http://wetten.overheid.nl/BWBR0004627/2016-01-01.

155 De verwerking van persoonsgegevens ten behoeve van de Kieswet vallen wel onder de werking van EU-richtlijn 95/46/EC (zie memorie van toelichting op de Wbp, p. 70), maar op grond van artikel 2 sub f van de Wbp is de Wbp niet van toepassing op de verwerking van persoonsgegevens ten behoeve van de uitvoering van de Kieswet.

156 Zie artikel 7:466 Burgerlijk Wetboek.

157 Zie ook artikel 11 van de Grondwet over lichamelijke integriteit. Merk op dat de WGBO geen recht voor patiënten bevat om hun gegevens in medische dossiers te laten veranderen of te laten verwijderen. Patiënten hebben wel het recht documenten aan hun medisch dossier te laten toevoegen op basis van artikel 454 WGBO.

158 Zie artikel 7:449 Burgerlijk Wetboek.

geeft, als er sprake is van conflicterende plichten of wanneer sprake is van een wettelijke verplichting. In 2016 heeft het Nederlandse parlement wetgeving aangenomen met betrekking tot het elektronisch verwerken van hun persoonsgegevens waarbij patiënten onder meer zelf kunnen beslissen met welke zorgverleners hun persoonsgegevens elektronisch kunnen worden gedeeld.[159]

Zelfregulering en gedragscodes

Artikel 25 van de Wbp creëert ruimte voor organisaties om gedragscodes op te stellen met sectorspecifieke regels die het juridisch raamwerk voor het verwerken van persoonsgegevens verder invullen. Zulke gedragscodes kunnen aan de Autoriteit Persoonsgegevens worden voorgelegd om te toetsen of ze passen binnen de bestaande wetgeving. De gedragscodes worden goedgekeurd voor een maximale duur van vijf jaar. In 2015 heeft de Nederlandse toezichthouder drie gedragscodes beoordeeld (4 in 2012, 4 in 2013 en 2 in 2014).[160] Een voorbeeld van een goedgekeurde gedragscode in 2016 betrof een gedragscode voor het gebruik van zogeheten smartmeters door een collectief van aanbieders uit de energiesector.[161] Een ander voorbeeld van een goedgekeurde gedragscode is die voor particuliere recherchebureaus.[162] De wetgever moedigt zelfregulering, in het bijzonder gedragscodes, aan in de veronderstelling dat dit het open, abstracte juridische raamwerk voor de bescherming van persoonsgegevens verder invult en concretiseert.[163] Een ander voordeel kan zijn dat gedragscodes en andere vormen van zelfregulering meer en beter worden geaccepteerd en resulteren in betere naleving, onder meer omdat de regels zijn opgesteld door degenen die ze moeten naleven. In de praktijk is de tevredenheid echter beperkt, onder meer omdat de toezichthouder een dominante rol speelt en weinig vrijheid biedt bij het opstellen van de gedragscodes.[164] Het opstellen van gedragscodes wordt gezien als een langdurig, tijdrovend en kostbaar proces, met weinig concrete voordelen.[165] Dit geldt in het bijzonder voor de private sector.[166]

Organisaties kunnen ook convenanten opstellen voor verdere samenwerking bij het verwerken van persoonsgegevens. Een andere mogelijkheid is het gebruik van modellen voor privacyreglementen voor organisaties die specifiek zijn toegesneden op hun eigen

159 https://www.rijksoverheid.nl/actueel/nieuws/2016/10/04/wet-clientenrechten-bij-elektronische-verwerking-van-gegevens-belangrijke-verbetering-voor-de-patient.

160 AP (2016), *Jaarverslag 2015*, Den Haag: AP, supplement, p. 7.

161 https://autoriteitpersoonsgegevens.nl/nl/nieuws/besluit-gedragscode-slimme-meters-overige-diensten-aanbieders.

162 https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/gedragscodes/gedragscode-voor-particuliere-recherchebureaus-2016.

163 Zwenne, G.J., Duthler, A.W., Groothuis, M., Kielman, H., Koelewijn, W., en Mommers, L. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*. Den Haag: WODC, p. 78.

164 Holvast, J. (2005) 'Interview met Jacob Kohnstamm', *Privacy & Informatie*, 2005-3, p. 114-119.

165 Cuijpers, C.M.K.C. (2006), Verschillen tussen de Wbp en richtlijn 95/46/EC en de invloed op de administratieve lasten- en regeldruk, 22 juni 2006. See www.actal.nl.

166 Zwenne et al. (2007).

sector. Typische voorbeelden van modelprivacyreglementen zijn beschikbaar voor het onderwijs[167] en voor veiligheidshuizen.[168]

2.4 Implementatie

Het gebruikmaken van zelfregulering en gedragscodes is in de vorige paragraaf aan bod gekomen. Enerzijds lijkt de overheid het gebruik van zelfregulering en gedragscodes aan te moedigen (op papier), anderzijds lijkt de toezichthouder soms een dominante rol te spelen en weinig speelruimte te laten (in de praktijk). In de afgelopen jaren heeft de Autoriteit Persoonsgegevens slechts kleine aantallen gedragscodes beoordeeld (twee tot vier elk jaar). Handhaving van gedragscodes gebeurt door de betrokken partijen zelf of door henzelf in klachtprocedures aangewezen partijen, niet door de Autoriteit Persoonsgegevens of andere toezichthouders.[169] Meer details over informatiebeveiligingsmaatregelen en de implementatie ervan komen hierna aan bod.

Privacyfunctionarissen
Op dit moment bestaat er in de Nederlandse wetgeving geen verplichting voor bedrijven of overheidsorganisaties om privacyfunctionarissen aan te stellen. Een uitzondering zijn politiediensten, die verplicht een privacyfunctionaris moeten aanstellen op grond van de Wet politiegegevens (Wpg). Organisaties kunnen echter wel privacyfunctionarissen (voluit functionarissen voor de gegevensbescherming, FG's, genoemd) aanstellen als interne toezichthouders op het verwerken van persoonsgegevens (artikel 62 Wbp) en de toezichthouder, de Autoriteit Persoonsgegevens, lijkt dit aan te moedigen.[170] Het melden van verwerkingen van persoonsgegevens bij de toezichthouder is niet verplicht als er een privacyfunctionaris is aangesteld en aangemeld (in dat geval kan bij de eigen privacyfunctionaris worden gemeld). De taken van de privacyfunctionaris kunnen onder meer zijn: intern toezicht houden, het bijhouden van een register van gegevensverwerkingen (zie ook artikel 30 Wbp), meldingen van gegevensverwerkingen bijhouden, vragen en klachten afhandelen, adviseren over technologie en beveiliging en input leveren voor gedragscodes.
Er zijn enkele vereisten waaraan privacyfunctionarissen moeten voldoen (art. 63-64 Wbp). Zo moet het gaan om een natuurlijk persoon die over voldoende kennis van de organisatie en de privacywetgeving beschikt en die betrouwbaar is. Dit laatste uit zich onder meer in een geheimhoudingsplicht. De gegevensbeheerder moet de privacyfunctionaris uitrusten met onderzoeksbevoegdheden (zie artikel 64 lid 3 Wbp)[171] en een onafhankelijke positie in de organisatie geven. De Autoriteit Persoonsgegevens houdt

167 https://www.passendonderwijs.nl/brochures/modelprivacyreglement-samenwerkingsverband/. Zie ook: https://www.kennisnet.nl/artikel/alle-privacyhulpmiddelen-voor-scholen-op-een-rij/.
168 www.veiligheidshuizen.nl/doc/publicaties/modelconvenant-veiligheidshuizen_ob.pdf. Merk op dat deze privacyreglementen niet zijn opgesteld door de toezichthouder.
169 Merk op dat de AP toezichthouder blijft en handhavend kan optreden naar aanleiding van een klacht of op eigen initiatief.
170 https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming.
171 Deze bevoegdheden zijn gelijkwaardig aan of ontleend aan titel 5.2 van de Algemene wet bestuursrecht.

een register bij van privacyfunctionarissen,[172] hoewel het melden van privacyfunctionarissen niet verplicht is. Begin 2008 waren er 215 privacyfunctionarissen geregistreerd bij de toezichthouder.[173] In december 2016 waren dit er 722.[174] Alle ministeries hebben een privacyfunctionaris, alle politiediensten hebben een (verplichte) privacyfunctionaris en ongeveer 10% van alle gemeenten heeft een privacyfunctionaris. Andere privacyfunctionarissen kunnen worden gevonden in ziekenhuizen en bedrijven.[175]
Privacyfunctionarissen hebben zichzelf verenigd in het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG).[176] De NGFG komt vier keer per jaar bij elkaar en heeft ongeveer honderd leden en enkele geassocieerde leden. Personen die geen privacyfunctionaris zijn, kunnen hun belangstelling laten blijken, maar volwaardig lidmaatschap vereist dat iemand privacyfunctionaris is en als zodanig is geregistreerd bij de toezichthouder.[177] Personen die privacyfunctionaris zijn maar niet staan geregistreerd bij de toezichthouder kunnen geassocieerd lid worden. De NGFG werk samen met vergelijkbare organisaties in andere Europese landen in de Confederation of European Data Protection Organisations (CEDPO). Deze koepelorganisatie is opgericht in 2011 en heeft zeven leden, uit Ierland, Oostenrijk, Frankrijk, Spanje, Duitsland, Nederland en Polen.[178]
Hoewel privacyfunctionarissen niet verplicht zijn, kunnen organisaties er toch voor kiezen deze aan te stellen omdat ze belang hechten aan de bescherming van privacy en persoonsgegevens. Privacyfunctionarissen worden doorgaans intern gerekruteerd uit het aanwezige personeelsbestand. Meer dan een op de vier privacyfunctionarissen is onderdeel van de juridische staf, iets minder dan een op de vier privacyfunctionarissen is onderdeel van de directie en minder dan 15% is onderdeel van een afdeling kwaliteitsmanagement.[179] Hoewel artikel 63 lid 2 van de Wbp voorschrijft dat privacyfunctionarissen geen instructies mogen krijgen van de gegevensbeheerder of de organisatie die hem of haar heeft aangesteld, geeft in 2009 niettemin bijna een op de vier privacyfunctionarissen aan instructies te moeten opvolgen van de directie van de organisatie.

172 https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming.
173 H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A.M. Klingenberg en H. Prakken (2009), *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*, Groningen. Zie ook De Zeeuw, J. (2009), 'De FG en de evaluatie van de WBP', *Privacy & Informatie*, afl. 2, april 2009, p. 91-93.
174 Zie de lijst op https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming. Register A-D: 137, Register E-H: 163, Register I-L: 77, Register M-P: 107, Register Q-T: 165, Register U-Z: 73.
175 Dubbeld, L. (2007), 'Functionarissen voor de gegevensbescherming: onzichtbare privacybeschermers', *Privacy & Informatie,* 2007, aflevering 2, p. 69-70.
176 http://www.ngfg.nl/.
177 Jaarverslag NGFG 2006-2007.
178 www.cedpo.eu.
179 H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A.M. Klingenberg en H. Prakken (2009), *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*. Groningen.

Dit is in strijd met de juridisch vereiste onafhankelijkheid.[180] Een verklaring hiervoor kan zijn dat privacyfunctionarissen hun rol doorgaans in deeltijd vervullen, waarbij ze in de resterende tijd van hun aanstelling een andere rol vervullen binnen de organisatie – een rol waarin ze niet onafhankelijk zijn. Omdat ze onderdeel zijn van de organisatie, ervaren privacyfunctionarissen ook moeilijkheden als het gaat om het innemen van een onafhankelijke positie ten opzichte van hun werkgever. Privacyfunctionarissen rapporteren gemiddeld 1,4 overtredingen in hun organisatie, maar de meeste tijd besteden ze aan het uitleggen van zaken en het bevorderen van bewustzijn.[181]
De rol van de privacyfunctionaris is niet erg populair.[182] Een uitzondering hierop vorm de rol van de privacyfunctionaris bij een multinational: dit zijn zeer invloedrijke posities omdat de bescherming van privacy en persoonsgegevens een belangrijk thema is voor klanten en reputatieschade kan voorkomen.

Beveiligingsmaatregelen
Op grond van artikel 13 Wbp moet elke gegevensbeheerder passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen tegen verlies en onrechtmatige verwerking. Bij onvoldoende beveiliging kan van alles misgaan, waaronder datalekken en het onrechtmatig koppelen van gegevensbestanden. Passende maatregelen kunnen bestaan uit autorisatieprotocollen, authenticatieprocedures en andere beveiligingsmaatregelen.[183] Om vast te stellen of beveiligingsmaatregelen passend zijn, is een eerste vereiste het uitvoeren van een risicoanalyse.[184] Vervolgens is de stand van de techniek relevant, evenals de kosten van implementatie ervan. Wanneer beveiligingsmaatregelen gedateerd zijn, zijn ze niet langer passend. Wanneer betere beveiligingsmaatregelen beschikbaar zijn, maar tegen uitzonderlijk hoge kosten, is het niet gebruiken van zulke technieken niet in strijd met het vereiste van passende beveiligingsmaatregelen. Voor online toepassingen kunnen hogere beveiligingseisen gelden om aan het vereiste van passende beveiligingsmaatregelen te voldoen, aangezien het internet een open systeem is dat extra privacyrisico's met zich meebrengt.[185]

180 H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A.M. Klingenberg en H. Prakken (2009), *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*. Groningen. Deze bevindingen zijn mogelijk gedateerd, maar meer recent onderzoek is niet beschikbaar.

181 H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A.M. Klingenberg en H. Prakken (2009), *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*. Groningen.

182 H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A.M. Klingenberg en H. Prakken (2009), *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk*. Groningen, p. 63.

183 Zwenne, G.J., Duthler, A.W., Groothuis, M., Kielman, H., Koelewijn, W., en Mommers, L. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*. Den Haag: WODC.

184 Zie de richtsnoeren van het AP: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf.

185 Hooghiemstra, T.F.M. (2002), *Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg*. Den Haag: Cbp, A&V 2002 nr. 26.

De Autoriteit Persoonsgegevens heeft richtlijnen ontwikkeld voor beveiligingsmaatregelen.[186] Deze richtlijnen zijn vooral gebaseerd op een van de meest gebruikte standaarden voor informatiebeveiliging, de zogeheten Code voor Informatiebeveiliging.[187] Dit is een NEN/ISO-code[188] die onderdeel is van een groep van standaarden voor het initiëren, implementeren, handhaven en verbeteren van informatiebeveiliging in organisaties. Deze standaarden zijn onderdeel van een lijst waarvoor overheidsorganisaties een 'comply-or-explain'-regime ('pas toe of leg uit') hebben.[189] De Code voor Informatiebeveiliging is een technologieneutrale standaard die breed kan worden toegepast bij het opstellen en implementeren van beveiligingsmaatregelen.
Voor de gezondheidszorg is er een verdere specificatie van de Code voor Informatiebeveiliging beschikbaar in de vorm van NEN 7510.[190] Toen de Inspectie voor de Gezondheidszorg (IGZ) de implementatie van deze standaard onderzocht, bleek dat voor 2003 niet een van de twintig onderzochte ziekenhuizen deze standaard had geïmplementeerd.[191] In 2008 was dit niet verbeterd.[192] Hoewel beveiligingsmaatregelen beschikbaar zijn, waren in 2003 veel elektronische patiëntendossiers niet voldoende beveiligd.[193] Toen bijvoorbeeld informatiebeveiligingsexperts de beveiliging van twee ziekenhuizen onderzochten, bleek dat ze toegang hadden tot een miljoen patiëntendossiers.[194] Sindsdien is de beveiliging nog steeds niet verbeterd.[195] Uit onderzoek blijkt bovendien dat niet alle zorginstellingen een compleet beeld hebben van wie toegang heeft tot de gegevens en wie de patiëntgegevens bewerken.[196]
Ook in andere sectoren lijkt informatiebeveiliging niet adequaat geïmplementeerd. De toenmalige Sociale Inlichtingen- en Opsporingsdienst (SIOD, tegenwoordig de Inspectie SZW) had geen beveiligingsplan en geen overzicht van beveiligingsmaatregelen toen de toezichthouder dit onderzocht.[197] Uit onderzoek van de Inspectie SZW bleek in 2013 ook dat maar 4% van de gemeenten voldoende beveiligingsmaatregelen had getroffen voor het opvragen van persoonsgegevens via Suwinet[198] en dat 13% van de gemeenten aan geen van de onderzochte normen voor informatiebeveiliging deed.[199]

186 CBP (2013), *Beveiliging van persoonsgegevens*. Den Haag: CBP.
187 NEN-ISO/IEC 27002:2007 nl.
188 NEN staat voor Nederlandse norm.
189 Artikel 3 sub b Instellingsbesluit College en Forum Standaardisatie 2012, *Stcrt*, 2011, 23581.
190 NEN, Steunpunt NEN 7510 (http://www.nen7510.org).
191 IGZ, 'ICT in ziekenhuizen', augustus 2004.
192 CBP (2008), *Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm*. Den Haag: CBP.
193 PvG. 'Implementatie van de Wbp: de resultaten van Prismant', *JPG* juni 2003.
194 Zwenne, G.J., Duthler, A.W., Groothuis, M., Kielman, H., Koelewijn, W., en Mommers, L. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*. Den Haag: WODC.
195 https://www.trouw.nl/samenleving/ziekenhuizen-beveiligen-sites-niet-goed~a8f5d976/.
196 Hooghiemstra, T., Oud, J.,Radema, M., Spruit, M., en Wielaard, P. (2016), *Onderzoek naar de beveiliging van patiëntgegevens*. Den Haag: PBLQ. Zie: https://www.rijksoverheid.nl/documenten/rapporten/2016/12/01/onderzoek-naar-de-beveiliging-van-patientgegevens.
197 CBP (2010), *Onderzoek van het College bescherming persoonsgegevens (CBP) naar bestandskoppelingen door de SIOD voor de ontwikkeling van risicoprofielen*. z2009-00672, mei 2010, Den Haag: CBP.
198 Suwinet is een automatiseerd systeem waarmee gemeenten en andere (semioverheids)organisaties gegevens uitwisselen die noodzakelijk zijn voor onder meer de uitvoering van de Participatiewet.
199 Inspectie SZW (2015), *Suwinet 2015. Vervolgonderzoek 'veilig omgaan met elkaars gegevens'*. Den Haag: Inspectie SZW, zie https://www.inspectieszw.nl/...veilig-omgaan-met-elkaars-gegevens/Suwinet-2015.pdf.

Tijdens een audit bleek dat ook de nationale politie beveiligingsmaatregelen ter bescherming van de persoonsgegevens die werden verwerkt niet voldoende en niet adequaat had geïmplementeerd.[200] Een algemeen beeld van de implementatie van beveiligingsmaatregelen in de private sector kan hier niet worden geschetst. Hoewel mag worden aangenomen dat veel bedrijven passende beveiligingsmaatregelen nemen, onder meer om hun bedrijfsgeheimen te beschermen, was ook in de private sector de afgelopen jaren sprake van datalekken (zie paragraaf 2.1). Concepten zoals Privacy by Design, privacy by default, need-to-know en role-based access worden in toenemende mate gebezigd in beleidsdocumenten, maar tot op heden heeft dit niet geleid tot daadwerkelijke implementatie ervan, althans niet op grotere schaal (zie paragraaf 2.2).

Transparantie

Zoals aangegeven in paragraaf 2.1 vertonen Nederlanders een hoog niveau van bewustzijn van het gebruik van persoonsgegevens door eigenaren van websites. Er zijn hoge niveaus van bewustzijn en acceptatie van het gebruik van persoonsgegevens door eigenaren van websites om gebruikers te e-mailen (bewustzijn 86%, acceptatie 80%).[201] Als ze de privacyvoorwaarden lezen, lezen Nederlanders zelden de hele tekst (Nederland 9%, EU-gemiddelde 11%). Niettemin zijn Nederlanders redelijk vol vertrouwen dat – als ze de privacyvoorwaarden lezen – ze de tekst grotendeels of geheel begrijpen (Nederland 72%, EU-gemiddelde 64%).[202] In het algemeen bieden bedrijven geen gepersonaliseerde privacy settings aan. Zulke opties zijn het meest aanwezig in (bepaalde) sociale media, maar dat zijn vooral diensten die worden aangeboden door internationale bedrijven en niet zozeer door Nederlandse bedrijven. In bepaalde gevallen worden anonieme diensten aangeboden. Bijvoorbeeld, klanten van supermarktketen Albert Heijn kunnen kiezen voor een anonieme variant van de Bonuskaart, de klantenkaart van de supermarkt. Toen de Autoriteit Persoonsgegevens de prioriteiten voor 2017 aankondigde, werd transparantie benadrukt, in het bijzonder in relatie tot profiling.[203] Dit kan erop wijzen dat er ruimte voor verbetering is wat betreft transparantie. Zoals aangegeven in paragraaf 2.3 probeert de rijksoverheid via de website www.mijnoverheid.nl de transparantie te verbeteren ten aanzien van de persoonsgegevens die worden verwerkt over burgers. Burgers die inloggen op deze website krijgen toegang tot hun persoonsgegevens, waaronder gegevens uit de Basisregistratie personen (BRP), voertuiggegevens bij de Dienst Wegverkeer (RDW) en perceel- of eigendomsgegevens van hun huis bij het Kadaster.[204]

200 Politie (2016), Verbeterplan Wet politiegegevens en Informatiebeveiliging. Zie: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2016/05/27/tk-bijlage-verbeterplan-wet-politiegegevens-en-informatiebeveiligign/tk-bijlage-verbeterplan-wet-politiegegevens-en-informatiebeveiligign.pdf.

201 Consent Country Report The Netherlands, (2012), p. 4.

202 Consent Country Report The Netherlands, (2012), p. 4.

203 https://autoriteitpersoonsgegevens.nl/nl/nieuws/autoriteit-persoonsgegevens-presenteert-agenda-2017.

204 https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/wat-is-mijnoverheid.

2.5 Toezicht en handhaving

Toezichthouders

De Nederlandse toezichthouder voor de bescherming van persoonsgegevens is de Autoriteit Persoonsgegevens (AP). Tot 2016 was de naam van deze toezichthouder het College bescherming persoonsgegevens (CBP). Het is niet voor het eerst dat deze toezichthouder van naam verandert: tot 2001 stond de toezichthouder bekend onder de naam Registratiekamer. De Autoriteit Persoonsgegevens is verantwoordelijk voor de controle op de naleving van de wettelijke voorschriften voor de bescherming van persoonsgegevens en adviseert over nieuwe wet- en regelgeving.[205] De reikwijdte van het toezicht en de handhaving omvat niet alleen de Wet bescherming persoonsgegevens (Wbp), maar alle wetgeving die het verwerken van persoonsgegevens regelen, zoals de Wet Politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg), zie vorige paragraaf.

De AP bestaat uit een college met een voorzitter en maximaal twee andere leden. Op dit moment bestaat het college uit twee leden, een voorzitter en een vicevoorzitter.[206] De voorzitter wordt benoemd voor een termijn van zes jaar. Deze termijn kan eenmalig worden verlengd met nog eens zes jaar. Benoemingen worden voorgedragen door de minister van Veiligheid en Justitie. Er is ook een raad van advies, bestaande uit vertegenwoordigers vanuit de overheid, het bedrijfsleven en de wetenschap.[207]

Afgezien van enkele stafafdelingen bestaat de AP uit twee grote afdelingen die zich richten op het toezicht op respectievelijk de publieke en de private sector. De AP heeft momenteel ongeveer 80 medewerkers.[208] In 2015 waren er 72,5 medewerkers en bedroeg het jaarlijks budget 8,2 miljoen euro.[209] In 2016 bedroeg het jaarlijks budget 8,1 miljoen euro.[210] In 2015 voerde de AP 43 onderzoeken uit, bemiddelde in 226 gevallen en verstrekte advies over 27 wetsvoorstellen.[211] In 2016 waren deze aantallen: 197 onderzoeken, 303 bemiddelingen en 33 wetgevingsadviezen.[212]

Taken en bevoegdheden

De vier belangrijkste activiteiten van de Autoriteit Persoonsgegevens zijn toezicht houden, adviseren, informatie verstrekken, verantwoording afleggen en participeren in internationale opdrachten.[213] Toezicht houden bestaat uit het starten van onderzoeken naar naleving en, in gevallen van gebrekkige naleving, het gebruik van handhavingsbevoegdheden, waaronder het toepassen van sancties. Toezicht omvat ook het beoordelen

205 https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/missie-visie-en-kernwaarden.

206 https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/de-leden-van-de-autoriteit-persoonsgegevens.

207 https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/organisatie/raad-van-advies.

208 AP (2017), Bijlage *Jaarverslag 2016*, Den Haag: AP, p. 3.

209 AP (2016), *Jaarverslag 2015*, Den Haag: AP, p. 63.

210 AP (2017), Bijlage *Jaarverslag 2016*, Den Haag: AP, p. 4.

211 AP (2016), *Jaarverslag 2015*, Den Haag: AP, p. 63.

212 AP (2017), Bijlage *Jaarverslag 2016*, Den Haag: AP, p. 5.

213 https://autoriteitpersoonsgegevens.nl/en/node/1930.

van gedragscodes, het bemiddelen in disputen en het beoordelen van verzoeken aangaande uitzonderingen op het verbod gevoelige persoonsgegevens te verwerken. Advies wordt gegeven over wetsvoorstellen die gaan over of raken aan het verwerken van persoonsgegevens en over ontheffingen voor het verstrekken van persoonsgegevens aan derde landen ingeval de ontvangende landen niet beschikken over een adequaat beschermingsniveau. Adviezen aan de wetgever worden overigens niet zonder meer overgenomen.[214] Het verstrekken van informatie betreft informatie over hoe de wet- en regelgeving op het terrein van de bescherming van persoonsgegevens moet worden uitgelegd. Hieraan wordt hoofdzakelijk invulling gegeven via de website en de telefoon en is, als zodanig, erg algemeen. De AP spreekt op de website of in de jaarverslagen niet over het organiseren van workshops, symposia of opleidingen. Verder lijkt de AP terughoudend te zijn in het afhandelen van vragen van burgers en organisaties over hoe wet- en regelgeving moet worden nageleefd of hoe 'privacy-proof' te zijn. Zodoende kan gesteld worden dat het ondersteunen van burgers hoofdzakelijk beperkt is tot documentatie op de website.[215]

De AP geeft ook voorlichting aan burgers en organisaties via de pers. Zij onderhoudt actieve contacten met journalisten; in 2016 had zij 800 perscontacten met diverse media. Er verschijnen met regelmaat berichten in de pers over het werk van de AP en over actualiteiten rond privacybescherming. De voorzitter en vicevoorzitter geven geregeld interviews en de woordvoerders staan dagelijks de pers te woord. Daarnaast geven de collegeleden en MT-leden regelmatig toespraken en presentaties.

Internationale opdrachten omvatten onder meer het deelnemen aan de Artikel 29 Werkgroep (een onafhankelijk adviesorgaan waarin alle toezichthouders op de bescherming van persoonsgegevens van de EU en de European Data Protection Supervisor deelnemen), deelname aan internationale congressen (zoals de jaarlijkse Conference of European Data Protection Authorities en de jaarlijkse International Conference of Data Protection and Privacy Commissioners).

De speerpunten van de AP worden elk jaar gepubliceerd. Voor 2017 zijn de speerpunten de nieuwe Europese privacywetgeving, profiling, bijzondere gegevens en de beveiliging van persoonsgegevens.[216] Enkele jaren geleden werden er geen speerpunten geformuleerd.[217]

Er is geen sprake van een uitgebreide dialoog tussen de AP en de organisaties waarop toezicht wordt gehouden. De AP geeft in reactie op dit onderzoek aan dat de belangrijkste redenen hiervoor – naast de beperkte mankracht – is gelegen in het punt dat de AP terughoudend is een dergelijke dialoog te onderhouden omdat het belangenverstrengeling kan veroorzaken op het moment dat handhaving nodig is. Indien de toezichthouder concrete adviezen zou verstrekken over wat te doen of welke maatregelen te

214 Een typisch voorbeeld waarin de wetgever een dringend signaal van de toezichthouder terzijde schuift is het gebruik van het burgerservicenummer voor kerkelijke ledenadministraties. Zie https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-adviseert-over-nadere-uitwerking-basisregistratie-personen.

215 Op de website zijn ook diverse voorbeeldbrieven voor burgers opgenomen.

216 https://autoriteitpersoonsgegevens.nl/nl/over-de-autoriteit-persoonsgegevens/agenda. Merk op dat deze agenda nauwelijks verschilt van de agenda voor 2015.

217 Custers B.H.M. & Zwenne G.J. (2009), 'Aandachtspunten voor het College Bescherming Persoonsgegevens', *Openbaar Bestuur* 19(8): 14-17.

nemen, dan kunnen problemen ontstaan wanneer deze aanbevelingen of maatregelen worden geëvalueerd door de toezichthouder. Een mogelijke oplossing hiervoor is te adviseren over de beoogde gevolgen van maatregelen in plaats van over de te nemen maatregelen zelf.[218] De Autoriteit Persoonsgegevens heeft de laatste jaren, meer dan voorheen, contacten onderhouden met brancheorganisaties in de publieke en private sector, onder meer om hen te ondersteunen als zij tegen knelpunten aanlopen.
Een typisch voorbeeld hiervan zijn herhaalde waarschuwingen in 2013,[219] 2014[220] en 2016[221] van de AP richting gemeenten dat deze onvoldoende weten welke persoonsgegevens van hun burgers zij in het sociaal domein mogen verwerken en welke regels daarvoor gelden. De toezichthouder geeft duidelijke waarschuwingen en aanvullende handreikingen op de website,[222] maar geen een-op-eenadviezen. Tegelijkertijd blijven overigens tot dusverre ook handhavende acties uit. Ondertussen kan de burger zich niet onttrekken aan deze wettelijk verplichte, maar tegelijkertijd niet adequaat geregelde verwerking van persoonsgegevens.
Meldingen van burgers (via de website van de AP)[223] kunnen leiden tot onderzoek, maar de AP kan ook ambtshalve een onderzoek starten zonder dat sprake is van een melding. In 2015 was sprake van 6.778 vragen en tips van burgers.[224] In 2016 waren er 8.799 vragen en tips van burgers.[225] Er waren in 2015 in totaal 43 onderzoeken en 226 zaken waarin de AP bemiddelde voor een oplossing.[226] In 2016 waren er 197 onderzoeken en 303 bemiddelingen.[227] Het is onduidelijk hoeveel van deze onderzoeken zijn gestart op basis van meldingen van bezorgde burgers.
De bevoegdheden van de AP kunnen worden gevonden in artikelen 60, 61 en 66 van de Wbp en de Algemene wet bestuursrecht. Art. 60 Wbp verschaft de AP de bevoegdheid om op verzoek van een belanghebbende (een handhavingsverzoek) of ambtshalve een onderzoek te starten. Art. 61 Wbp verschaft de AP de bevoegdheid tot huiszoekingen (met een rechterlijke machtiging en onder bepaalde voorwaarden) zonder toestemming van de bewoners. De onderzoeksresultaten kunnen de AP tot een op normnaleving gerichte interventie doen besluiten of tot het inzetten van bestuursrechtelijke sanctiebevoegdheden zoals een last onder bestuursdwang (inclusief een last onder dwangsom). Art. 66 Wbp geeft de AP de mogelijkheid boetes op te leggen met een maximum van 20.500 euro of boetes met een maximum van 820.000 euro, afhankelijk van het type overtreding van de Wbp. In sommige gevallen kan zelfs een omzetgerelateerde boete

218 Custers B.H.M. & Zwenne G.J. (2009), 'Aandachtspunten voor het College Bescherming Persoonsgegevens', *Openbaar Bestuur* 19(8): 14-17.
219 https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-adviseert-over-wetsvoorstel-ter-vervanging-van-wet-gba.
220 https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-gemeenten-mogen-bij-decentralisatie-privacywetgeving-niet-negeren.
221 https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-gemeenten-onzorgvuldig-bij-uitwerking-privacyregels-sociaal-domein.
222 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gemeente/sociaal-domein.
223 https://autoriteitpersoonsgegevens.nl/nl/contact-met-de-autoriteit-persoonsgegevens/tip-ons.
224 AP (2016), *Jaarverslag 2015*, Den Haag: AP, p. 64.
225 AP (2017), Bijlage *Jaarverslag 2016*, Den Haag: AP, p. 9.
226 AP (2016), *Jaarverslag 2015*, Den Haag: AP, p. 63.
227 AP (2017), Bijlage *Jaarverslag 2016*, Den Haag: AP, p. 5.

worden opgelegd. Boetes met een maximum van 20.500 euro zijn onder meer van toepassing op gevallen van onrechtmatige gegevensverstrekkingen aan derde landen. Boetes met een maximum van 820.000 euro kunnen worden toegepast door de AP in de meest andere gevallen waarin sprake is van gebrekkige naleving, bijvoorbeeld wanneer bindende aanwijzingen van de toezichthouder niet worden nagekomen, wanneer persoonsgegevens worden verwerkt zonder een juridische grondslag, in het geval van niet-naleving van de beginselen voor een eerlijke verwerking van persoonsgegevens (zoals doelbinding), wanneer beveiliging ontbreekt of onvoldoende is, etc. De bevoegdheid om voor nagenoeg alle overtredingen van de Wbp boetes op te leggen, is relatief nieuw: deze bevoegdheid is pas beschikbaar voor de AP sinds januari 2016.[228] Inmiddels heeft de AP ook beleidsregels opgesteld waarin is vastgelegd hoe de hoogte van boetes specifieker wordt bepaald binnen de toegestane maxima.[229]
Tot slot publiceert de Autoriteit Persoonsgegevens ook af en toe beleidsregels, voorheen ook wel richtsnoeren genoemd, voor bepaalde onderwerpen. Beleidsregels en richtsnoeren zijn er voor de publicatie van persoonsgegevens op internet (2007), de informatieplichten van basisscholen (2009), de toepassing van automatische kentekenherkenning door de politie (2009), de openbaarmaking van overheidsinformatie (2009), kopieën van identiteitsbewijzen (2012), de beveiliging van persoonsgegevens (2013), de meldplicht datalekken (2015), cameratoezicht (2016), de zieke werknemer (2016) en de machtigingsvereiste zorgpolis (2016).[230]

Gebruik van bevoegdheden
De AP lijkt het indienen van klachten niet echt aan te moedigen: in geval van een klacht over het gebruik van persoonsgegevens is het officiële advies om eerst contact op te nemen met de gegevensbeheerder en, als dat niet het gewenste resultaat oplevert, naar de rechter te stappen.[231] Daarnaast wordt gestimuleerd om via de website tips over vermeende overtredingen in te dienen.
Op grond van de aankomende EU-verordening is elke toezichthouder op de bescherming van persoonsgegevens verplicht klachten te behandelen van betrokkenen of van organisaties die die persoon vertegenwoordigen.[232] In lijn hiermee heeft de nieuwe voorzitter van de AP de ambitie uitgesproken dit te willen uitbreiden: in een recent persbericht gaf hij de wens aan de toezichthouder te laten uitgroeien tot een 'privacy ombudsman'

228 https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-krijgt-boetebevoegdheid-en-wordt-autoriteit-persoonsgegevens. Merk op dat voor 2016 sprake was van beperkte bevoegdheden tot het opleggen van administratieve boetes. Bijvoorbeeld, het niet melden van het verwerken van persoonsgegevens aan de toezichthouder kon worden gesanctioneerd met een administratieve boete van maximaal 4.500 euro (art. 66 Wbp).

229 Beleidsregels van de Autoriteit Persoonsgegevens van 15 december 2015, zoals laatstelijk gewijzigd op 6 juli 2016, met betrekking tot het opleggen van bestuurlijke boetes (Boetebeleidsregels Autoriteit Persoonsgegevens 2016), zie https://www.privacycompany.eu/files/Factsheet%20boetebeleidsregels%20meldplicht.pdf.

230 https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/thematische-beleidsregels

231 https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-over-gebruik-persoonsgegevens?qa=klacht

232 Zie ook art 57 sub 1 sub f van de GDPR.

die klachten (sic) van burgers kan afhandelen.[233] Het lijkt daarbij wel raadzaam om klachten en handhavingsverzoeken van elkaar te onderscheiden.
Er zijn geen officiële cijfers beschikbaar over het aantal klachten dat de AP heeft ontvangen. In het jaarverslag geeft de AP aan dat er in 2016 in totaal 8.799 vragen en tips zijn ontvangen. Dit cijfer kan de ontvangen klachten omvatten. Ongeveer 29% van dit cijfer betreft gezondheid en welzijn.[234] Ongeveer 17% betreft financiële dienstverlening, 15% betreft openbaar bestuur.[235]
Bestuurlijke boetes waren wel al mogelijk, maar zijn niet toegepast in de periode 2012-2015.[236] Ook in 2016 zijn boetes niet toegepast.[237] De last onder dwangsom is 20 keer toegepast in 2016.[238] Daarvoor is de last onder dwangsom 17 keer toegepast in 2015, 13 keer in 2014, 19 keer in 2013 en 12 keer in 2012.[239] Bijvoorbeeld in 2014 legde de toezichthouder een last onder dwangsom op aan Google met een dwangsom van 20.000 euro per dag (met een maximum van 5 miljoen euro) omdat Google zijn gebruikers niet behoorlijk informeerde en niet expliciet om toestemming vroeg voor het gebruik van hun persoonsgegevens.[240]
Tegen sanctiebesluiten van de AP staat bestuursrechtelijke rechtsbescherming open. Een belangrijke zaak is die van de AP tegen Facebook. In 2015 weigerde Facebook tijdens een onderzoek van de toezichthouder informatie te verstrekken over de gebruikersvoorwaarden en legde de AP een last onder dwangsom op. De zaak stond al op de rol bij de rechtbank in Den Haag toen Facebook op het laatste moment besloot alsnog mee te werken en de gevraagde informatie te verstrekken.[241] Recenter, in 2016, werd het beroep van Whatsapp tegen het dwangsombesluit wegens overtreding van artikel 4 lid 3 Wbp ongegrond verklaard.[242]

Reputatie
In 2006 had slechts 17% van de Nederlanders ooit gehoord van het CBP (de toenmalige naam van de AP).[243] In dit onderzoek gaf 32% van de mensen aan tevreden te zijn met de informatie verschaft door de toezichthouder, terwijl 16% ontevreden was. In een recent onderzoek geeft 76% van de Nederlanders aan gehoord te hebben van de toezichthouder.[244] Zodoende kan worden geconcludeerd dat dit cijfer het afgelopen decennium aanzienlijk is gestegen. Mogelijk is dit (deels) toe te schrijven aan het actieve

233 http://nos.nl/artikel/2150430-5500-datalekken-gemeld-bij-waakhond.html.
234 AP (2017), *Jaarverslag 2016*, Den Haag: AP, p. 7.
235 AP (2017), Jaarverslag 2016, Den Haag: AP, p. 7.
236 AP (2016), Bijlage *Jaarverslag 2015*, Den Haag: AP, p. 6.
237 AP (2017), Bijlage *Jaarverslag 2016*, Den Haag: AP, p. 5.
238 AP (2017), Bijlage *Jaarverslag 2016*, Den Haag: AP, p. 5.
239 AP (2016), Bijlage *Jaarverslag 2015*, Den Haag: AP, p. 6.
240 http://nos.nl/artikel/2009119-privacywaakhond-dreigt-google-met-miljoenenboete.html.
241 http://www.volkskrant.nl/tech/rechtszaak-facebook-tegen-cbp-van-de-baan~a4003468/.
242 http://www.nu.nl/mobiel/4354627/whatsapp-verliest-rechtszaak-van-nederlandse-privacywaakhond.html.
243 Tolboom, M., & Mazor, L. (2006), *Bekendheid en beleving informatieplicht onder burgers. Kwantitatief onderzoek onder burgers.* Amsterdam: TNS-NIPO Consult, p. 15.
244 Roosendaal, A., Nieuwenhuis, O., Ooms, M., Bouman-Eijs, A., en Huijboom, N. (2015), *Privacybeleving op het internet in Nederland*. Den Haag: TNO, p. 39.

mediabeleid van de toezichthouder: in 2016 had de toezichthouder 797 contactmomenten met de media.[245]
Bedrijven lijken meer bevreesd voor reputatieschade dan voor boetes en proberen in toenemende mate publicaties van de toezichthouder te vermijden.[246] In het verleden werd de toezichthouder nog wel eens afgeschilderd als een waakhond zonder tanden,[247] maar gegeven de aanzienlijk toegenomen mogelijkheden om boetes op te leggen, behoort dit beeld tot het verleden. Vrees voor de AP zal mogelijk verder toenemen wanneer de AVG in mei 2018 van kracht wordt. Na die datum kunnen bestuurlijke boetes worden opgelegd van 10 of 20 miljoen euro (afhankelijk van het type overtreding) of, in het geval van ondernemingen, tot 2 of 4% (eveneens afhankelijk van het type overtreding) van de wereldwijde jaarlijkse omzet van het afgelopen boekjaar indien dit cijfer hoger is.

245 AP (2017), Bijlage *Jaarverslag 2016*, Den Haag: AP, p. 11.

246 Teeffelen, K. van (2015), 'Organisaties zijn banger voor reputatieschade bij schending privacy', *Trouw*, 29 april 2015.

247 Essen, J. van (2014), 'CBP een waakhond zonder tanden?', Mr-online, 1 december 2014. http://www.mr-online.nl/opinie/432-wetgeving/25169-cbp-een-waakhond-zonder-tanden; Custers B.H.M. & Zwenne G.J. (2009), 'Aandachtspunten voor het College Bescherming Persoonsgegevens', *Openbaar Bestuur* 19(8): 14-17.

3. Duitsland

3.1 Algemene situatie

Duitsland lijkt in cultureel en juridisch opzicht erg op Nederland (zie paragraaf 1.3.2). Vanwege deze overeenkomsten is Duitsland geselecteerd om de situatie betreffende de bescherming van persoonsgegevens te vergelijken met Nederland. De federale Duitse grondwet heeft een uitgebreide opsomming van grondrechten (*Grundrechte*).[1] De sterke focus op deze rechten is een nasleep van de Tweede Wereldoorlog die een terughoudendheid ten opzicht van te veel overheidsmacht heeft opgeleverd. Deze grondrechten zijn rechtstreeks van toepassing voor Duitse burgers.[2] Artikel 10 van de federale Duitse grondwet beschermt de geheimhouding van correspondentie, post en telecommunicatie. Het recht op privacy wordt niet als zodanig benoemd in de Duitse grondwet. Contouren van het recht op privacy zijn reeds te zien in het *Elfes*-arrest van het federale constitutionele hof (Bundesverfassungsgericht) in 1957.[3] Het recht op informationele zelfbeschikking werd geconstrueerd door het federale constitutionele hof vanuit het recht op de bescherming van persoonlijke vrijheid (artikel 2, paragraaf 1) en de bescherming van menselijke waardigheid (artikel 1, paragraaf 1) in het *Mikorzensus*-arrest in 1969.[4]
Duitsland is een federale bondsrepubliek, bestaande uit zestien deelstaten (*Bundesländer*, of afgekort *Länder*). Deze structuur werd in 1949 opgezet, in de nasleep van de Tweede Wereldoorlog. Met de Duitse hereniging in 1990, werden de Oost-Duitse DDR-deelstaten onderdeel van de Bondsrepubliek. De Duitse federale grondwet bevat exclusieve bepalingen voor verantwoordelijkheden voor de federatie (het federale niveau), zoals buitenlandse zaken en defensie.[5] Alle andere verantwoordelijkheden, waaronder de wetgevende macht, liggen op deelstaatniveau, zoals inzake educatie, wetenschap en cultuur. Voor privacy en de bescherming van persoonsgegevens hebben zowel de federale overheid als de deelstaten wetgevende bevoegdheden en toezichthoudende

1 De deelstaten hebben in Duitsland ook hun eigen grondwetten. Deze bevatten ook grondrechten. In dit rapport zullen we enkel focussen op de federale grondwet.
2 Pintens, W. (1998), *Inleiding tot de rechtsvergelijking*. Leuven: Universitaire Pers Leuven.
3 Elfes, 6 BVerfGE 32, p. 41 (1957). Zie voor de rechtsontwikkeling met betrekking tot het recht op privacy in Duitsland ook Janssen, H.L., *Constitutionele interpretatie* (diss. UM), Den Haag: Sdu 2003, p. 296 e.v.
4 *Mikrozensus*, 27 BVerfGE 1, 6 (1969). Zie ook Dörr, D. and Aernecke, E. (2012), A never ending story: Caroline v Germany. In D. Dörr and R.L. Weaver (eds.), *The right to privacy in the light of media convergence*. Berlin: De Gruyter, p. 114.
5 Kommers, D.P. (2012), *The Constitutional Jurisprudence of the FederalRepublic of Germany*. Durham NC, Duke University Press.

autoriteit. In tegenstelling tot andere EU-landen verzamelt de Federale Commissaris voor de bescherming van persoonsgegevens (*Bundesdatenschutzbeauftragte* of *BfDI*) zelf geen gegevens over het algemeen bewustzijn van de bescherming van persoonsgegevens.[6] Echter, volgens andere bronnen[7] zijn de Duitse burgers zich over het algemeen redelijk goed bewust van problematiek rondom de bescherming van persoonsgegevens en de ontwikkelingen hieromtrent. Hetzelfde geldt voor bedrijven. Zodoende zijn hun maatregelen rondom de bescherming van persoonsgegevens normaal gesproken van hoge kwaliteit. Om deze inzichten te onderbouwen, zullen hieronder een aantal aanvullende bevindingen van onderzoeken van derden worden besproken.

Internetgebruik

Duitsland heeft ruim 80 miljoen inwoners waarvan een geschatte 71 miljoen, ofwel 89%, toegang heeft tot het internet en online diensten. Toch lijken Duitsers, in vergelijking tot burgers van andere EU-landen, terughoudend te zijn om deze diensten ook daadwerkelijk te gebruiken. Duitsland is een van de weinige landen waarbij minder dan de helft van de inwoners (46%, EU-gemiddelde 57%) minstens eens per week gebruikmaakt van online sociale netwerken.[8] Een soortgelijk aantal (48%) gebruikt instant messaging en chat websites ten minste een keer per week.[9] De mate waarin Duitsers het internet gebruiken voor het spelen van online games (17%, EU-gemiddelde 25%) of om muziek of video's uit te wisselen via peer-to-peer netwerken (8%, EU-gemiddelde 18%) is relatief laag. Duitsers scoren ook het laagst (18%, EU-gemiddelde 27%) als het gaat om de mate waarin ze telefoon- en videogespreken voeren via internet.[10] Er zijn echter bepaalde online diensten die Duitsers sneller geneigd zijn te gebruiken. Bijvoorbeeld, ongeveer 95% doet aankopen via internet (EU-gemiddelde 87%).[11] Ook maakt 40% van de Duitsers ten minste een keer per week gebruik van internetbankieren.[12]

(Gevoel van) controle

Volgens een recente studie heeft ongeveer 42% van de Duitsers het gevoel deels controle te hebben over de informatie die zij online verstrekken, terwijl 45% het gevoel heeft hier geen enkele controle over te hebben.[13] Slechts 4% heeft het gevoel volledige controle te hebben. Hiermee liggen de Duitse waarden iets lager dan de EU-gemiddelden met betrekking tot 'deels controle' (EU-gemiddelde 50%) en 'volledige controle' (EU-gemiddelde 15%), en bovengemiddeld met betrekking tot 'geen enkele controle' (EU-gemiddelde 31%). Over het algemeen lijken de Duitsers nogal bezorgd te zijn over het

6 German DPA Survey, p. 1.
7 Vodafone Survey on Big Data (2016); Eurobarometer 431 (2015); EMC Privacy Index of 2014; Consent Country Report Germany (2012).
8 Eurobarometer 431 (2015), p. 109.
9 Eurobarometer 431 (2015), p. 110.
10 Eurobarometer 431 (2015), p. 111.
11 Consent Country Report Germany (2012) p. 3.
12 Eurobarometer 431 (2015), p. 110.
13 Eurobarometer 431 (2015), p. 10.

gebrek aan controle. Ongeveer 70% van de mensen geeft aan bezorgd te zijn, tegenover een EU-gemiddelde van 69%.
78% van de Duitsers beschouwt het verstrekken van persoonlijke informatie als een onderdeel van het moderne leven. Dit ligt iets hoger dan het EU-gemiddelde (71%).[14] In deze context geeft ongeveer 38% aan het verstrekken van persoonsgegevens geen probleem te vinden, terwijl 56% zich hier juist zorgen over maakt.[15] Gevraagd naar het verstrekken van persoonsgegevens in ruil voor gratis online diensten, geeft 49% van de Duitsers aan dit te doen.[16] Deze uitkomst wordt door een andere recente studie bevestigd, waarbij ongeveer 54% van de ondervraagde Duitsers aangaf liever voor een online dienst te betalen dan de online dienstaanbieder toe te staan hun persoonsgegevens te gebruiken voor commerciële doeleinden.[17]

Bewustzijn
In vergelijking met de rest van de EU zijn Duitsers zich het meest bewust van het gebruik van persoonsgegevens door de eigenaren van websites.[18] Daarbij vinden zij het gebruik van persoonsgegevens door website-eigenaren om de inhoud van websites en advertenties te personaliseren in bovengemiddelde mate onacceptabel. Ook hebben zij aanzienlijk hogere niveaus van non-acceptatie als het gaat om het contacteren van gebruikers per e-mail, het diepgaand verzamelen van informatie, het verkopen van informatie of het hiervan beschikbaar stellen aan anderen. Dergelijke praktijken worden gezien als grotendeels onacceptabel en commerciële afwegingen veranderen hier in dit verband weinig aan. Ook hierbij hebben Duitsers over het algemeen het laagste acceptatieniveau (83%, EU-gemiddelde 74%). De daadwerkelijke ervaring van privacyinbreuk is al net zo hoog, Duitsers scoren hier 3,36 (EU-gemiddelde 2,89) op een 7-puntsschaal (1 = nooit, 7 = zeer vaak).[19]
Als het gaat om privacy policies, geven veel Duitsers (50%, EU-gemiddelde 47%) aan een website wel eens niet gebruikt te hebben vanwege onvrede over het betreffende privacybeleid. Een bijna even groot aantal Duitsers geeft echter aan de algemene voorwaarden (45%) of het privacybeleid (39%) van websites nooit of nauwelijks door te lezen.[20] Als Duitsers de privacy policies wel doorlezen, dan lezen zij net als andere EU-burgers zelden de hele tekst (Duitsland 13%, EU-gemiddelde 11%); desondanks is er een hoge mate van vertrouwen dat zij de tekst – als ze deze doorlezen – grotendeels of volledig begrijpen (Duitsland 73%, EU-gemiddelde 64%).

Vertrouwen
Wat betreft vertrouwen lopen Duitsers gelijk op met het EU-gemiddelde. Dit geldt voor sectoren als de gezondheidszorg (77%, EU-gemiddelde 74%), overheidsinstellingen (71%, EU-gemiddelde 66%) en banken en financiële instellingen (57%, EU-gemiddelde

14 Eurobarometer 431 (2015), p. 29.
15 Eurobarometer 431 (2015), p. 32.
16 Eurobarometer 431 (2015), p. 40.
17 Vodafone Survey on Big Data (2016), p.79.
18 Consent Country Report Germany (2012) p. 4.
19 Consent Country Report Germany (2012) p. 4.
20 Consent Country Report Germany (2012) p. 4.

56%). Vertrouwen in winkels ligt met 39% ook dicht bij het EU-gemiddelde (40%). Hetzelfde geldt voor telecom- en internetproviders (32%, EU-gemiddelde 33%). Vertrouwen in online bedrijven, zoals zoekmachines, ligt met 19% net onder het EU-gemiddelde (24%).
Gevraagd naar de algemene risico's verbonden aan het verstrekken van persoonsgegevens op sociale media, schatten Duisters deze iets lager in dan het EU-gemiddelde. Hetzelfde geldt voor specifieke risico's als reputatieschade, bedreiging van persoonlijke veiligheid of het risico om slachtoffer te worden van fraude of discriminatie. Risico's die verband houden met: gebruikersinformatie die gebruikt wordt zonder dat de gebruiker hiervan afweet (Duitsland 89%, EU-gemiddelde 74%), informatie die gedeeld wordt zonder dat de gebruiker hier toestemming voor gegeven heeft (Duitsland 82%, EU-gemiddelde 81%) of het ongewenst toesturen van aanbiedingen op basis van informatie die gedeeld is op sociale media; schatten Duitsers echter juist iets hoger in dan de gemiddelde EU-burger.[21]

Beschermingsmaatregelen
Het percentage Duitsers dat ooit heeft geprobeerd privacyinstellingen op hun socialemediaprofielen aan te passen is 54 (EU-gemiddelde 57%).[22] Een totaal van 61% (in vergelijking met een EU-gemiddelde van 64%) vindt het gemakkelijk om dit te doen.[23] Mensen die nooit geprobeerd hebben om de privacyinstellingen aan te passen, geven aan erop te vertrouwen dat de website gepaste instellingen hanteert (26%), dat ze niet weten hoe de instellingen veranderd kunnen worden (24%), dat ze niet bezorgd zijn over hun persoonsgegevens online (19%), dat ze geen tijd hebben naar de mogelijkheden te kijken (12%) of dat ze niet wisten dat deze instellingen aangepast kunnen worden (24%).[24] Met 77% van de mensen die vaak tot altijd de privacyinstellingen van hun persoonlijke profielen op sociale media aanpassen, scoren Duitsers ruim boven het EU-gemiddelde (54%). Bovendien geeft 90% (EU-gemiddelde 80%) van de Duitsers die hun privacyinstellingen aanpassen aan deze strikter te maken, zodat anderen minder informatie over hen kunnen zien.[25]
Als het gaat om specifieke technische maatregelen om persoonlijke internetbeveiliging te onderhouden of te verbeteren, zijn sommige maatregelen (zoals het blokkeren van pop-ups, het aanvinken van opt-in- en opt-outopties, het controleren op spyware en het verwijderen van de zoekgeschiedenis) populairder dan andere (zoals het blokkeren van e-mails), waarbij Duitsers over het algemeen iets hoger scoren dan het EU-gemiddelde.[26] Het vermogen om dergelijke technische maatregelen te nemen, wijst op een bepaald niveau van gepercipieerde controle over de praktijken van gegevensbeheerders van (socialemedia)websites.[27]

21 Consent Country Report Germany (2012) p. 4.
22 Eurobarometer 431 (2015), p. 92.
23 Eurobarometer 431 (2015), p. 95.
24 Eurobarometer 431 (2015), p. 98.
25 Consent Country Report Germany (2012) p. 4.
26 Consent Country Report Germany (2012) p. 3.
27 Consent Country Report Germany (2012) p. 38.

Nationale politiek

Sinds 2013 bestaat de regeringscoalitie in Duitsland uit de Christen-democratische Unie (CDU/CSU) en de Sociaal Democratische Partij (SPD). In het regeerakkoord[28] zijn de partijen overeengekomen om het bewaren van bepaalde telecommunicatiegegevens te beperken tot gevallen van ernstige strafbare feiten of levensgevaar. Bovendien zijn de partijen overeengekomen om de Europese termijn voor het bewaren van dergelijke data tot drie maanden te beperken en om strenge informatiebeveiligingsnormen te bevorderen. Sindsdien lijkt de bestuurlijke coalitie echter van koers te zijn veranderd. Tot nu toe waren alleen telecommunicatiebedrijven verplicht gegevens te bewaren. In een recente toespraak heeft de Duitse minister van Binnenlandse Zaken, De Maizière, echter verzocht om uitbreiding van deze verplichting naar alle media-aanbieders.[29]

Onder de grote politieke partijen lijkt er een groeiende consensus te zijn over de noodzaak van een strengere bescherming van privacy en persoonsgegevens. De Linkse Partij (Die Linke), de Vrije Democratische Partij (FDP), de Groene Partij (Bündnis 90/Die Grünen) en de Piratenpartij (Die Piratenpartei)[30] verzetten zich collectief tegen onvoorwaardelijke gegevensopslag. Dit is tevens een van de meest besproken onderwerpen rondom de bescherming van persoonsgegevens.[31]

De FDP heeft haar bezorgdheid geuit over de grondrechtelijkheid van cameratoezicht in openbare ruimtes, terwijl de Groene, de Linkse en de Piratenpartij er over het algemeen tegen zijn. Cameratoezicht in openbare ruimtes is sinds de nieuwjaarsnacht van 2015 onderdeel van een verhit publiek debat; er vonden toen tal van seksuele geweldplegingen plaats zonder dat de politie ingreep.[32] Hoewel de regeringscoalitie in 2013 heeft toegezegd cameratoezicht uit te breiden, heeft een recente uitspraak van de rechter bepaald dat een deel van de huidige methoden voor cameratoezicht in openbare ruimtes in strijd is met de grondwet. De uitspraak zette verder vraagtekens bij het streven van de overheid naar het vergroten van de surveillance-inspanningen.

Alle grote partijen zijn voor 'netneutraliteit', ofwel het op dezelfde manier en volgens dezelfde regels behandelen van alle gegevens op het internet. Ook verzetten zij zich tegen netwerkbewaking en de handel in data zonder de uitdrukkelijke toestemming van de gebruiker. De Linkse Partij pleit voor het 'recht om te worden vergeten', terwijl de Groene Partij de bescherming van persoonsgegevens op wil nemen in de grondwet. De Piratenpartij is op haar beurt voor het uitbreiden van de privacy van brieven naar alle vormen van communicatie.[33] Ondanks deze lopende debatten, heeft het Duitse

28 https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf, https://www.cdu.de/sites/default/files/media/dokumente/regierungsprogramm-2013-2017-langfassung-20130911.pdf, https://www3.spd.de/linkableblob/96686/data/20130415_regierungsprogramm_2013_2017.pdf.

29 Munster, p. 2.

30 De Piratenpartij is een nieuwe politieke partij met als hoofddoel privacy en de bescherming van persoonsgegevens te vergroten.

31 Munster, p. 2.

32 Eddy, M. (2016), 'Reports of Attacks on Women in Germany Heighten Tension Over Migrants', *The New York Times*, 5th January 2016.

33 Munster, p. 3.

parlement tijdens de huidige regeerperiode slechts tweemaal over de bescherming van persoonsgegevens gestemd.[34]
De Duitse federale gegevensbeschermingswet (Federal Data Protection Act – FDPA of *Bundesdatenschutzgesetz*) garandeert de aanstelling van een federale commissaris voor de bescherming van persoonsgegevens en vrijheid van informatie (zie paragraaf 3.5 voor meer details). Terwijl de commissaris toezicht houdt op de bescherming van persoonsgegevens bij overheidsinstellingen, bedrijven, telecommunicatie- en postdiensten informeert hij ook het publiek over de bescherming van persoonsgegevens. Daarnaast heeft de Duitse regering in 2013 de stichting voor de bescherming van data (Stiftung Datenschutz) opgericht.[35] Deze stichting streeft ernaar om zelfbescherming op het gebied van privacy te bevorderen.

Media-aandacht
Zowel belangrijke ontwikkelingen op het gebied van de bescherming van persoonsgegevens als hieraan gerelateerde incidenten krijgen regelmatig aandacht van de mainstream media.[36] Ook zijn er verschillende online platforms (www.heise.de, www.golem.de en www.netzpolitik.org) die toegelegd zijn op het schrijven over ontwikkelingen rondom de bescherming van persoonsgegevens en gegevensbeveiliging. De eerste twee zijn meer toegespitst op de technologische aspecten, terwijl netzpolitik.org een bredere focus heeft en publiceert over allerhande zaken rondom internet en de samenleving, netneutraliteit, de regulering van het internet, de impact van politiek op het internet en vice versa, en digitale vrijheden en de implementatie daarvan.[37] Interessant genoeg wordt netzpolitik.org bijna volledig gefinancierd door lezers en publiceert het platform jaarlijkse verslagen over hoe het de ontvangen donaties gebruikt.[38] Alle drie de platforms hebben een sterke voorkeur voor een uitgebreidere bescherming van persoonsgegevens.[39]
In de Duitse media voeren in de debatten rondom privacy en de bescherming van persoonsgegevens vooral de onthullingen van Snowden over de NSA en de openbaarmakingen van soortgelijke activiteiten door de Duitse Nationale Veiligheidsdienst (Bundesnachrichtendienst of BND), de boventoon.[40] Om die reden is gegevensover-

34 Munster, p. 1.
35 https://stiftungdatenschutz.org/startseite.
36 Zie bijvoorbeeld deze artikelen: http://www.faz.net/aktuell/politik/inland/mangelnder-datenschutz-fuer-wohnungssuchende-14484176.html; http://www.handelsblatt.com/adv/digitalatscale/spark-finalist-relayr-ploetzlich-vernetzt-/14545808.html; http://www.zeit.de/2016/43/datenschutz-terrorabwehr-geheimdienste-fluechtlinge-chemnitz; https://www.tagesschau.de/inland/faq-ip-adressen-103.html.
37 https://netzpolitik.org//about-this-blog/.
38 https://netzpolitik.org/2016/jahresbericht-uns-liegen-die-einnahmen-nicht-nur-vor-wir-veroeffentlichen-sie-auch/.
39 DPA survey, p. 1.
40 German DPA Survey, p. 2.

dracht naar de VS voor en na de *Safe Harbor*-uitspraak van het Europese Hof van Justitie regelmatig onderwerp van debat.[41]
Een verhit publiek debat is ook aangewakkerd door een voorgesteld wetsontwerp omtrent cameratoezicht dat zich richt op het uitbreiden van de bestaande bevoegdheden van inlichtingendiensten.[42] Daarnaast heeft de discussie tussen de verschillende takken van de overheid rondom een wetsontwerp om de Europese Algemene Verordening Gegevensbescherming (AVG) te implementeren in 2018, permanent een plek in de belangrijkste kranten en omroepen van Duitsland. In dit opzicht heeft een uitspraak van bondskanselier Angela Merkel, die pleit tegen het principe van dataminimalisatie (het principe dat data alleen verzameld mogen worden als het strikt noodzakelijk is en alleen zolang bewaard mogen worden als strikt noodzakelijk is), verder bijgedragen aan de controverse.[43]

Datalekken
Project Data Bescherming, een initiatief gelanceerd in september 2009 door PR-COM,[44] documenteert incidenten rondom de bescherming van persoonsgegevens, zoals datalekken bij bedrijven of overheidsorganisaties in Duitsland.[45] Ook onderzoekt het zaken gerelateerd aan de Snowden-onthullingen. Hierbij wordt er rekening gehouden met het feit dat incidenten elkaar in steeds sneller tempo opvolgen zodat het steeds lastiger wordt om ze allemaal bij te kunnen houden. Een ander doel van Project Data Bescherming is om alle betrokkenen bewust te maken van het voorzichtig en verantwoord omgaan met data.
Project Data Bescherming publiceert alle datalekken op zijn website, inclusief gegevens over de datum en oorsprong van de betreffende data, de aard van het incident, de getroffen organisatie en het aantal getroffen individuen.[46] Vaak gaat het hierbij om bedrijven, hoewel het soms ook om datalekken bij overheidsorganisaties gaat. Hieronder worden een paar recente incidenten besproken.
Een incident uit februari 2017 betreft een energiebedrijf uit Wissen (Rijnland-Palts). Het e-mailde 800 van zijn klanten en zette daarbij onbedoeld alle geadresseerden in cc zodat alle e-mailadressen zichtbaar waren. De directie heeft publiekelijk excuses gemaakt en de betrokkenen verzekerd dat het bedrijf de nodige stappen heeft genomen om te voldoen aan zijn juridische verplichtingen.[47]

41 http://www.handelsblatt.com/my/technik/it-internet/attacke-auf-google-und-co-transatlantische-daten-blockade/12506476.html?nlayer=Organisation_11804700; http://www.handelsblatt.com/technik/sicherheit-im-netz/datenschutz-in-deutschland-so-ungeschuetzt-sind-deutsche-surfer-im-netz/14592766.html.
42 German DPA Survey, p. 2.
43 http://www.handelsblatt.com/politik/deutschland/merkel-gegen-datensparsamkeit-bundesregierung-zerstreitet-sich-ueber-datenschutz/19237484.html.
44 PR-Com is een agentschap voor strategische communicatiebedrijven en pr in München, http://www.pr-com.de.
45 https://www.projekt-datenschutz.de/ueber-die-projekte.
46 https://www.projekt-datenschutz.de/datenschutzvorfaelle.
47 https://www.projekt-datenschutz.de/vorfall/mailing-versehentlich-ffentlichem-verteiler?position=0&list=_82070XiNPLS1iD65vURVFw7nY689qoiB8uWo-uUWck.

Een bericht uit november 2016 betreft een gehackt online carpooling portaal. Het bedrijf waarschuwde dat de gearchiveerde data van ex-klanten waren ontvreemd. De data bevatten onder meer 638.000 IBAN-nummers, 101.000 e-mailadressen, 15.000 mobiele nummers, en namen en adresgegevens.[48] Het bedrijf stelde dat er nog geen misbruik gemeld was en opende een speciaal telefoonnummer voor zijn klanten om vragen te beantwoorden over hun persoonlijke data.
In 2016 wordt er een veiligheidslek gemeld bij het Berlijnse bedrijf Aerticket dat online vliegtickets verkoopt. Dit lek bleek al in 2011 ontstaan.[49] Miljoenen mensen raken gedupeerd. Namen en adressen van passagiers, reisinformatie zoals vertrekluchthaven, datum en prijs van het ticket, maar ook betaalgegevens zoals IBAN- en BIC-nummers waren gemakkelijk online terug te vinden. Het veiligheidslek is inmiddels gedicht en volgens Aerticket zijn de gegevens niet door criminelen misbruikt. De zaak wordt momenteel onderzocht door de Berlijnse toezichthouder.[50] Exacte aantallen rondom rechtszaken of economische schade rondom deze veiligheidslekken zijn niet beschikbaar.

Burgerrechtenorganisaties
Er zijn verschillende burgerrechtenorganisaties die opkomen voor de bescherming van persoonsgegevens en de privacyrechten van Duitse en Europese burgers. De invloed van deze organisaties op het opstellen en handhaven van wetgeving moet niet onderschat worden. Zij nemen actief deel aan wetgevingscommissies door standpunten aan te dragen aan de betreffende wetsvoorstellen. Verder zien zij het als hun missie om gegevensmisbruik bij bedrijven en overheden aan het licht te brengen. Ze vragen de aandacht van het publiek door uitspraken naar de pers te doen en evenementen en lezingen te organiseren om zo de dialoog over de bescherming van persoonsgegevens gaande te houden. Een aantal van de sleutelfiguren op dit gebied worden hieronder besproken.
Consumentenadviescentra (*Verbraucherzentralen* of CAC's), gevestigd in alle 16 federale deelstaten, zijn onafhankelijke non-profitorganisaties die voornamelijk gefinancierd worden door publieke fondsen. Hun overkoepelende organisatie (*Verbraucherzentrale Bundesverband*) bestaat uit de 16 deelstaatbesturen samen met 25 andere burgerrechtenorganisaties. Hun missie is om consumenten te voorzien van relevante informatie en om hun belangen te vertegenwoordigen in politieke debatten op lokaal of landelijk niveau. De CAC's zijn de schakel tussen de overheid, de industrie en de consument. De bescherming van persoonsgegevens en de privacy van consumenten zijn thema's waarbij de CAC's erg betrokken zijn. Ze nemen dan ook actief deel aan politieke beslissingen op deze gebieden om namens de consumenten te lobbyen en wetsvoorstellen in te dienen.[51]
De Duitse Privacy Associatie (GPA), opgericht in 1997, is een non-profitorganisatie die de belangen van burgers als mensen achter de data en gegevens, behartigt. Een van

48 https://www.projekt-datenschutz.de/vorfall/mitfahrgelegenheitde-daten-gestohlen?position=4&list=_82070XiNPLS1iD65vURVFw7nY689qoiB8uWo-uUWck.
49 Stüber, J. (2016), 'Datenpanne bei Berliner Flugticket-Grosshändler', *Berliner Morgenpost*, 2 augustus 2016.
50 https://www.projekt-datenschutz.de/vorfall/pers-nliche-angaben-von-millionen-flugreisenden-offen-im-web?position=16&list=_82070XiNPLS1iD65vURVFw7nY689qoiB8uWo-uUWck.
51 https://www.verbraucherzentrale.nrw/home; http://www.vzbv.de/.

hun prioriteiten is het adviseren en voorlichten van burgers over de risico's van het elektronisch verwerken van informatie en de daarbij behorende implicaties op het recht op informationele zelfbeschikking. Om die reden publiceert de GPA regelmatig nieuwsbrieven en houdt zij persconferenties. Ook organiseert zij lezingen, houdt zij speeches tijdens evenementen en organiseert zij seminars voor verschillende doelgroepen (vakbonden, ondernemingsraden, etc.) in samenwerking met verschillende partnerorganisaties.[52] Verder neemt de GPA deel aan expertmeetings over verschillende wetten omtrent de bescherming van persoonsgegevens op zowel lokaal als landelijk niveau.

Het netwerk voor gegevensbeschermingsexpertise (NDPE of *Netzwerk Datenschutzexpertise*) is een samenwerkingsverband van experts die het publieke debat rondom de bescherming van persoonsgegevens en de bescherming van fundamentele rechten in de digitale wereld in het algemeen willen stimuleren. Zij zien zichzelf als een noodzakelijke aanvulling op het werk van andere burgerrechtenorganisaties. De NDPE streeft ernaar om wetenschappelijke artikelen over een verscheidenheid van onderwerpen aan te bieden, zoals informatietechnologie, het fundamentele recht op vertrouwelijkheid en integriteit in informatietechnologiesystemen, de vrijheid van meningsuiting op het internet, de vrijheid van informatie op het internet en andere constitutionele rechten zolang deze verwant zijn aan digitalisering. De NDPE onderzoekt specifieke kwesties, wetsvoorstellen en gerechtelijke uitspraken.[53]

De Vereniging voor Gegevensbescherming en Gegevensbeveiliging (ADPDS) is opgericht in 1976 en staat als een non-profitorganisatie voor praktische en effectieve gegevensbescherming. Zij zoekt en onderhoudt contacten met overheidsdiensten, gegevensbeschermingsautoriteiten, verenigingen en privacyexperts over de hele wereld. De vereniging helpt gegevensbeheerders en met name privacyfunctionarissen bij het uitoefenen van hun taken, om zo een goed evenwicht te bereiken tussen de belangen van de betrokkenen die bescherming verdienen en de gerechtvaardigde behoefte aan informatie van de controllers. Een belangrijk doel van de ADPDS is het versterken van effectieve zelfregulering en corporate self-monitoring, om het toezicht vanuit de overheid en de controle op gegevensbescherming zoveel mogelijk overbodig te maken.[54]

De stichting voor gegevensbescherming (*Stiftung Datenschutz*) is in 2013 door de federale overheid opgericht als een onafhankelijke organisatie. Haar doel is een platform voor discussie te bieden aan de verschillende stakeholders vanuit de publieke sector, de industrie, de wetenschap en de beleidsmakers, om voorstellen te ontwikkelen voor een praktijkgericht en goed werkend gegevensbeleid in Duitsland. De stichting ondersteunt het werk van de gegevensbeschermingsautoriteiten op nationaal en federaal niveau als neutrale instantie. Verder wil zij mensen bewustmaken van de waarde van hun persoonsgegevens.[55]

52 https://www.datenschutzverein.de/.
53 http://www.netzwerk-datenschutzexpertise.de/.
54 https://www.gdd.de/ueber-uns.
55 https://stiftungdatenschutz.org/ueber-uns/die-stiftung/.

3.2 Beleid

Nationaal beleid, Privacy Impact Assessments

Momenteel werken de meeste overheidsinstanties op federaal en deelstaatniveau toe naar de realisatie van de wetgeving die nodig is om de Europese Algemene Verordening Gegevensbescherming (AVG, EU 2016/679), die mei 2018 in werking treedt, in te kunnen voeren.[56]

In 2011 publiceerde het Bundesamt für Sicherheit in der Informationstechnik (BSI) een richtlijn[57] voor de implementatie van het Privacy Impact Assessment Framework (PIAF) voor radiofrequentie-identificatieapparatuur (RFID) dat door de industrie is ontwikkeld en mede gereguleerd werd door de Europese Commissie in mei 2009.[58] Het doel van de richtlijn was om de Duitse industrie in staat te stellen om te voldoen aan de aanbevelingen van de PIAF en tegelijkertijd het veilige gebruik van RFID's te bevorderen. Om de richtlijn te ontwikkelen, werkte de BSI nauw samen met de Vienna University of Economics and Business Administration.[59] De richtlijn beschrijft uitgebreid op wie de PIAF van toepassing is en biedt gedetailleerde informatie over hoe dit beoordeeld kan worden.[60] Verder wordt er ingegaan op privacydoelstellingen, potentiële bedreigingen en controles en bevat het document een evaluatiemethodiek waarmee privacyeisen en -bedreigingen kwalitatief geanalyseerd kunnen worden, zodat passende controlemaatregelen kunnen worden gekozen.[61] Privacy Impact Assessments (of *Datenschutz-Folgenabschätzung*) zijn niet verplicht onder de huidige federale privacywetgeving.

Privacy en de bescherming van persoonsgegevens in nieuw beleid

In het algemeen zijn privacy en gegevensbescherming belangrijk voor alle politieke partijen in Duitsland. Sinds het begin van deze zittingsperiode lijkt het erop dat de belangrijkste doelstellingen van de regeringscoalitie – met name met betrekking tot het bewaren van gegevens en dataminimalisatie – zijn veranderd. De huidige sociale, economische en politieke omstandigheden lijken hierbij bepalend te zijn.[62] Naar aanleiding van het idee dat iedereen moet kunnen profiteren van technologische vooruitgang en hier bovendien aan moet kunnen deelnemen, stimuleert de 'digitale agenda' van de

56 German DPA Survey, p. 2.

57 Privacy Impact Assessment Guideline for RFID Applications, available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1.

58 Commission of the European Communities (EC): Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification. Brussels, 2009. Available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009H0387.

59 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/RadioFrequencyIdentification/PIA/pia_node.html.

60 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1.

61 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Langfassung.pdf?__blob=publicationFile&v=1.

62 Munster, p. 2-3.

federale overheid de ontwikkeling van innovatieve diensten.[63] De digitale agenda heeft als prioriteiten: economische groei en werkgelegenheid, toegang tot en participatie in de digitale wereld, en veiligheid en vertrouwen binnen de IT-infrastructuur. Als een noodzakelijke voorwaarde om deze doelen te verwezenlijken, heeft de overheid ervoor gezorgd dat er een infrastructuur wordt gecreëerd die de uitdagingen van nieuwe datastromen het hoofd kan bieden.
Verschillende federale ministeries houden zich bezig met de invoering van de digitale agenda. Opmerkelijk is bijvoorbeeld de betrokkenheid van het Federale ministerie van Onderwijs en Onderzoek.[64] Dit ministerie ondersteunt diverse projecten die betrekking hebben op big data, waarvan de meest prominente 'Abida – Assessing Big Data' is.[65] Abida is een interdisciplinair project dat de kansen en risico's van big data bestudeert.[66] Het project dient als een kenniscentrum voor wetenschappers en praktijkmensen uit verschillende domeinen die werken aan vraagstukken rondom big data.

Maatschappelijk debat
De Duitse regering verzamelt input van een aantal NGO's en bedrijven voordat nieuwe wetgeving inzake gegevensbescherming wordt opgesteld en aangenomen. In dit opzicht kan de aanpak van de regering ten opzichte van het ontwerpen van nieuw beleid beschouwd worden als proactief ten opzichte van eventuele zorgen van burgers. Verder is elke burger gerechtigd om de overheidsinstanties te bereiken en informeren via petities en verzoekschriften.[67]

Informatiecampagnes
De federale toezichthouder (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI) publiceert talrijke informatiematerialen en activiteitenverslagen voor zowel de wetgevende instanties als het grote publiek.[68] De overheidsinstanties op staatsniveau doen hetzelfde voor hun respectievelijke verantwoordelijkheden. Alle toezichthouders zijn voortdurend op zoek naar nieuwe gelegenheden en strategieën om bewustwording van gegevensbescherming te bevorderen en om daarbij aansluitende informatie te publiceren.[69] Ook sommige federale ministeries publiceren met regelmaat informatie over kwesties rondom gegevensbescherming in een bredere context. In 2014 hebben de federale ministeries van Economie en Energie, Binnenlandse Zaken en Verkeer en Digitale Infrastructuur gezamenlijk de brochure 'Digitale Agenda 2014-2017' gepubliceerd, bedoeld om burgers te informeren over het digitale beleid van de overheid.[70] De brochure licht het digitaliseringsbeleid van de overheid in een aantal

63 https://www.digitale-agenda.de/Webs/DA/DE/Home/home_node.html; https://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/digitale-agenda-2014-2017,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.
64 https://www.bmbf.de/de/big-data-management-und-analyse-grosser-datenmengen-851.html.
65 www.abida.de.
66 http://www.abida.de/de/content/forschungsfragen-und-ziele.
67 German DPA Survey, p. 2.
68 German DPA Survey, p. 2.
69 German DPA Survey, p. 2.
70 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/digitale-agenda.html.

sectoren toe en gaat in op de middelen en initiatieven die de overheid gebruikt om dit beleid te implementeren. De belangrijkste onderwerpen van de handleiding zijn digitale infrastructuur; digitale economie en werk; innovatie van de staat; onderwijs, onderzoek, media en cultuur; en veiligheid voor de samenleving en de economie.[71] In het laatste gedeelte wordt uitgebreid ingegaan op de bescherming van persoonsgegevens van burgers en consumenten op het internet.
De deelnemende ministeries publiceren regelmatig verslagen en onderzoeksrapporten over ontwikkelingen omtrent de digitale agenda. Het laatste rapport over de bescherming van persoonsgegevens *Sicher unterwegs im Netz*[72] (veilig navigeren op internet) werd eind maart 2016 gepubliceerd, en bevat tips over hoe men zich kan beschermen tegen misbruik van persoonsgegevens.

3.3 Wet- en regelgeving

Implementatie van de EU-richtlijn
Hoewel pas na het verstrijken van de deadline van de EU, is richtlijn 95/46/EC inzake de bescherming van de verwerking van persoonsgegevens in de 16 Duitse deelstaten (*die Bundesländer*) eerder ingevoerd dan op federaal niveau. De deelstaatwetgeving is alleen van toepassing op de publieke sector.
Met de Federal Data Protection Act (FDPA of *Bundesdatenschutzgesetz*) is de EU-richtlijn met een vertraging van tweeënhalf jaar in de federale Duitse wet geïmplementeerd.[73] Eerdere pogingen om de richtlijn op federaal niveau te implementeren zijn mislukt door onenigheid over de gewenste omvang van de hervorming. Terwijl sommigen van de gelegenheid gebruik wilden maken te komen tot ingrijpende hervormingen van de huidige Duitse wetgeving inzake de bescherming van persoonsgegevens, drongen anderen er juist op aan om deze te behouden en slechts kleine veranderingen door te voeren. Onder druk van een inbreukprocedure volgens art. 226 ECT (huidige art. 258 TFEU) vanuit de Europese Commissie tegen Duitsland,[74] heeft de Duitse wetgever uiteindelijk besloten om de hervormingen voorlopig te beperken. Zo zijn er destijds slechts enkele aspecten geïntroduceerd ter aanvulling op de minimale eisen van de EU-richtlijn.[75] De wetgeving is in 2001 in werking getreden en is in 2003 en in de eerste helft van 2009 aanzienlijk gewijzigd. De wijzigingen in 2003 hadden voornamelijk betrekking op de registratie van gegevensverwerkers en de rechten en plichten van privacyfunctionarissen.[76] De wijzigingen in 2009 betroffen afzonderlijke bepalingen en

71 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/digitale-agenda.pdf;jsessionid=6655B3B8D024FE8B5F1790C4FBDDA3B2.2_cid287?__blob=publicationFile.
72 https://www.bundesregierung.de/Content/Infomaterial/BPA/Bestellservice/Sicher_unterwegs_im_Netz.pdf?__blob=publicationFile&v=17.
73 Dit had reeds 24.10.1998 moeten hebben plaatsgevonden.
74 Commission of the European Community against the Federal Republic of Germany, Rs. C-443/00.
75 Pseudonymisierung, data thrift en data avoidance, videosupervisie en data protection audit vallen hier onder andere onder.
76 https://www.bfdi.bund.de/bfdi_wiki/index.php/Synopse_BDSG_1990-2001-2003.

lijken verder de juridische oplossingen van op zichzelf staande problemen te hebben vergemakkelijkt.[77]
De FDPA wordt beschouwd als onduidelijk en bevat veel onduidelijke juridische concepten en dubbelzinnige wettelijke uitzonderingen.[78] Daarnaast beoordeelt het Europese Hof van Justitie de implementatie als ontoereikend.[79] Volgens de rechters voldoet de Duitse gegevensbeschermingshervorming niet aan de eisen van de EU-richtlijn. Hiermee schendt de FDPA 2001 de Europese wet.

Sectorale wetgeving
Zowel de Federale Data Protection Act (FDPA) als wetgeving op deelstaatniveau zijn alleen van toepassing indien er geen verdere sectorspecifieke regels zijn. De telecommunicatiewet (*Telekommunikationsgesetz*) bevat bijvoorbeeld specifieke gegevensbeschermingsbepalingen die van toepassing zijn op telecommunicatiediensten zoals internetproviders. De Duitse telemediawet (*Telemediengesetz*) bevat ook sectorspecifieke bepalingen die van toepassing zijn op telemediadienstverleners zoals websiteproviders. Daarnaast zijn regels voor online marketing via e-mail, sms of MMS vastgelegd in de wet tegen oneerlijke concurrentie (*Gesetz gegen den unlauteren Wettbewerb*).
Als gevolg van de gestelde eisen in artikel 8 van de EU-richtlijn inzake de bescherming van persoonsgegevens, bevat de FDPA-bepalingen voor 'bijzondere categorieën persoonsgegevens' in de artikelen 13 (2), 28 (6) tot (9) en 29 (5). Sectie 3 (9) verduidelijkt dat 'bijzonder' verwijst naar gegevens die betrekking hebben op iemands ras of etniciteit, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, gezondheid of seksualiteit. De lijst is uitputtend en gebaseerd op het non-discriminatiebeginsel in artikel 14 ECHR.[80] Informatie over strafbare feiten wordt niet gezien als gevoelige persoonsgegevens. De bepalingen kregen de kritiek dat de ernst van de effecten van het omgaan met gevoelige informatie niet alleen afhankelijk is van de aard van de informatie zelf, maar ook van de context waarin deze gebruikt wordt.[81] Zo kan schijnbaar onschuldige informatie, zoals een adres, ineens zeer gevoelige informatie worden als dit het adres van een psychiatrische instelling blijkt te zijn.
Sectie 3 (9) bevat geen verdere richtlijnen over hoe de status van de gegevens bepaald moet worden. Voor veel soorten informatie is het daarom nodig om na te gaan of ze tot een speciale categorie behoren (zoals bijvoorbeeld een aantekening als 'deelname aan turnwedstrijd' wordt beschouwd als een indicatie van een goede gezondheid). In lijn met de *ratio legis* ter bescherming tegen discriminatie, moeten ook gegevens die (indirect) verwijzen naar informatie die valt binnen de 'bijzondere categorieën persoonsgegevens' zoals vermeld in sectie 3 (9), als gevoelige informatie worden gezien. Bijvoorbeeld, huidskleur kan de etniciteit van een persoon onthullen, deelname aan een religieuze ceremonie onthult iemands religieuze overtuiging en de deelname aan een speciale revalidatie- of zelfhulpgroep wijst op een medische achtergrond. Mocht er echter twijfel

77 Munster, p. 10.
78 Munster, p. 10.
79 *EuGH*, Urt. v. 9.3.2010 – Rs. C-518/07.
80 https://www.bfdi.bund.de/bfdi_wiki/index.php/3_BDSG_Kommentar_Absatz_9.
81 Kommentar zum BDSG, 10. Auflage, § 3.

bestaan over de bewijskracht van de gegevens (bijvoorbeeld omdat er ook mensen zonder religieuze overtuiging of medische condities deel uitmaken van de groep), dan worden de data als niet-gevoelig beschouwd.[82]
De FDPA-regels maken het moeilijker om gevoelige informatie te verwerken zonder dit in het geheel te verbieden. De regels voor het verwerken van gevoelige informatie zijn terug te vinden in artikel 13 (2), 14 (5) en (6), 16 (1) nr. 2 voor overheidsinstanties en artikel 28 (6) tot (9), 29 (5), 30 (5) en 30a (5) voor de niet-overheid. Het verzamelen, verwerken en gebruiken van gevoelige informatie vereist, overeenkomstig sectie 4a (3), toestemming van de betrokkene.
De FDPA bevat ook aanvullende regels die van toepassing zijn op het verwerken van opnamen van beveiligingscamera's. Ook hebben de Duitse autoriteiten die gaan over de bescherming van persoonsgegevens in 2014 richtlijnen aangenomen voor het gebruik van cameratoezicht. Bovendien, alhoewel niet beschouwd als een bijzondere categorie persoonsgegevens, wordt informatie over strafbare feiten (vooral met betrekking tot misdrijven gepleegd door werknemers), behandeld als gevoeliger dan andere persoonsgegevens.[83]

Zelfregulering en gedragscodes
Zelfregulering wordt uitdrukkelijk aangemoedigd in artikel 38a van de FDPA, die de vereisten van EU-richtlijn 95/46/EC art. 27 formeel implementeert. De bepaling maakt het mogelijk om sectorspecifieke richtlijnen inzake de bescherming van persoonsgegevens te ontwikkelen in de vorm van gedragscodes. De gedragscodes zijn onderworpen aan de goedkeuring van de betreffende toezichthoudende instantie.[84] De gedachte achter de zelfregulering is om extra sectorspecifieke wetgeving onnodig te maken.[85]
Enkel beroepsorganisaties en brancheorganisaties die als doel hebben de invoering van gegevensbeschermingsmaatregelen voor al hun geaffilieerde bedrijven, handelaren of zzp'ers gelijk te trekken, kunnen gebruik maken van de bepaling.[86] Eenmaal goedgekeurd zijn de richtlijnen echter niet wettelijk bindend. Hun wettelijke status hangt grotendeels af van de statuten van de betreffende brancheorganisatie.[87]

3.4 Implementatie

Sectie 3a van de FDPA schrijft voor dat er zo min mogelijk persoonsgegevens moeten worden verzameld, verwerkt en gebruikt en dat dataverwerkingssystemen hier ook op uitgekozen en ingesteld moeten worden. Verder moeten organisaties persoonsgegevens anonimiseren als het doel waarvoor ze verwerkt worden dit toestaat en de benodigde

82 https://www.bfdi.bund.de/bfdi_wiki/index.php/3_BDSG_Kommentar_Absatz_9.
83 https://clientsites.linklaters.com/Clients/dataprotected/Pages/Germany.aspx#enforcement.
84 Omdat de bescherming van persoonsgegevens bij bedrijven valt onder de zeggenschap van de toezichthouders in de deelstaat, refereert artikel 38 (6) BDSG naar de betreffende deelstaatwet in het bepalen van de toezichthoudende autoriteit.
85 Bull, RDV 1999, 148.
86 Kommentar zum BDSG, 10. Auflage, § 38a, para. 4.
87 Kommentar zum BDSG, 10. Auflage, § 38a, para. 6.

inspanning om dit te doen niet disproportioneel is.[88] Het artikel wijst verder nog op het principe van dataminimalisatie en data-efficiency *(data economy)* en stelt daarmee eisen aan het ontwerp van de technische en organisatorische structuren die de mate van gegevensverwerking bepalen (*Privacy by Design*). Echter, aangezien het artikel ernaar streeft om algemene technologische doelen te stellen die niet afdwingbaar zijn[89] en de huidige dataverwerkingssystemen niet onwettig maken indien het artikel niet wordt nageleefd,[90] is *Privacy by Design* nog steeds zeldzaam in Duitsland. Bedrijven implementeren doorgaans een aantal beveiligingsmaatregelen, met name met betrekking tot IT-beveiliging, maar deze beschermen vaak alleen bedrijfsgegevens en bedrijfsgeheimen in plaats van persoonsgegevens.
Artikel 28 van de FDPA regelt het verzamelen en opslaan van persoonsgegevens voor zakelijke doeleinden. De bepaling staat de verzameling, opslag, wijziging, overdracht of het gebruik van persoonsgegevens toe in het geval dat dit nodig is om met de betrokkene een wettelijke of anderszins juridische verplichting op te stellen, uit te voeren of te beëindigen. Een voorwaarde is wel dat de verwerking noodzakelijk is om de gerechtvaardigde belangen van de databeheerder te waarborgen. Ook mag er geen reden zijn om aan te nemen dat de betrokkene een groot rechtmatig belang heeft om zijn of haar gegevens uit te laten sluiten van de gegevensverwerking in deze. De doelen van de gegevensverwerking moeten op concrete wijze vooraf zijn vastgelegd. Om ervoor te zorgen dat deze regels worden nageleefd, moeten organisaties een privacyfunctionaris aanwijzen, overeenkomstig sectie 4f FDPA.

Privacyfunctionarissen
Artikel 4f(1) van de FDPA stelt dat er een privacyfunctionaris moet worden aangewezen bij zowel bedrijven als overheidsorganisaties. Echter, organisaties met negen (of minder) personeelsleden die regelmatig persoonsgegevens verwerken, zijn hiervan vrijgesteld. Organisaties die geautomatiseerde gegevensverwerking gebruiken voor commerciële gegevensoverdracht, geanonimiseerde commerciële gegevensoverdracht of markt- of opinieonderzoek, moeten echter altijd een privacyfunctionaris aanstellen.[91] De privacyfunctionaris moet binnen een maand na aanvang van de gegevensverwerking worden benoemd. De privacyfunctionaris is onafhankelijk in de uitoefening van zijn taken en geniet een speciale bescherming tegen ontslag.[92] Verder voorzien uitdrukkelijke bepalingen dat de privacyfunctionaris voldoende expertise bezit op dit gebied.[93]
Privacyfunctionarissen houden vooral toezicht op de naleving van regels op het gebied van de bescherming van persoonsgegevens. Ook adviseren zij het management en de medewerkers over zaken rondom de bescherming van persoonsgegevens, over het opleiden van het personeel en fungeren zij als aanspreekpunt voor personen die zich voelen aangetast in hun rechten inzake bescherming van persoonsgegevens. Bovendien

88 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/germany#chaptercontent1.
89 Toezichthouders hebben alleen een adviserende rol. Zie Kommentar zum BDSG, 10. Auflage, § 3a, para. 2.
90 Kommentar zum BDSG, 10. Auflage, § 3a, para. 2.
91 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/germany#chaptercontent6.
92 Zie artikel 4f (3) 2 and 4f (3) 4-6 BDSG.
93 Zie artikel 4f (2) 1-2 BDSG.

voeren zij regelmatig controles uit op dataverwerkingsprocedures en stellen zij, op verzoek van de autoriteiten, een lijst van procedures op en stellen deze vervolgens ter beschikking. Afhankelijk van de omvang van de organisatie kunnen de taken van de privacyfunctionaris als fulltimebaan of als extra taak worden ontworpen.

Beveiligingsmaatregelen

Op grond van artikel 9 van de FDPA moet elke gegevensbeheerder passende technische en organisatorische maatregelen nemen om de juiste implementatie van de wetgeving omtrent de bescherming van persoonsgegevens te kunnen garanderen. Om de algemene uitgangspunten van artikel 9 te concretiseren en daarmee organisaties te begeleiden, heeft het Bundesamt für Sicherheit in der Informationstechnik (BSI) samen met afgezanten uit de industrie technische standaarden[94] ontwikkeld. Daarnaast stimuleert het BSI een specifieke methode van IT-basisbescherming die computerbeveiligingsmaatregelen identificeert en implementeert.[95] Organisaties die deze methode gebruiken kunnen een ISO/IEC 27001-certificaat verkrijgen.

Verder biedt Sectie 9a FDPA leveranciers van dataverwerkingssystemen de mogelijkheid om hun systemen te laten controleren om de beveiliging en de bescherming van persoonsgegevens te verbeteren. Als gevolg daarvan kunnen zowel leveranciers als organisaties die data verwerken, hun gegevensbeschermingsstrategieën en technische voorzieningen laten testen en evalueren door onafhankelijke en erkende auditors. De resultaten van de audit mogen gepubliceerd worden. De systeemevaluatiecriteria evenals de selectieprocedure van de auditoren zouden in een apart statuut moeten worden opgenomen. Er is tot nu toe echter nog geen dergelijk statuut opgesteld.[96] Sommige wetten op deelstaatniveau inzake de bescherming van persoonsgegevens voorzien in regels voor vrijwillige data-auditing.[97] Deze regels zijn echter alleen van toepassing op de overheidsinstanties van de betreffende deelstaat.

Wat zelfregulering betreft, blijkt Sectie 38a FDPA tot op heden geen brede implementatie te hebben gevonden. Wetenschappers stellen dat het ontbreken van duidelijke procedures voor het administratieve proces van goedkeuring van gedragscodes hiervan de oorzaak is.[98] Ook worden de door de wetgever opgestelde richtlijnen als te vaag beschouwd om daadwerkelijk een drijfveer te zijn om een gedragscode te ontwikkelen en hieraan te committeren.[99] In dit opzicht is het bijvoorbeeld onduidelijk welke eisen van toepassing zijn op de inhoud. Veel toezichthouders zijn er tot nu toe van uitgegaan

94 https://www.bsi.bund.de/DE/Themen/StandardsKriterien/standardskriterien_node.html.

95 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html; jsessionid=BB468510300255177D9DC2974F43883F.2_cid359.

96 Munster, p. 12.

97 § 11c Brandenburgisches Datenschutzgesetz; § 7b Bremisches Datenschutzgesetz; § 10a Datenschutzgesetz Nordrhein-Westfalen; § 4 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein.

98 Patrick von Braunmühl, Regulierte Selbstregulierung im Datenschutz, https://berliner-datenschutzrunde.de/node/145.

99 Patrick von Braunmühl, Regulierte Selbstregulierung im Datenschutz, https://berliner-datenschutzrunde.de/node/145.

dat de richtlijnen verder moeten gaan dan het wettelijk niveau van de bescherming van persoonsgegevens om te worden erkend.[100]

Transparantie

De FDPA legt een transparantieplicht op aan organisaties. In artikel 4 (3) worden gegevensbeheerders verplicht om de betrokkene te informeren als zijn of haar persoonsgegevens verzameld worden. De kennisgeving moet de identiteit van de gegevensbeheerder, het doel van de gegevensverzameling, de beoogde verwerking of het gebruik van de gegevens en de betreffende ontvangers bevatten. Deze laatste eis is echter enkel van toepassing wanneer de omstandigheden van een individuele zaak niet zodanig zijn dat de betrokkene er reeds van uit mocht gaan dat de gegevens worden verstrekt aan dergelijke ontvangers. Als bovendien persoonsgegevens worden verzameld op grond van een wettelijke bepaling die dit vereist voor het bevorderen van de rechtspositie van betrokkene, moet de betrokkene ook op de hoogte worden gebracht van het doel van de verzameling van de gegevens. Afhankelijk per geval of op verzoek van de betrokkene, dient deze laatste wettelijk te worden geïnformeerd over de gevolgen van het achterhouden van de vereiste gegevens.

Bovendien heeft het federale ministerie van Justitie en Consumentenbescherming in samenwerking met het internetplatform 'Consumentenbescherming in de Digitale Wereld'[101] een *one-pager* geïntroduceerd over transparantie van gegevensverwerking.[102] Dit is een overzicht van relevante informatie en is bedoeld als een gids voor organisaties die hun gegevensverwerking op een eenvoudige manier inzichtelijk willen maken voor de consument.

In een poging meer transparant en toegankelijk te zijn over hun gegevensverwerkingsbeleid, publiceren sommige organisaties dit (interne) beleid op hun website.[103] Ongeveer de helft van de Duitsers (45%) leest nooit tot nauwelijks de algemene voorwaarden, terwijl 39% akkoord gaat met privacybeleid zonder dit daadwerkelijk door te lezen.[104] Van degenen die privacyvoorwaarden lezen, leest ongeveer 89% niet de gehele tekst. Zo'n 73% claimt het merendeel of alles wat ze in het privacybeleid lezen te begrijpen. Bovendien blijkt dat ongeveer 50% ooit een keer heeft besloten een website niet meer te gebruiken vanwege ontevredenheid over de privacyvoorwaarden van de site.

100 Patrick von Braunmühl, Regulierte Selbstregulierung im Datenschutz, https://berliner-datenschutzrunde.de/node/145.

101 Het platform bestaat uit consumentenvertegenwoordigers en vertegenwoordigers uit de politiek, economie en wetenschap en gegevensbeschermingsorganisaties. Het platform richt zich momenteel op twee belangrijke initiatieven: 'Privacy door ontwerp/Gegevensbescherming via technologie' en 'Consumenten Soevereiniteit en Transparantie'.

102 https://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2015/11192915_Vorstellung_OnePager.html.

103 Zie bijvorbeeld Bayer http://www.bayer.com/en/group-regulation-data-protection-and-personal-data-privacy.aspx.

104 Consent Country Report Germany (2012), p. 36.

3.5 Toezicht en handhaving

Toezichthouders
De Duitse wet, zoals besproken in paragraaf 3.3, maakt onderscheid tussen toezichthouders voor de bescherming van persoonsgegevens op federaal en op deelstaatniveau. Op federaal niveau is de federale commissaris voor de bescherming van persoonsgegevens (*Bundesdatenschutzbeauftragte* of *BfDI*) hiervoor verantwoordelijk. Dit instituut is opgericht in 1978 en telt in het meeste recente begrotingsverslag 110 werknemers.[105]
De federale commissaris is enkel onderworpen aan de wet en is onafhankelijk in de uitoefening van zijn taken. Noch individuele ministers, noch de federale overheid kunnen de commissaris hierin aansturen. De bevoegdheden van de commissaris worden voornamelijk bepaald door artikel 24 en 26 van de FDPA. Volgens deze bepalingen houdt de commissaris toezicht op en handhaaft de naleving van de bescherming van persoonsgegevens bij de federale ministeries, overige federale overheidsinstanties, telecommunicatie- en postdiensten in het kader van de telecommunicatiewet (TKG) en de postwet (PostG), en bedrijven die vallen onder de SÜG (Sicherheitsüberprüfungsgesetz ofwel de Veiligheidscontrolewet).

Taken en bevoegdheden
Tot de taken van de BfDI behoren het geven van adviezen en aanbevelingen over de bescherming van persoonsgegevens, het indienen van vraagstukken en rapporten en ook legt hij elke twee jaar verantwoording af aan het Duitse parlement middels een activiteitenrapport.[106] Verder kan iedereen die vindt dat de instanties die onder zijn toezicht vallen inbreuk hebben gemaakt op hun privacy, hierover een klacht indienen bij de commissaris.[107] De commissaris zal de klacht onderzoeken en de betrokkene over de uitkomst informeren. Alle gegevens worden vertrouwelijk behandeld. Op verzoek van de klager kan deze anoniem blijven tot de overheidsinstantie hem of haar aanklaagt. Ook kunnen betrokkenen een klacht indienen bij de autoriteiten voor de bescherming van persoonsgegevens op deelstaatniveau (*Landesdatenschutzbeauftragten*) indien zij van mening zijn dat hun rechten geschonden zijn in het betreffende rechtsgebied. Rechtspraak op deelstaatniveau voor bedrijven en andere niet-overheidsinstanties wordt bepaald door hun respectievelijke locatie.[108] Het toezicht op de bescherming van persoonsgegevens voor particulieren behoort tot het takenpakket van de regionale autoriteiten.[109] Er zijn zestien instanties op deelstaatniveau die toezicht houden op de bescherming van persoonsgegevens bij bedrijven en de overheidsinstellingen binnen

105 https://www.bundeshaushalt-info.de/fileadmin/de.bundeshaushalt/content_de/dokumente/2016/soll/epl21.pdf.
106 http://www.bmi.bund.de/SharedDocs/Behoerden/DE/bfdi_einzel.html.
107 http://www.bfdi.bund.de/DE/BfDI/Artikel_BFDI/AufgabenBFDI.html.
108 Text und Erläuterungen zum BDSG, p. 64.
109 See Section 38 FDPA.

hun deelstaat en deze tevens handhaven.[110] Deze instanties zijn gebonden door wetgeving inzake de bescherming van persoonsgegevens op deelstaatniveau.
De FDPA is niet van toepassing op kerken en kerkelijke instellingen. Daarom hebben de evangelische kerk, de evangelische regionale kerken en de bisdommen van de katholieke kerk hun eigen autoriteiten voor de bescherming van persoonsgegevens aangesteld.
Autoriteiten voor de bescherming van persoonsgegevens op zowel federaal als deelstaatniveau zijn bevoegd om handhavingsmaatregelen te nemen. Naar aanleiding van data audits, meestal uitgevoerd in de vorm van inspecties of vragenlijsten, kunnen zij (soms in samenwerking met andere overheidsinstanties) organisaties 1) administratieve boetes opleggen,[111] 2) verplichten om de geconstateerde overtreding te verhelpen en 3) in het geval van ernstige schendingen de organisatie een verbod opleggen om door te gaan met gegevensverwerkingsprocedures. Voor strafrechtelijke sancties moeten de autoriteiten volgens artikel 44 (2) FDPA echter doorverwijzen naar het openbaar ministerie. Deze laatste kan geldboetes en gevangenisstraffen tot twee jaar opleggen.[112]
Autoriteiten voor de bescherming van persoonsgegevens hebben een adviserende rol bij wetsontwerpen inzake de bescherming van persoonsgegevens. Hun advies is alleen bindend voor uitvoeringsverordeningen.[113]

Gebruik van bevoegdheden
In 2016 heeft de BfDI 3.699 schriftelijke klachten en 6.687 telefonische informatieverzoeken ontvangen.[114] Verdere informatie over de aard en uitkomst van deze klachten is echter moeilijk te verkrijgen aangezien de BfDI deze cijfers niet publiceert. Hetzelfde geldt voor cijfers en informatie met betrekking tot de hoeveelheid klachten die de toezichthouders (DPA's) op deelstaatniveau ontvangen en behandelen. Ook zij publiceren hierover geen informatie. Slechts enkele klachten worden via persberichten of de media openbaar gemaakt en enkel als de zaak door de betreffende DPA als nieuwswaardig wordt beschouwd. Enkele van deze gevallen worden hierna behandeld. Ieder van de gevallen toont aan dat de naleving van de bescherming van persoonsgegevens door de Duitse DPA's en rechtbanken erg serieus wordt genomen.
Enkele van de recentere voorbeelden betreffen de DPA's van Rijnland-Palts en Beieren. Opmerkelijk is een zaak uit december 2014 waarbij de DPA van Rijnland-Palts een boete van € 1.300.000 aan verzekeringsgroep Debeka opgelegde.[115] Volgens het persbe-

110 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/germany#chaptercontent; https://www.bfdi.bund.de/bfdi_wiki/index.php/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte.
111 Zowel de federale als deelstaattoezichthouders kunnen volgens artikel 43 (1) BDSG boetes tot € 50,000 opleggen aan bedrijven (deelstaat toezichthouders) en overheid (federale toezichthouder) die zich niet aan hun informatieplicht hebben gehouden. Hetzelfde geldt volgens artikel 43 (2) BDSG voor het niet aanstellen van een privacyfunctionaris. Hier kan de boete oplopen tot € 300.000.
112 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/germany#chaptercontent14.
113 Text und Erläuterungen zum BDSG, p. 9; See also Data Protection in the European Union: the role of National Data Protection Authorities, 2010, p. 28.
114 German DPA Survey, p. 3.
115 https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/bussgeldverfahren-gegen-die-debeka-einvernehmlich-abgeschlossen-debeka-akzeptiert-geldbusse-und-gar/.

richt heeft het sales team (in sommige gevallen tegen een vergoeding) lijsten met contactgegevens van potentiële klanten verkregen, zonder dat deze hiervoor toestemming hadden gegeven. Bovendien ging dit in tegen het interne beleid van Debeka. Debeka kreeg de boete opgelegd vanwege het gebrek aan interne controles en schending van de wetgeving inzake de bescherming van persoonsgegevens. Naast de geldelijke boete werd Debeka verplicht gesteld zich te houden aan strikte gegevensbeschermingsprocedures. Hieronder viel ook dat medewerkers eerst schriftelijke toestemming van de klanten moesten verkrijgen alvorens zij hun adressen bekend mochten maken. Het bedrijf heeft verder toegezegd om 600.000 euro extra ter beschikking te stellen ter financiering van een leerstoel aan de Johannes Gutenberg Universiteit van Mainz, ter bevordering van de bescherming van persoonsgegevens en de uitvoering hiervan in de praktijk.
Ook zijn er recente voorbeelden van de Beierse DPA. Op 30 juli 2015 bracht deze een persbericht[116] uit waarin het bekendmaakte een grote boete te hebben opgelegd vanwege de onrechtmatige overdracht van e-mailadressen van klanten van een online winkel. De boete werd zowel aan de verkoper als de koper opgelegd omdat zij beiden geen toestemming van de klanten hadden en ook geen stappen hadden ondernomen om deze te informeren. Beiden handelden hiermee in strijd met de wet. De DPA gaf ook aan dat beide organisaties gegevensbeheerders waren, hetgeen een grotere mate van verantwoordelijkheid met zich meebrengt. Hoewel de hoogte van de boete niet werd onthuld, blijkt uit het persbericht dat deze ten minste uit vijf cijfers bestaat.
Op 26 augustus 2015 kwam er een persbericht[117] naar buiten waarin bekend werd gemaakt dat er een aanzienlijke boete was opgelegd aan een gegevensbeheerder voor het niet specificeren van beveiligingscontroles ter bescherming van persoonsgegevens in een gegevensverwerkingsovereenkomst met een ingehuurde gegevensverwerker. De DPA stelde dat de gegevensverwerkingsovereenkomst niet genoeg informatie bevatte omtrent de technische en organisationele maatregelen die getroffen zouden moeten worden om persoonsgegevens te beschermen. Verder werd de overeenkomst vaag bevonden en bleek deze alleen de wettelijk opgelegde bepalingen te herhalen. In alle gegevensverwerkingsovereenkomsten moeten de volgende controles worden gespecificeerd: (1) fysieke toegangscontrole, (2) virtuele toegangscontrole, (3) autorisatiecontrole, (4) transmissiecontrole, (5) invoercontrole, (6) opdrachtcontrole, (7) beschikbaarheidscontrole en (8) scheidingscontrole.

Reputatie

In tegenstelling tot andere EU-toezichthouders voor de bescherming van persoonsgegevens, voert de Duitse DPA (of een andere publieke/particuliere organisatie) zelf geen onderzoek uit naar de mening van de burgers of bedrijven over de uitoefening van hun beleid of hun populariteit. Daarom zijn officiële statistische bronnen grotendeels afwezig.

116 https://www.lda.bayern.de/media/pm2015_10.pdf.

117 https://www.datenschutzbeauftragter-online.de/datenschutz-aufsicht-bayern-bussgeld-vertrag-auftragsdatenverarbeitung/9001/.

Echter, media-aandacht naar aanleiding van de aanstelling van de commissaris in 2013 en krantenartikelen over de eerste twee jaar in deze rol wijzen erop dat het publiek de DPA grotendeels onzichtbaar lijkt te vinden.[118] Hoewel men op de hoogte is van de DPA en zijn activiteiten, blijkt er behoefte te zijn aan meer interactie met zowel de commissaris als zijn kantoor. Verder is de BfDI bekritiseerd omdat hij steun heeft uitgesproken voor plannen voor massale gegevensverzameling door de Duitse regering. Dit is volgens velen in strijd met zijn mandaat ter bescherming van persoonsgegevens.[119]

118 http://www.zeit.de/digital/datenschutz/2013-12/datenschutzbeauftragte-vosshoff-bundestag-gewaehlt; http://www.zeit.de/2015/51/andrea-vosshoff-datenschutz-telekommunikation.

119 http://www.zeit.de/digital/datenschutz/2013-12/datenschutzbeauftragte-vosshoff-bundestag-gewaehlt.

4. Zweden

4.1 Algemene situatie[1]

De Zweedse grondwet bestaat uit vier fundamentele wetten (*grundlager*). Dit zijn onder meer de wet van troonopvolging uit 1810 (Successionsordningen), de wet inzake persvrijheid uit 1949 (Tryckfrihetsförordningen), het 'regeringsinstrument' uit 1974 (Regeringsformen) en het fundamentele recht van vrijheid van meningsuiting uit 1991 (Yttrandefrihetsgrundlagen). Deze bevatten alle een aantal bepalingen die relevant zijn voor het recht op privacy. Zo bevat artikel 2 van hoofdstuk 1 van het regeringsinstrument bijvoorbeeld de bepaling dat overheidsinstellingen het privéleven en gezinsleven van betrokkenen zullen beschermen. In artikel 6 van hoofdstuk 2 is een bepaling opgenomen om eenieder te beschermen tegen fouillering, huiszoekingen en andere dergelijke soorten van schending van privacy, waaronder ook schending van de privacy van post, correspondentie, telefoongesprekken en vertrouwelijke communicatie. Zweden is ondertekenaar van de Universele Verklaring van de Rechten van de Mens (*Universal Declaration of Human Rights, UDHR*), het Europees Verdrag voor de Rechten van de Mens (*European Convention on Human Rights, ECHR*) en het Internationaal Verdrag inzake burgerrechten en politieke rechten (*International Covenant on Civil and Political Rights, ICCPR*), drie wettelijke instrumenten die een recht op privacy bevatten (respectievelijk in de artikelen 12, 8 en 17). Zweden volgt een dualistische benadering van internationale verdragen. Een internationaal verdrag moet dus eerst worden omgezet in nationale wetgeving om de bepalingen voor de Zweedse rechtbanken en overheidsinstanties toepasbaar te maken.[2] Internationale verplichtingen die voortkomen uit een geratificeerd verdrag, wegen niet automatisch zwaarder dan de grondwet.[3]
Zweden heeft, net als de andere Scandinavische landen, een lange traditie van transparantie met betrekking tot gegevens over persoonlijk inkomen en eigendom. Omdat de publieke middelen, zoals onderwijs en gezondheidszorg, door de staat worden betaald en relatief hoge belastingtarieven vereisen, biedt deze transparantie burgers de mogelijkheid om melding te maken wanneer zij merken dat de belastingwetgeving niet wordt nageleefd. Als tegenhanger van deze traditie was Zweden ook vroeg met het vastleggen

1 Vertalingen van Zweedse terminologie: *personsuppgift* = persoonsgegevens, *personsuppgiftsombud* = privacyfunctionaris, *personuppgiftsbehandling* = verwerken van persoonsgegevens, *integritet* = privacy.
2 Hermida, J. (2004), *Legal basis for national space legislation*. Dordrecht: Kluwer, p. 141.
3 Council of Europe (2001), The implications for Council of Europe Member States of the Ratification of the Rome Statute of the International Criminal Court, Progress Report, Sweden, consult/icc 37.

van grenzen aan welke informatie beschikbaar zou moeten worden gesteld. De Zweedse *Datalag* uit 1973 was in feite het eerste wetsvoorstel gegevensbescherming ter wereld.[4] De Zweedse cultuur is egalitair, individualistisch en richt zich meer op verzorging dan op concurrentie. Gematigdheid speelt een centrale rol in de cultuur, zoals uitgedrukt wordt in het Zweedse woord *lagom*, wat 'niet te veel, niet te weinig' betekent. Over het algemeen hebben de Zweden een ontspannen en optimistische levenshouding.[5]

Internetgebruik

Zweden telt bijna 10 miljoen inwoners, waarvan naar schatting 94% gebruikmaakt van het internet (dit is het op drie na hoogste aantal ter wereld, na de Falklandeilanden, IJsland en Noorwegen). Internetsnelheid is het op een na hoogste ter wereld, na Noorwegen.[6] Zweedse mensen zijn zeer actief online, met name als het gaat om sociale media en online bankieren. Zo gebruikt 66% van de Zweden sociale media minstens een keer per week – dit is de vijfde plaats in vergelijking met de andere EU-landen (EU-gemiddelde is 57%).[7] Ze behoren ook tot de topgebruikers van online bankieren (67%, duidelijk boven het EU-gemiddelde van 43%).[8]

Het gebruik van instant messaging en chatwebsites is iets lager dan het EU-gemiddelde, 52% gaf aan dit minstens een keer per week te gebruiken (EU-gemiddelde 53%).[9] 31% gebruikt het internet ten minste een keer per week om (video)gesprekken te voeren, hetgeen ietwat hoger ligt dan het EU-gemiddelde van 27%.[10] Als het gaat om online aankoopgedrag nemen de Zweden ook een middenpositie in; er zijn weinig mensen die nooit online winkelen (12%). Een groot aantal doet dit wel en dan gemiddeld minder dan één keer per week (74% vergeleken met het EU-gemiddelde van 59%).[11] Zweden scoren relatief gezien laag wanneer er gekeken wordt naar het gebruik van internet voor online games. 69% speelt nooit online games (EU-gemiddelde 59%) en slechts 20% doet dit vaker dan een keer per week (tegenover een gemiddelde van 25%).[12]

(Gevoel van) controle

Zweden behoren tot de groep Europeanen die zich het minste zorgen maken over het gebrek aan controle over hun persoonsgegevens (41%). Alleen Estland scoort op dit gebied lager (met 37%, EU-gemiddelde op 67%).[13] De Zweedse bevolking is het niet eens met de stelling dat hun overheid steeds meer informatie vraagt (27% gaat wel akkoord met deze stelling), hetgeen Zweden het laagst scorende Europese land maakt

4 DATALAG (Svensk författningssamling [SFS] 1973:289); Peter Siepel, Sweden, in NORDIC DATA PROTECTION LAW 115, 116 (Peter Blume Ed., 2001).
5 https://geert-hofstede.com/sweden.html.
6 https://www.stateoftheinternet.com/downloads/pdfs/Q4-2015-SOTI-Connectivity-Executive-Summary.pdf.
7 Eurobarometer 431 (2015), p. 109.
8 Eurobarometer 431 (2015), p. 110.
9 Eurobarometer 431 (2015), p. 110-111.
10 Eurobarometer 431 (2015), p. 111.
11 Eurobarometer 431 (2015), p. 112.
12 Eurobarometer 431 (2015), p. 111.
13 Eurobarometer 431 (2015), p. 13.

(EU-gemiddelde 56%). Deze cijfers zijn ook aanzienlijk lager dan in 2010, toen 40% het wel eens was met de stelling.[14]
Een relatief klein percentage Zweden is bereid te betalen voor diensten in ruil voor het prijsgeven van persoonlijke informatie (24%, EU-gemiddelde 29%). Dit percentage neemt duidelijk af sinds 2010 toen dit nog op 32 lag.[15] Een onderzoek[16] naar de houding van consumenten ten opzichte van algemene voorwaarden in de EU laat zien dat algemene voorwaarden in Zweden het minst vaak geaccepteerd worden en in de meeste gevallen worden nagelezen.[17]

Bewustzijn
De EU-enquête[18] over de houding van de consument ten aanzien van algemene voorwaarden toont aan dat bekendheid met consumentenorganisaties in Zweden zeer laag is (2,49 op een 7-punts schaal).[19] NGO D-FRI (*Föreningen för Digitala Frioch Rättigheter*) geeft aan dat zij het lage bewustzijn onder Zweedse burgers en organisaties omtrent gegevensbescherming als een van de grootste problemen zien.[20]

Vertrouwen
Wanneer er gekeken wordt naar de mate van vertrouwen die Zweden hebben in verschillende soorten organisaties als het gaat om het verantwoordelijk omgaan met hun gegevens, is de Zweedse bevolking het minst bezorgd dat autoriteiten en bedrijven gebruikmaken van hun informatie voor andere doeleinden dan waarvoor verzameld en waar de betrokkenen niet over zijn ingelicht (slechts 41% tegenover 69% gemiddeld in de EU). Relatief weinig Zweden zijn van mening dat de handhaving van de regels inzake gegevensbescherming op Europees niveau geregeld moet worden, in vergelijking met het Europese gemiddelde (45%) en vooral ten opzichte van Nederland en Frankrijk (respectievelijk 61% en 62%).[21]

Beschermingsmaatregelen
Uit een onderzoek naar cybernormen door de universiteit van Lund uitgevoerd in 2012, is gebleken dat een toenemend aantal Zweden (ongeveer 15% in de leeftijdsgroep van 15-25 jaar en een geschat totaal van 700.000 mensen) technieken gebruikt om online anoniem te blijven uit angst voor online toezicht. Het onderzoek suggereert dat dit verband houdt met de toentertijd opkomende invoering van de auteurswet (de IPRED-wet).[22]

14 Eurobarometer 431 (2015), p. 31.
15 Eurobarometer 431 (2015), p. 33.
16 CentERdata, Tilburg University, *Study on consumers' attitudes towards Terms and Conditions*, final report. Publications Office of the EU, Luxembourg 2016, doi:10.2818/950733.
17 Terms & Conditions 2016, Tables 7.19, p. 82 and 7.27, p. 88.
18 CentERdata, Tilburg University, *Study on consumers' attitudes towards Terms and Conditions*, final report. Publications Office of the EU, Luxembourg 2016, doi:10.2818/950733.
19 Terms & Conditions 2016, p.71.
20 Response from D-FRI to our enquiry (by Peter Michanek, secretary, March 2017).
21 Eurobarometer 431 (2015), p. 48.
22 https://www.svd.se/allt-fler-svenskar-anonyma-pa-natet (1 may 2012, consulted 21/2/2017).

Nationale politiek

Een Internet Policy Review uit 2013 vermeldt het volgende ten aanzien van Zweden: "Het lijkt erop dat Zweden vanuit een beleidsperspectief een interessant voorbeeld is, omdat het als vrij en neutraal wordt gezien, terwijl er tegelijkertijd een zware en zeer betwiste beleidsaanpak wordt uitgeoefend."[23] In de webindex van de World Wide Web Foundation staat Zweden op de eerste plaats van de in totaal 61 geïndexeerd landen, als zijnde het land waar internet de belangrijkste politieke, sociale en economische impact heeft. Verrassend genoeg heeft de Zweedse implementatie van de richtlijn inzake de handhaving van intellectuele eigendomsrechten (IPRED) de reikwijdte van de richtlijn dermate overschreden, dat critici stellen dat het recht op privacy wordt beperkt. Vergelijkbaar is het aannemen van de FRA-wet begin 2009, een wettelijke maatregel die overheidsinstanties het recht geeft om toezicht te houden op internetverkeer. Dit heeft controverse veroorzaakt, aangezien de wet verder gaat dan het door de Europese Commissie vastgestelde controlegebied. Als gevolg hiervan hebben sommige NGO's de zaak voor het Europees Hof voor de Rechten van de Mens gebracht wegens schending van de mensenrechten.[24]

Scandinavië heeft een traditie van openheid met betrekking tot persoonsgegevens ten aanzien van belastingen en dit is ook het geval in Zweden. Sites zoals Eniro, Hitta.se, Birthday.se, Ratsit en Merinfo[25] maken gebruik van die beschikbare informatie en staan eenieder toe om contactgegevens (straatadres, telefoonnummer en e-mailadres) op te zoeken, evenals de geboortedatum van iedereen die geregistreerd staat als inwoner van Zweden. Deze sites hebben een zogenoemde *openbare machtiging* en zijn derhalve vrijgesteld van de wet bescherming persoonsgegevens.

Zweden heeft de ambitie om "de beste van de wereld te worden in het benutten van de mogelijkheden die digitalisering biedt".[26] Om de vooruitgang bij de verwezenlijking van dit beleidsdoel te kunnen volgen en analyseren, heeft de Zweedse regering in 2012 de digitalisatiecommissie opgericht. Deze commissie heeft ook de taak om voorstellen voor nieuwe beleidsmaatregelen te presenteren, waarbij de voordelen van de digitale transformatie worden benadrukt en best practices worden gedeeld. In hun rapport aan de Zweedse regering over digitale transformatie 'Veiligheid en privacy in een digitaal tijdperk', dat in december 2015 werd gepresenteerd, is dit als een van de zes strategische gebieden geïdentificeerd.[27]

In de begeleidende bloemlezing over digitale mogelijkheden,[28] een verzameling bijdragen van verschillende deskundigen, wordt gegevensbescherming alleen genoemd in een hoofdstuk 'De deconstructie van de digitale economie. Vooruitgang op weg naar een holistisch IT-beleidskader' door Irene Ek en Rene Summer, als een van de *demand-side*

23 *Internet Policy Review*, Vol 2 Issue 2, 10 May 2013, Merlin Münch.

24 https://policyreview.info/articles/analysis/do-swedes-do-internet-policy-and-regulation-sweden-snapshot.

25 http://www.datainspektionen.se/fragor-och-svar/personuppgiftslagen/fragor-och-svar-om-webbplatser-med-utgivningsbevis/.

26 https://digitaliseringskommissionen.se/in-english/.

27 Digitaliseringens transformerande kraft – vägval för framtiden. Met betrekking tot de vertaling: *integritet* is het Zweedse woord voor privacy.

28 *https://digitaliseringskommissionen.se/wp-content/uploads/2015/11/SOU2015_65_engvers_webb.pdf.*

IT-beleidsproblemen.[29] In het hoofdstuk 'De biologische samenleving' beweert Anders Ekholm dat "persoonlijke privacy, zoals nu het geval is, is gebaseerd op het standpunt van een extreem kleine minderheid van de bevolking, namelijk juristen van de Zweedse overheidsinstanties". Hij raadt aan de rol van toezichthouder voor de bescherming van persoonsgegevens te herdefiniëren om de taken af te kunnen schaffen die obstakels voor innovatie en efficiëntie vormen.[30]
De huidige minderheidsregering (138 van de 349 zetels in het parlement) bestaat uit de Sociaal Democratische Partij (*Socialdemokraterna*, 113 zetels) en de Groene Partij (*Miljöpartiet de gröna*, 25 zetels). De Groene Partij in het bijzonder benadrukt het belang van het recht op privacy:[31] Zij wil 1) het recht op privacy in de grondwet, 2) het eerbiedigen van het bescherming van privacy in internationale samenwerkingen (VN, EU), 3) het herzien van de FRA-wet, en 4) het legaal maken van het delen van bestanden voor persoonlijk gebruik. De sociaal-democraten stellen in hun politieke programma de FRA- en IPRED-wetten (punten 3 en 4 van de Groene Partij) te willen vervangen, een ombudsman op het gebied van privacy te willen oprichten en in het algemeen wetgeving voor mediagebruik te willen maken die meer toekomstgericht is.[32]
De grootste oppositiepartij is de conservatieve partij (*Moderaterne*, 84 zetels), die de houding ten opzichte van privacy als volgt beschrijft: "We hebben een open samenleving met een reeks waarden gebaseerd op tolerantie, vrijheid, gelijkheid en eerbiediging van mensenrechten. Wetten die persoonlijke integriteit beperken, moeten evenredig, noodzakelijk en passend zijn. De bescherming van de privacy moet sterk zijn."[33] Op lokaal niveau geven de conservatieven wel aan dat meer toezicht op openbare ruimtes wenselijk kan zijn ter bestrijding van georganiseerde criminaliteit.[34] De derde grootste partij is de Zweedse Democraten (49 zetels). Zij hebben geen expliciete verklaring omtrent privacy, maar in hun veiligheidsbeleid verleent deze partij wel steun aan toenemend gebruik van gegevens (met inbegrip van persoonsgegevens, onder meer om pedofielen te volgen en terrorisme te kunnen bestrijden).[35]

Media-aandacht

De Zweedse krant Dagens Nyheter publiceerde eind augustus/begin september 2015 een uitgebreid dossier over privacy,[36] waaraan ook op de Zweedse nationale televisie aandacht werd besteed.[37] Deze krant heeft onlangs ook melding gedaan van het feit dat de politie zwaar investeert in nieuwe slimme camerabewakingssystemen, waarbij wordt aangegeven dat deze alleen kunnen worden geplaatst op locaties met een aantoonbaar

29 Digitaliseringskommissionen, *Digital Opportunies 2015,* p. 151-179.
30 Digitaliseringskommissionen, *Digital Opportunies 2015,* p. 71-95.
31 https://www.mp.se/politik/internet-och-integritet.
32 https://www.socialdemokraterna.se/upload/Internationellt/Dokument/Political%20guidelines.pdf (p. 92).
33 http://www.moderat.se/integritet (3 november 2015, consulted 21/2/2017).
34 http://www.moderat.se/ett-tryggare-linkoping/trygghet-kontra-integritet (13 juni 2014, consulted 21/2/2017).
35 https://sd.se/wp-content/uploads/2015/01/Kriminalprogram_2015-10-26.pdf (p. 7).
36 http://www.dn.se/stories/dn-granskar-vara-overvakade-liv/ (31/8-2/9/2015, consulted 17/2/2017).
37 http://www.svt.se/opinion/article3451479.svt (7/9/2015, consulted 17/2/2017).

hoog criminaliteitsrisico, op grond van de wetgeving inzake privacybescherming.[38] De algemene houding ten opzichte van dergelijke nieuwsberichten lijkt te zijn dat persoonlijke gegevens beter beschermd moeten worden.
Artikelen die gaan over privacy in verband met internetgebruik verschijnen ongeveer één keer per twee maanden in de grote kranten.[39] In gespecialiseerde media is dit (natuurlijk) vaker. Zo publiceert CIO Zweden van de technologische website www.IDG.se voor IT-professionals artikelen over de Algemene Verordening Gegevensbescherming (AVG) door middel van interviews met vier Chief Information Officers (CIO's) over hoe ze zich voorbereiden op de AVG.[40]

Datalekken
Er heeft de afgelopen jaren een aantal hacks en datalekken plaatsgevonden. In 2011 werd een hacker die op dat moment 90.000 e-mailadressen en wachtwoorden openbaar maakte als meest desastreuze datalek gezien.[41] Overheidsservers werden door de hackersgroep Anonymous gehackt als vergelding voor acties tegen The Pirate Bay in 2014.[42] Ook het Zweedse bedrijf Spotify heeft in 2014 met een datalek te maken gehad.[43]
Zoals reeds genoemd, heeft het aannemen van de FRA-wet in begin 2009 – een wettelijke maatregel die overheidsinstanties het recht geeft om toezicht te houden op internetverkeer – controverse veroorzaakt aangezien de wet verder gaat dan het door de Europese Commissie vastgestelde controlegebied. Zo heeft Sveriges Konsumenten bijvoorbeeld de fitness-app MyFitnessPals aangeklaagd omdat de algemene voorwaarden in strijd waren met de Zweedse wet inzake gegevensbescherming en de EU-richtlijn betreffende gegevensbescherming.[44]
De toezichthouder heeft in 2014 in totaal 85 inspecties uitgevoerd, hetgeen een daling is ten opzichte van de 209 inspecties in 2013.[45] De sancties die worden opgelegd voor schending van de wet zijn normaliter boetes en schadevergoedingen die worden toegekend aan het slachtoffer. Het bedrag van de geldboetes varieert afhankelijk van de ernst van het misdrijf en het inkomen van de persoon die verantwoordelijk is voor de overtreding van de wetgeving inzake de bescherming van persoonsgegevens.
In 2013 heeft de Zweedse Commissie voor Veiligheid en Integriteitsbescherming (*Säkerhets- en integriteitsskyddsnämnden* of 'SAKINT' in het Zweeds), die de politie en de rechterlijke instanties inspecteert, geconstateerd dat de verwerking van een register van 'reizende mensen' dat door de politie in het zuiden van Zweden werd bijgehouden, in verschillende opzichten onwettig was. Het register bevatte ongeveer 4.000 namen

38 http://www.aftonbladet.se/senastenytt/ttnyheter/inrikes/article24398726.ab (13/2/2017, consulted 17/2/2017).
39 Inventory of online news content of Dagens Nyheter, Svenska Dagbladet, and Dagens Media (dd. 17/2/2017).
40 http://cio.idg.se/2.1782/1.675960/gdpr-cio-forberedelser (consulted 20-02-2017).
41 http://www.bcs.org/content/conWebDoc/42623.
42 http://thehackernews.com/2014/12/anonymous-pirate-bay.html.
43 https://news.spotify.com/us/2014/05/27/important-notice-to-our-users/.
44 http://www.sverigeskonsumenter.se/nyheter-press/pressmeddelanden/sveriges-konsumenter-anmaler-traningsapp/ (publ. 30 March 2016).
45 LinkLaters Data Protected, https://clientsites.linklaters.com/Clients/dataprotected/Pages/Sweden.aspx.

van Roma's in Zweden. De ernstigste overtreding was dat het doel van de verwerking veel te breed was. SAKINT verklaarde dat een onnauwkeurig omschreven doel geen voldoende grondslag biedt voor de verwerking van persoonsgegevens, omdat dit in de praktijk de bescherming van de integriteit van de betrokkene ondermijnt. SAKINT onderzoekt momenteel de acties die de politie heeft genomen om een einde te maken aan de overtredingen.[46]
Er zijn gevallen geweest waarbij gevangenisstraf werd opgelegd voor het inbreuk maken op de wetgeving inzake de bescherming van persoonsgegevens, met name wanneer de inbreukmaker ook aanvullende misdrijven heeft gepleegd, zoals ernstige smaad. Een zaak waar gevangenisstraf voor de inbreuk op de wetgeving inzake de bescherming van persoonsgegevens werd opgelegd, betrof twee personen met nazistische neigingen die een register hadden opgesteld met gegevens van een grote groep mensen ten aanzien van hun religieuze en politieke overtuigingen, seksleven en ras. De veroordeling had hoofdzakelijk betrekking op de overtreding van de wetgeving inzake de bescherming van persoonsgegevens. Een van de slachtoffers van die inbreuk kreeg 10.000 Zweedse kronen aan schadevergoedingen (wat toentertijd ongeveer gelijk was aan 1.070 euro).[47]

Burgerrechtenorganisaties
DFRI (*Föreningen för Digitala Frioch Rättigheter*, uit te spreken als D-Fri, wat staat voor 'D-free') is een organisatie zonder winstoogmerk en zonder politieke overtuiging die zich inzet voor de bevordering van digitale rechten en lid is van European Digital Rights (EDRi).[48] De organisatie heeft momenteel 80 leden en werkt uitsluitend met vrijwilligers (geen werknemers). Haar budget is ongeveer 80.000 Zweedse kronen per jaar (ongeveer 8.400 euro).[49] Ze streeft ernaar om een samenleving tot stand te brengen die zo min mogelijk toezicht, tracking en onderschepping nodig heeft.
DFRI verdedigt vrijheid van meningsuiting, transparantie en vrijheid van informatie, privacy en het recht op zelfbeschikking ten aanzien van persoonlijke informatie en digitale voetafdrukken. Ook heeft ze protesten georganiseerd tegen verscherpt toezicht.[50] Tevens heeft ze in 2014 de toezichthouder (*Datainspektionen*) geholpen met de technische details van het onderzoek dat liep tegen het monitoringcentrum van Bumbee Lab voor het gebruik van MAC-adressen.[51]
In 2012 richtte voormalig Europees parlementslid Amelia Andersdotter in samenwerking met webdesigner Plus Stahre de website Dataskydd.net op. Sinds april 2015 is het officieel een ledenorganisatie zonder winstoogmerk en zonder politieke overtuiging geworden. Het voornaamste doel hiervan is gefundeerde beslissingen over wetgeving en technologie te bevorderen, die in overeenstemming zijn met het fundamentele recht op gegevensbescherming en privacy.[52]

46 LinkLaters Data Protected, https://clientsites.linklaters.com/Clients/dataprotected/Pages/Sweden.aspx.
47 LinkLaters Data Protected, https://clientsites.linklaters.com/Clients/dataprotected/Pages/Sweden.aspx.
48 https://www.dfri.se/dfri/.
49 Response from D-FRI to our enquiry (by Peter Michanek, secretary, March 2017).
50 Dagens Nyheter, 14 april 2016: http://www.dn.se/sthlm/protester-mot-okad-overvakning/.
51 https://www.dfri.se/mobilkartlaggning-bryter-mot-lagen/, http://www.datainspektionen.se/Documents/beslut/2015-06-23-vasteras.pdf.
52 https://dataskydd.net/om.

In een verklaring aan belanghebbenden voor het Universal Periodic Report 2012-2016 van UNHRC, maakt de Britse NGO Privacy International melding van de volgende aandachtsgebieden die betrekking hebben op privacy:[53] het aan het NSA-gerelateerde toezichtsprogramma FRA (zie hiervoor), de strafregisterdatabank Lexbase, de zaak die door SAKINT is voorgelegd (zie hiervoor), veiligheidsschending van de persoonsgegevenssilo van Logica, praktijken van de Zweedse geheime dienst met betrekking tot telecommunicatiedata waardoor overheidsinstanties toegang hebben tot communicatie van burgers die via de Zweedse netwerken plaatsvindt, en de afwezigheid van controlemaatregelen die de uitvoer van surveillancetechnologie naar onderdrukkende regimes verhinderen.

4.2 Beleid

Nationaal beleid, Privacy Impact Assessments

De Zweedse regering heeft drie beleidsprioriteiten geïdentificeerd, maar in geen hiervan lijkt gegevensbescherming een expliciete rol te spelen (een nieuwe arbeidsagenda, onderwijs en toonaangevend zijn op het gebied van emissiereductie ter vertraging van klimaatverandering).[54] De beleidsverklaring van de huidige minderheidsregering (138 van de 349 parlementaire zetels), bestaande uit de Sociaal Democratische Partij (*Socialdemokraterna*, 113 zetels) en de Groene Partij (*Miljöpartiet de gröna*, 25 zetels), vermeldt het volgende over privacy en gegevensbescherming:[55] "De overheid zal zich in Zweden en de EU inzetten om de rechtszekerheid en persoonlijke privacy te verbeteren en schenkt hierbij ook aandacht aan gegevensopslag. De toezichthouder en de parlementaire commissie voor privacy zullen een evaluatie van de bestaande wetgeving uitvoeren, rekening houdend met het toenemend aantal actoren uit de particuliere sector dat informatie verzamelt over consumenten."

Privacy en de bescherming van persoonsgegevens in nieuw beleid

In het verslag over de uitvoering van EU-richtlijn 95/46/EC in 2010, noemt het Zweedse ministerie van Justitie de verwerking van persoonsgegevens in de vorm van geluids- en beeldgegevens, de opkomst van *cloud computing* en onbeperkte gegevensverwerking (*ubiquitous computing*) als reden om de noodzaak van een hervorming van het juridisch kader voor gegevensbescherming te onderstrepen. Dit herziene juridisch kader moet algemeen aanvaard worden in een geglobaliseerde maatschappij en in staat zijn om te gaan met veranderingen die inherent zijn aan de snelle technologische ontwikkeling. Een vereenvoudiging van de Algemene Verordening Gegevensbescherming (AVG) zou waarschijnlijk ook een positief effect hebben in de zin dat het een bevordering van de acceptatie en eerbiediging van de gegevensbeschermingsprincipes in de praktijk kan

53 Privacy International, *The right to Privacy in Sweden*, stakeholder report for the UNHRC Universal Periodic Report, 2nd cycle 2012-2016 (21st session, January 2015 for Sweden).

54 http://www.regeringen.se/regeringens-politik/regeringens-prioriteringar/.

55 Beleidsverklaring Zweedse minderheidsregering, 2014, p. 19.

bewerkstelligen, aangezien de regels die van toepassing zijn op de verwerking begrijpelijker worden en aldus te rechtvaardigen zijn.[56]
Het ministerie schrijft ook dat de steeds nieuw opduikende verschijnselen die specifieke risico's ten aanzien van privacy met zich meebrengen en waar aandacht van de samenleving in een vroeg stadium doorslaggevend kan zijn voor de mate van privacy van individuen een andere uitdaging is. In het licht van deze ontwikkeling is het van belang dat gegevensbeschermingsautoriteiten effectieve instrumenten tot hun beschikking hebben om vroegtijdig nieuwe fenomenen die specifieke risico's kunnen opleveren te ontdekken en controleren. Een mogelijke manier zou zijn om de huidige algemene meldplicht met bijbehorende uitzonderingen te vervangen door een beperkte meldplicht met een aantal positieve uitzonderingen. Een dergelijke meldplicht kan gericht worden op nieuwe verschijnselen en technische toepassingen en de toezichthoudende autoriteiten zouden gemachtigd kunnen worden om voorschriften uit te vaardigen betreffende de strekking van de genoemde meldplicht.[57]

Maatschappelijk debat
Elk jaar legt de Zweedse regering ongeveer 200 wetsvoorstellen voor aan het parlement. Veel van deze voorstellen vereisen uitvoerige beraadslagingen en debatten voordat er gestemd wordt.[58] Hoewel de meeste wetsvoorstellen ingediend worden door de overheid, kunnen deze ook gebaseerd zijn op suggesties die zijn binnengekomen van het parlement, burgers, belangengroepen of overheidsinstanties. Voorafgaand aan de opstelling van wetsvoorstellen is er een onderzoeksfase waarbij de zaak geanalyseerd en geëvalueerd wordt. Deze taak kan worden toegewezen aan onafhankelijke personen of commissies, waaronder deskundigen, ambtenaren en politici. Als de onderzoeksfase is afgerond, wordt er een verwijzingsprocedure gestart waarbij relevante instanties worden geraadpleegd. Dit kunnen onder meer overheidsinstanties, belangengroepen en andere instanties zijn wier werkzaamheden door de voorstellen kunnen worden beïnvloed. Door middel van dit proces worden de meningen van burgers en bedrijven (via speciale belangengroepen) in aanmerking genomen.
Het maatschappelijk debat over burgerrechten, waarvan privacy en gegevensbescherming ook deel uitmaken, vindt ook plaats buiten de meer formele wetgevingsprocedures. Toen bijvoorbeeld de surveillancewet (FRA) werd voorgesteld, vond in Zweden een uitgebreid maatschappelijk debat plaats.[59] (Zie de vorige paragraaf voor meer informatie over aandacht van de media voor gegevensbescherming.)

Informatiecampagnes
Een brochure over de wet inzake gegevensbescherming werd in 2006 ter beschikking gesteld op de overheidssite www.regering.se en is in 2015 bijgewerkt.[60] De website is

56 Memorandum 23 april 2010, Question 18, p.14-15.
57 Memorandum 23 april 2010, Questions 19-21, p. 14-18.
58 http://www.government.se/how-sweden-is-governed/swedish-legislation-how-laws-are-made/.
59 https://professorsblogg.com/2008/09/22/sweden-the-surveillance-law-fra-debate/.
60 http://www.regeringen.se/informationsmaterial/2006/12/personal-data-protection/, voor het laatst geraadpleegd op 9 december 2016.

het belangrijkste communicatiemiddel van de *Datainspektionen*.[61] Deze toezichthouder heeft ook een website gelanceerd waar online misbruik kan worden gerapporteerd: www.krankt.se. De *Datainspektionen* publiceert een publiekstijdschrift over privacy: Privacy in Focus (*Integriteit i Focus*).[62]

4.3 Wet- en regelgeving

Implementatie van de EU-richtlijn

Zweden was het eerste land ter wereld dat beschikte over gegevensbeschermingswetgeving, met de datawet (*Datalag*) in 1973.[63] Deze werd in 1998 aangepast en vervangen, in overeenstemming met de EU-richtlijn 95/46/EC inzake de bescherming van persoonsgegevens, nadat Zweden zich in 1995 bij de EU had aangesloten. De website Library of Congress Online Privacy Law schrijft het volgende over het karakter van de wetgeving in Zweden:[64] "Er bestaat een belangrijk onderscheid tussen privacywetten en de manier waarop Zweden de persoonlijke integriteit van zijn burgers beschermt.[65] De Zweedse privacywetgeving richt zich op het gebruik van persoonlijke en gevoelige online informatie door anderen en niet op het individuele recht op privacy wanneer hij of zij online is, dat wil zeggen het recht om anoniem online te blijven."[66]

De richtlijn 95/46/EC is in Zweden voornamelijk geïmplementeerd door middel van de Wet op persoonsgegevens (*Personal Data Act, PDA*) (1998: 204), de persoonsgegevensverordening (*Personal Data Ordinance* 1998: 1191) en een groot aantal sectorspecifieke wetten.[67] Naast de PDA zijn aanvullende voorschriften opgenomen in de persoonsgegevensverordening (1998: 1191) (*Personuppgiftsförordningen*) en het wetboek (DFIS) van de gegevensbeschermingsautoriteit (*Data Protection Authority (DPA)* of in het Zweeds*Datainspektionen*). Indien bepalingen in andere wetteksten afwijken van wat in de PDA staat, zullen deze voorschriften prioriteit hebben (als *lex specialis*).[68] De overheid heeft ook voorbereidingen voor de nieuwe Algemene Verordening Gegevensbescherming (AVG) gepubliceerd.[69]

---

61 Datainspektionens årsredovisning 2014 – Dnr 231-2015, p. 8.

62 https://www.joomag.com/en/newsstand/integritet-i-fokus/M0368835001443601288.

63 DATALAG (Svensk författningssamling [SFS] 1973:289); Peter Siepel, Sweden, in NORDIC DATA PROTECTION LAW 115, 116 (Peter Blume ed., 2001).

64 www.loc.gov/law/help/online-privacy-law/sweden.php.

65 This distinction is mentioned in Siepel, supra note 1, at 119.

66 THOMAS CARLÉN-WENDELS, NÄTJURIDIK – LAG OCH RÄTT PÅ INTERNET 95-98 (3rd Ed. 2000).

67 Voor meer informatie en algemene achtergrond over de wet- en regelgeving in Zweden met betrekking tot EU richtlijn 95/46/EC aangaande de verwerking van persoonsgegevens, zie:
'Questionnaire for Member States on the Implementation of Directive 95/46/EC' and 'Annex 1-4';
'Myndighetsdatalag SOU 2015:39', een publicatie van de Zweedse overheid, Official Reports (SOU Series) (hoofdstuk 3.2.2 en hoofdstuk 4.1.2-4.2.2).

68 Cf. the Thomson Reuters Practical Law Privacy in Sweden Overview: http://uk.practicallaw.com/3-385-8827.

69 http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/.

Sectorale wetgeving

Er zijn meer dan 300 sectorspecifieke wetten en voorschriften in Zweden die regelingen bevatten voor de verwerking van persoonsgegevens binnen verschillende werkgebieden.[70] De Wet patiëntgegevens (2008:355) en de Wet geneesmiddelen (2009: 367) regelen het gebruik van persoonsgegevens in de zorgsector. Het gebruik van persoonsgegevens voor reclame- en marketingdoeleinden wordt gereguleerd in de Marketingwet (2008: 486) en de Wet op namen en afbeeldingen in reclame (1978:800). Het gebruik van kredietinformatie over particulieren en incassobedrijven, waarvoor doorgaans een vergunning van de DPA nodig is, valt onder de Wet kredietgegevens (1973:1173) en de Wet schuldsanering (1974:182).

De Wet electronische communicatie (LEK, 2003:389) implementeert EU-richtlijn 2002/58/EG inzake het beschermen van privacy in de sector elektronische communicatie. Hij bevat onder meer bepalingen over het behoud van gegevens die zijn gegenereerd of verwerkt in verband met de levering van elektronische communicatienetwerken en -diensten. De Wet cameratoezicht (2013: 460) (*Kameraövervakningslag*) is van toepassing op cameratoezicht in Zweden en verwerking van de desbetreffende beeld- en geluidsopnamen. Een vergunning is over het algemeen vereist voor het toezicht houden op openbare ruimtes.

Zelfregulering en gedragscodes

Gedecentraliseerde regelgeving en zelfregulering is niet ongebruikelijk in Zweden. In plaats van het hanteren van een sterk regelgevend lichaam, wordt er veel gebruikgemaakt van zelfregulering die voortkomt uit onderhandelingen.[71] Zo heeft de effectenmarkt een instantie voor zelfregulering van de particuliere verzekeringsmaatschappijen.[72] Ook op het gebied van gegevensbescherming vindt er zelfregulering plaats. Zo heeft een breed collectief van industrieorganisaties en online internationale en binnenlandse bedrijven samengewerkt aan een gedragscode voor het gebruik van cookies.[73]

In 2013 organiseerde de Koninklijke Academie voor Ingenieurswetenschappen (IVA) een seminar genaamd 'Svensk moral på export' (Zweedse moraal voor export). De toenmalige minister van Financiën, Peter Norman, heeft tijdens de slotzitting het duurzaamheidsbeleid van de staat besproken, waarbij gelijkheid, diversiteit, milieu, mensenrechten, arbeid, corruptiebestrijding en bedrijfsethiek aan bod kwamen. Hij zei: "Wij geloven dat dit waarde creëert. Er worden meer klanten aangetrokken als er rekening gehouden wordt met deze zaken en dit vergoot ook de kans dat naar andere belangrijke zaken gekeken wordt." Om deze reden heeft de overheid alle staatsbedrijven verplicht om zelf een reeks meetbare duurzaamheidsdoelen vast te stellen die verenigbaar zijn met hun activiteiten.[74]

---

70 Thomson Reuters Practical Law Privacy in Sweden Overview: http://uk.practicallaw.com/3-385-8827.

71 Boddewyn, J.J. (1985), 'The Swedish Consumer Ombudsman System and Advertising Self-Regulation', *The Journal of Consumer Affairs*, Vol. 19, No. 1, p. 140-162.

72 http://www.corporategovernanceboard.se/about-the-board/swedish-self-regulation.

73 http://iclg.com/practice-areas/data-protection/data-protection-2016/sweden.

74 http://www.iva.se/publicerat/hog-etik-kan-bli-svensk-konkurrensfordel/.

4.4 Implementatie

Privacyfunctionarissen

Gegevensbeheerders zijn niet verplicht om een privacyfunctionaris (*Personuppgiftsombud*) aan te stellen. Als een gegevensbeheerder een privacyfunctionaris heeft geregistreerd bij de DPA, wordt hij vrijgesteld van de verplichting om de DPA op de hoogte te brengen wanneer er een begin wordt gemaakt met de verwerking van persoonsgegevens. In dat geval dient de privacyfunctionaris een register bij te houden waarin de verwerking van persoonsgegevens door de gegevensbeheerder wordt vastgelegd.[75]

De privacyfunctionaris heeft geen specifieke kwalificaties nodig en kan een werknemer of een extern persoon zijn, zoals een advocaat. De privacyfunctionaris draagt er op onafhankelijke wijze zorg voor dat de gegevensbeheerder persoonsgegevens op een wettige, correcte manier en in overeenstemming met 'good practices' verwerkt en dient tevens te wijzen op eventuele onvolkomenheden. De privacyfunctionaris dient de DPA op de hoogte te brengen als er sprake is van een ontoereikende reactie op de gemelde overschrijding van de bepalingen die van toepassing zijn op de verwerking van persoonsgegevens. Bovendien moet de privacyfunctionaris de DPA raadplegen als hij twijfelt aan de toepasbaarheid van de regels. De privacyfunctionaris dient geregistreerde personen te ondersteunen bij het verkrijgen van een rectificatie wanneer er reden bestaat om te vermoeden dat de verwerkte persoonsgegevens onjuist of onvolledig zijn.[76]

In 2015 (in vergelijking met 2014) steeg het aantal geregistreerde privacyfunctionarissen van 7.276 tot 7.513 (een stijging van 3%). Het aantal mensen dat als privacyfunctionaris werkte steeg van 4.548 naar 4.756 (een stijging van 5%). Een persoon kan privacyfunctionaris zijn bij meerdere databeheerders en tegelijkertijd kan een databeheerder meerdere mensen registreren als privacyfunctionaris.[77]

Beveiligingsmaatregelen

De *Datainspektionen* biedt informatie en richtlijnen voor bedrijven om Privacy by Design (*innbygd integritet*) te implementeren.[78] In een folder met richtlijnen voor persoonsgegevensbeveiliging uit 2008 wordt de 27000 ISO-beveiligingscertificaat-serie als aanvullende bron genoemd.[79]

Transparantie

Artikel 14 (b) van EU-richtlijn 95/46/EC is omgezet in artikel 11 van de Personal Data Act. Onder de genoemde bepaling mogen persoonsgegevens niet worden gebruikt voor direct marketing-doeleinden indien de betrokkene de beheerder schriftelijk heeft medegedeeld dat hij of zij niet akkoord gaat met dergelijke verwerking. Het ministerie van Justitie heeft informatiemateriaal in het Zweeds en Engels uitgegeven over de

75 https://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/sweden.
76 https://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/sweden.
77 Annual report 2015 of Datainspektionen: http://www.datainspektionen.se/Documents/arsredovisning-2015.pdf (p. 10).
78 http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/inbyggd-integritet-privacy-by-design/.
79 http://www.datainspektionen.se/Documents/faktabroschyr-allmannarad-sakerhet.pdf.

rechten van de betrokkene op basis van de Personal Data Act. Deze informatie en aanvullende toelichting is onder andere beschikbaar op de website van het ministerie van Justitie.
De Data Inspection Board informeert de betrokkenen over hun rechten op grond van artikel 11 van de Personal Data Act, door middel van verschillende informatiebrochures ('Het afwegen van belangen op basis van de Personal Data Act', 'Persoonlijke registers in Zweden' en 'Uw rechten volgens de Personal Data Act'). De informatie is verkrijgbaar in gedrukte vorm en op de website van de Data Inspection Board. Op de website is ook informatie te vinden over de rechten van de betrokkenen in de rubriek vragen en antwoorden.
In Zweden zijn particuliere zogenoemde NIX-registers, NIX-adressen en een NIX-telefoon opgezet. Particulieren kunnen NIX op de hoogte stellen van het feit dat ze niet per post of telefoon benaderd willen worden voor marketingdoeleinden. Particulieren hebben ook de mogelijkheid om zich tot SPAR te wenden, het register van de staat dat persoonlijke adressen bevat en aan te geven dat deze gegevens niet voor directe marketingdoeleinden bekend moeten worden gemaakt. Marketingmanagers die goede marketingpraktijken hanteren, controleren deze registers voordat er beslissingen omtrent marketing worden genomen. Dit komt voort uit de gedragscode die regels bevat voor het gebruik van persoonsgegevens in relatie tot direct marketing met het oog op verkoop, financiering, ledenwerving en dergelijke. Deze code is uitgewerkt op initiatief van de Zweedse Direct Marketing Association (SWEDMA).[80]

4.5 Toezicht en handhaving

Toezichthouders
De Zweedse toezichthouder voor de bescherming van persoonsgegevens (*Datainspektionen,* DPA) is een overheidsinstantie met ongeveer 40 medewerkers, waarvan de meerderheid jurist is.[81] In 2014 bedroeg het budget 45 miljoen Zweedse kronen, wat ongeveer gelijk is aan 4,6 miljoen euro.[82] In 2014 adviseerde *Datainspektionen* over 117 wetsvoorstellen. De *Datainspektionen* is de toezichthoudende autoriteit voor bijna alle verwerking van persoonsgegevens. Op bepaalde gebieden die onder artikel 3 (2) van de EU-richtlijn vallen, is het toezicht aangescherpt door de oprichting van andere autoriteiten. Dit is het geval bij de Swedish Commission on Security and Integrity Protection, die onder andere de verwerking van persoonsgegevens door de Zweedse veiligheidsdienst controleert, en de Court of Foreign Intelligence en de Swedish Foreign Intelligence Inspectorate, die belast zijn met de taak om bescherming te bieden tegen inbreuken op persoonlijke integriteit met betrekking tot de werkzaamheden van de *Försvarets radioanstalt,* een regeringsagentschap in Zweden dat verantwoordelijk is voor het onderscheppen van radiosignalen.

80 David Törngren, Department of Constitutional Law, *Ministry of Justice Sweden,* Memorandum 23 april 2010, Questionnaire for Member States on the implementation of Directive 95/46/EC. Answer to question 15.
81 http://www.datainspektionen.se/.
82 Datainspektionens årsredovisning 2014 – Dnr 231-2015, p. 29.

Privacykwesties en de verwerking van persoonsgegevens worden ook indirect behandeld door de justitieombudsman, de parlementaire ombudsman, het rijksarchief, het Zweeds registratiebureau voor ondernemingen, de Zweedse financiële inspectie, en de dienst post en telecommunicatie (*Pos toch telestyrelsen*, PTS).[83] De PTS[84] is opgericht in 1992 en is een overheidsinstantie die toezicht houdt op elektronische communicatie en post in Zweden. De PTS zorgt ervoor dat de Wet electronische communicatie (LEK, 2003:389) wordt nageleefd. De PTS heeft vier overkoepelende doelen: het toewerken naar blijvende voordelen voor de consument, het creëren van duurzame mededinging op de lange termijn, het doeltreffend gebruiken van middelen en het streven naar veilige communicatie.[85]

Taken en bevoegdheden

De taak van de Zweedse toezichthouder voor de bescherming van persoonsgegevens (DPA) is het waarborgen van privacy van individuen in de informatiemaatschappij. De DPA ziet erop toe dat autoriteiten, bedrijven, organisaties en individuen de volgende wetten naleven:[86]

- de Wet persoonsgegevens/Personal Data Act (1998);
- de Datawet (1973);
- de Wet schuldsanering (1974); en
- de Wet kredietgegevens (1973).

De DPA treedt op om inbreuk op privacy te voorkomen door middel van het geven van informatie en het uitbrengen van richtlijnen en regelgevingscodes (*Svensk författssamling*, de officiële bekendmaking van nieuwe wetten). De DPA behandelt ook klachten en voert inspecties uit. Door de wetsvoorstellen van de overheid te onderzoeken zorgt de DPA ervoor dat nieuwe wetten en verordeningen persoonsgegevens op adequate wijze beschermen. In een memorandum worden de bevoegdheden van de Datainspektionen als volgt beschreven: "De DPA is de autoriteit die is opgericht overeenkomstig artikel 28 van de richtlijn."[87]

De bevoegdheden van de DPA zijn uiteengezet in de artikelen 43-47 van de Personal Data Act en zijn ongewijzigd gebleven sinds de uitvoering van de richtlijn. De DPA heeft het recht om toegang te vragen tot persoonsgegevens die worden verwerkt. Ook is de DPA gemachtigd om informatie en documentatie ten aanzien van de verwerking van persoonsgegevens en de gebruikte beveiligingsmaatregelen op te vragen en heeft

83 David Törngren, Department of Constitutional Law, *Ministry of Justice Sweden,* Memorandum 23 april 2010, Questionnaire for Member States on the implementation of Directive 95/46/EC. Answer to question 5.

84 http://www.pts.se/sv/Om-PTS/.

85 Library of Congress, Online Privacy catalogue www.loc.gov/law/help/online-privacy-law/sweden.php.

86 David Törngren, Department of Constitutional Law, *Ministry of Justice Sweden,* Memorandum 23 april 2010, Questionnaire for Member States on the implementation of Directive 95/46/EC. Answer to question 5.

87 David Törngren, Department of Constitutional Law, *Ministry of Justice Sweden,* Memorandum 23 april 2010, Questionnaire for Member States on the implementation of Directive 95/46/EC. Answer to question 5.

toegang tot faciliteiten die verband houden met de verwerking van persoonsgegevens. De DPA kan tevens voorschrijven welke beveiligingsmaatregelen de gegevensbeheerder moet toepassen in bepaalde gevallen.[88]
De PTS helpt de betrokkenen bij het uitoefenen van hun rechten door ervoor te zorgen dat marktpartijen de integriteitsregels van de Law on Electronic Communication (LEK) volgen.[89] De PTS bewerkstelligt dit door klachten te verwerken, inspecties uit te voeren en toezicht te houden om ervoor te zorgen dat aan bepaalde eisen wordt voldaan.[90] De meeste beslissingen van de PTS hebben betrekking op vrije concurrentie tussen internetleveranciers, prijsstelling en toegang tot internet, in plaats van veiligheid en privacy op het internet.[91]

Gebruik van bevoegdheden
Eenieder heeft de mogelijkheid om klachten in te dienen bij de DPA wanneer hij of zij de verwerking van zijn of haar persoonlijke gegevens betwist. De DPA zal – in zijn hoedanigheid van toezichthoudende autoriteit volgens de Personal Data Act – onafhankelijk beslissen of er een controle ten aanzien van de gegevensbeheerder uitgevoerd moet worden. Een memorandum uit 2010 beschrijft: "Het is lastig om een exact aantal te noemen als het gaat om het totale aantal controles dat de DPA heeft uitgevoerd op basis van klachten van betrokkenen. De DPA is onlangs begonnen met een taak die gericht is op het beter in kaart brengen van wat er met ingediende klachten van particulieren gebeurt."[92]
Het is voorgekomen dat een klager, dat wil zeggen de betrokkene, beroep heeft ingesteld tegen een vonnis van de DPA, bewerende dat een controle niet zou hebben plaatsgevonden. Een dergelijk beroep kan niet door een administratieve rechtbank herzien worden. Betrokkenen hebben ook wel eens beroep ingesteld tegen beslissingen ten aanzien van vrijstellingen van het verbod voor andere partijen dan overheidsinstanties om persoonsgegevens te verwerken betreffende wettelijke overtredingen van artikel 21 van de Personal Data Act. De rechtbanken hebben geoordeeld dat de klagers niet ontvankelijk zijn in dergelijke gevallen.[93]
In de eerste jaren na de implementatie van de richtlijn werd er een aantal Zweedse rechtszaken gehouden betreffende de doorgifte van persoonsgegevens naar derde landen, met name ten aanzien van de publicatie van persoonsgegevens op internet. Specifieke melding kan worden gemaakt van de *Ramsbro*-zaak (NJA 2001, s. 409) die betrekking heeft op de interpretatie van artikel 7 van de Personal Data Act (wat overeenkomt met artikel 9 van de richtlijn). De meest invloedrijke rechterlijke beslissingen zijn echter

88 http://uk.practicallaw.com/8-502-0348?service=ipandit.
89 LAGEN OM ELEKTRONISK KOMMUNIKATION [LEK] (SFS 2003:389), http://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2003389-om-elektronisk-kommunikation_sfs-2003-389.
90 http://www.pts.se/upload/Ovrigt/Internet/Plan-PTS-tillsyn-saker-konfidentiell-kommunikation.pdf.
91 See http://www.pts.se/.
92 David Törngren, Department of Constitutional Law, *Ministry of Justice Sweden,* Memorandum 23 april 2010, Questionnaire for Member States on the implementation of Directive 95/46/EC. Answer to question 8.
93 Memorandum 23 april 2010, Answer to question 9.

uitspraken van het Hof van Justitie van de Europese Unie, zoals de zaak *Lindqvist* (arrest van 6 november 2003 in zaak C-101/01) en de zaak *Satakunnan* (arrest van 16 december 2008 in zaak C73/07).[94]
Een recente uitspraak, in 2016, betreft een overtreding van de Personal Data Act in de gemeentelijke samenwerking Östra Östergötland in het informatiesysteem Aventus, waar persoonsgegevens buiten de doelstelling van de samenwerking om gebruikt werden. Een andere uitspraak heeft betrekking op een overtreding van de wet inzake gegevensgebruik voor sociale diensten door de thuiszorgorganisatie ParaGå (2001: 454).[95] Beide zaken betroffen ongeautoriseerd gebruik van persoonsgegevens.

Reputatie
Zweden (51%) behoort met Nederland (50%) tot de Europese landen waar meer dan de helft van de bevolking aangeeft dat ze op de hoogte zijn van de nationale overheidsinstantie die hun rechten betreffende persoonsgegevens beschermt.[96] In Zweden is dit percentage tussen 2010 en 2015 met 9 procentpunten gestegen, terwijl deze toename in Nederland 16 procentpunten was. Het Europese gemiddelde van 2015 ligt met 37% significant lager. Op de vraag waar ze klachten over de bescherming van persoonsgegevens zouden indienen, geeft 77% van de Zweden aan dat zij de klacht liever rechtstreeks indienen bij de autoriteit of onderneming die hun gegevens behandelt, 57% zou naar de Zweedse DPA gaan en 17% zou de DPA van het land waar de autoriteit of de particuliere onderneming gevestigd is benaderen. Slechts 2% noemt de EU-instellingen en -organen (laagste percentage, gedeeld met onder meer Duitsland en Ierland, in tegenstelling tot Nederland en Roemenië die 6% scoren en Frankrijk met 7%).[97] Zweden heeft het hoogste percentage respondenten dat van mening is dat de autoriteit of het bedrijf dat de gegevens verwerkt melding moet maken van datalekken: 91% (hoogste van de EU-landen, EU-gemiddelde 65%), slechts 31% stelt dat dit de taak van de DPA is (laagste van de EU-landen, EU-gemiddelde 45%).[98] Dit kan erop wijzen dat Zweden een sterke neiging hebben de verantwoordelijkheid voor gegevensbescherming naar bedrijven te schuiven.

94 Memorandum 23 april 2010, Answer to question 10.
95 http://www.datainspektionen.se/Documents/beslut/2016-02-18-paraga.pdf.
96 Eurobarometer 431 2015, p. 51.
97 Eurobarometer 431`2015, p. 56.
98 Eurobarometer 431 2015, p.76; de percentages betreffen de subgroep respondenten die eerder aangaven dat ze geïnformeerd wilden worden.

5. Verenigd Koninkrijk

5.1 Algemene situatie

In tegenstelling tot veel andere Europese landen, heeft het Verenigd Koninkrijk een *common law* rechtsstelsel, waarbij de nadruk ligt op gerechtelijke uitspraken. Het Verenigd Koninkrijk heeft drie rechtsstelsels voor Engeland en Wales, voor Noord-Ierland en voor Schotland. Veel materiële wetten gelden voor het gehele Verenigd Koninkrijk, maar er is niet één specifiek grondwettelijk document. De grondwet is gebaseerd op een aantal (veelal geschreven) bronnen, waaronder formele wetgeving (wetgeving van de wetgevende macht), common law (wetten door gerechtelijke uitspraken), parlementaire conventies en andere gezaghebbende werken (van de academische wereld).[1] De Britse grondwet bevat geen uitdrukkelijk recht op privacy. Het Verenigd Koninkrijk is sinds 1973 lid van de EU en is lid van het Europees Verdrag voor de Rechten van de Mens (EVRM). In 1998 heeft het Verenigd Koninkrijk de Human Rights Act aangenomen om de toepassing van het EVRM in de nationale wetgeving rechtstreeks mogelijk te maken. Deze mensenrechtenwet is twee jaar later, in 2000, van kracht geworden. Via de Human Rights Act is het mogelijk inbreuken op de grondrechten in het EVRM, waaronder het recht op privacy in artikel 8 EVRM, voor de Britse rechter te brengen.
Hoewel in 2016 een meerderheid van de Britse burgers in een referendum gestemd heeft voor het vertrek uit de Europese Unie, zal het Verenigd Koninkrijk zich blijven houden aan het Europees Verdrag voor de Rechten van de Mens en het daarin vermelde recht op privacy. Wanneer het Verenigd Koninkrijk de EU echter verlaat, is het niet verplicht zich te houden aan het Handvest van de grondrechten van de Europese Unie, waarvan de artikelen 7 en 8 betrekking hebben op het recht op privacy en de bescherming van persoonsgegevens. Ook zal de Algemene Verordening Gegevensbescherming (AVG) niet langer rechtstreeks van toepassing zijn in het Verenigd Koninkrijk na het verlaten van de EU.[2] Echter, sommige andere Europese landen die ook geen lid zijn van de EU (zoals IJsland, Liechtenstein en Noorwegen) houden zich wel aan de huidige EU-richtlijn 95/46/EC betreffende de bescherming van persoonsgegevens. Het Verenigd Koninkrijk kan er ook voor kiezen om zich te blijven houden aan de EU-regels inzake de bescherming van persoonsgegevens, bijvoorbeeld door gegevensoverdracht met

1 Blick, A., Blackburn, R. (2012), Mapping the Path to Codifying or not Codifying – the UK's Constitution, Series paper 2. Centre for Political and Constitutional Studies, King's College London.

2 http://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/Data-Protection/brexit_impact_on_gdpr_170616.

derde landen te waarborgen. Uiteraard blijven het EVRM en de Britse Human Rights Act nog steeds van toepassing na het verlaten van de EU.

Internetgebruik

Het internetgebruik in het Verenigd Koninkrijk is in de afgelopen jaren aanzienlijk gestegen, tot 78% in 2013.[3] De digitale kloof is kleiner geworden, aangezien het internet steeds toegankelijker is geworden voor mensen met lagere inkomens of opleiding en gepensioneerden en gehandicapten. 61% van de internetgebruikers is actief op sociale netwerken.[4] Uit onderzoek blijkt dat 96% van de Britse burgers online winkelt (EU-gemiddelde 87%), waarbij geldt dat online winkelen toeneemt met een stijgende leeftijd.[5] Britse burgers hebben een sterke voorkeur om hun online bestelling direct af te rekenen met een debet- of creditcard of via elektronisch geld.

De voor dit onderzoek geraadpleegde deskundigen geven aan dat het verzamelen en verwerken van persoonsgegevens door bedrijven of overheidsorganisaties mensen over het algemeen niet veel zorgen baart.[6] De heersende houding tegenover de controle van hun persoonsgegevens lijkt er een van onverschilligheid te zijn. Tevens zien Britten de verzameling en verwerking van hun gegevens in deze context als onvermijdelijk.[7] Burgers geven wel aan bezorgd te zijn wanneer ze hier naar worden gevraagd, maar lijken hier zelden iets aan te doen.[8] Uitzonderingen hierop zijn specifieke aan de overheid gerelateerde zaken zoals ID-kaarten, een nationaal kinderregister of een nationale gezondheidsdatabase.[9] Deskundigen wijzen er tevens op dat het onwaarschijnlijk is dat het grote publiek zich bewust is van de mate waarin gegevens daadwerkelijk worden verzameld, verwerkt, vergeleken of uitgewisseld tussen bedrijven en overheidsorganisaties, en de implicaties hiervan. Deze bevindingen overlappen grotendeels met gegevens uit recent onderzoek naar de publieke opinie rondom de bescherming van persoonsgegevens.[10]

3 Dutton, W.H., and G. Blank. 2013. Cultures of the Internet. The Internet in Britain, Oxford Internet Survey 2013. http://oxis.oii.ox.ac.uk/reports, p. 3.

4 Dutton, W.H., and G. Blank. 2013. Cultures of the Internet. The Internet in Britain, Oxford Internet Survey 2013. http://oxis.oii.ox.ac.uk/reports, p. 3.

5 Consent Country Report UK (2012) p. 3.

6 UK Expert Survey, p. 1.

7 UK Expert Survey, p. 1.

8 ICO-statistieken over verzoeken van burgers om de praktijken van gegevensbeheerders te beoordelen, bieden een aantal compenserende bewijzen voor deze houding. Zie ICO (ongedateerd), *Complaints and concerns data sets* [webpagina].
https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/. Het feit dat Britse burgers derde in de EU zijn op Googles lijst voor URL-verwijderingen, en dat bedrijven die aanzienlijke datalekken hebben gehad hierna veel klanten hebben verloren (bijvoorbeeld TalkTalk in 2015), geven aan dat burgers daadwerkelijk handelen wanneer hun persoonlijke gegevens in gevaar zijn.

9 UK Expert Survey, p. 1.

10 Eurobarometer 431 (2015).

(Gevoel van) controle

Volgens een recent onderzoek voelt ongeveer 50% van de Britten dat zij slechts gedeeltelijk controle hebben over de informatie die ze online verstrekken, terwijl 26% van de ondervraagden het gevoel heeft hier geen enkele controle over te hebben.[11] Verder geeft 18% aan een gevoel van volledige controle te hebben. Hiermee wijkt het Verenigd Koninkrijk niet ver af van het EU-gemiddelde met betrekking tot de gedeeltelijke controle (EU-gemiddelde 50%), scoort het net bovengemiddeld met volledige controle (EU-gemiddelde 15%) en onder het gemiddelde met geen enkele controle (EU-gemiddelde 31%). Over het algemeen lijken de Britse burgers zeer bezorgd te zijn over het gebrek aan controle. Ongeveer 80% van de mensen geeft aan zich hierover zorgen te maken, vergeleken met een EU-gemiddelde van 69%.

Het merendeel van de Britten (83%) beschouwt het online verstrekken van persoonsgegevens als een toenemend onderdeel van het moderne leven. Dit ligt boven het EU-gemiddelde (71%).[12] Binnen deze context geeft ongeveer 38% aan dat het verstrekken van persoonsgegevens geen groot punt is, terwijl 56% zich hier zorgen over maakt.[13] Gevraagd naar het gebruik van persoonsgegevens in ruil voor gratis diensten geeft 50% aan dit wel eens te doen.[14] Dit wordt ondersteund door de bevindingen van een ander onderzoek waarbij rond de 56% van de mensen aangaf liever voor een online dienst te betalen, dan deze toe te staan hun persoonlijke gegevens voor commerciële doeleinden te gebruiken.[15]

Bewustzijn

In vergelijking met de rest van de EU-vertonen de Britse burgers een laag niveau van bewustzijn als het gaat om het gebruik van persoonsgegevens door de eigenaren van websites.[16] Desondanks lijkt er een zeker evenwicht tussen bewustzijn en acceptatie te zijn. Hoewel bijvoorbeeld sprake is van een bovengemiddeld niveau van bewustzijn van het feit dat persoonsgegevens gebruikt worden om gebruikers per e-mail te contacteren, tonen Britten tegelijkertijd ook een bovengemiddeld niveau van acceptatie hiervoor. Hoewel de Britten een bewustzijnsniveau beneden het gemiddelde hebben ten opzichte van het delen van persoonlijke informatie met andere afdelingen binnen een bedrijf, het diepgaand vergaren van persoonsgegevens, het verkopen van persoonsgegevens of beschikbaar stellen van persoonsgegevens aan anderen zien zij dergelijke praktijken als bovengemiddeld onacceptabel. Commerciële afwegingen dragen hier niet aan bij. Daadwerkelijke ervaring met privacyinbreuken is relatief laag in het Verenigd Koninkrijk, met een score van 2,92 (EU-gemiddelde 2,89) op een 7-puntsschaal (1 = nooit, 7 = zeer vaak).[17]

Als het gaat om privacy policies, geven naar verhouding weinig Britten aan ooit een website niet gebruikt te hebben vanwege ontevredenheid met het privacybeleid van die

11 Eurobarometer 431 (2015), p. 10.
12 Eurobarometer 431 (2015), p. 29.
13 Eurobarometer 431 (2015), p. 32.
14 Eurobarometer 431 (2015), p. 40.
15 Vodafone Survey on Big Data (2016), p. 79.
16 Consent Country Report UK (2012) p. 4.
17 Consent Country Report UK (2012) p. 4.

website (40%, EU-gemiddelde 47%). Meer dan de helft geeft aan nooit of zelden de algemene voorwaarden (69%) of het privacybeleid (63%) van een website door te lezen.[18] Als het privacybeleid al gelezen wordt, lezen de Britten zelden de hele tekst (7%, EU-gemiddelde 11%). Desalniettemin geven ze aan redelijk vol vertrouwen te zijn de tekst – als ze deze lezen – grotendeels of helemaal te begrijpen (Nederland 59%, EU-gemiddelde 64%).

Vertrouwen

Wanneer er ingezoomd wordt op vertrouwen, ligt dat bij de Britten vrij hoog in vergelijking met het EU-gemiddelde. Dit geldt voor de meeste sectoren, zoals de gezondheidszorg (81%, EU-gemiddelde 74%), overheidsinstellingen (69%, EU-gemiddelde 66%), banken en financiële instellingen (70%, EU-gemiddelde 56%), winkels (46%, EU-gemiddelde 40%), telecom- en internetproviders (45%, EU-gemiddelde 33%) en online dienstverleners zoals zoekmachines (32%, EU-gemiddelde 24%). De enige uitzondering hierop vormen de Europese instellingen waarbij het gemiddelde met 44% beneden het EU-gemiddelde van 51% uitkomt.

Gevraagd naar de risico's verbonden aan het verstrekken van persoonsgegevens aan sociale media, schatten Britten deze relatief laag in. Dit geldt tevens voor specifieke risico's (informatie die gebruikt wordt voor het toesturen van ongewenste aanbiedingen of zonder toestemming van de gebruiker, bedreiging voor de persoonlijke veiligheid, het slachtoffer worden van fraude). Echter, gevraagd naar de risico's van discriminatie (UK 23%, EU-gemiddelde 23%) of schade aan de persoonlijke reputatie, ligt dit in lijn met het EU-gemiddelde.[19]

De houding van gegevensbeheerders ten opzichte van de bescherming van persoonsgegevens kan worden gezien als formalistisch, waarbij de nadruk ligt op compliance, in plaats van een toegewijde, holistische benadering.[20] Dit lijkt echter aangemoedigd te worden door hoe de regelgeving op dit gebied, de Data Protection Act (DPA) uit 1998, is ontworpen.[21] Rond 2009-2010 heeft de Britse toezichthouder (ICO) geprobeerd dit gedrag aan te pakken door Privacy Impact Assessments (PIA's) en een 'Privacy by Design'-benadering te stimuleren en zo de manier waarop persoonsgegevens verwerkt worden te verbeteren. PIA's worden nu gedaan door zowel bedrijven als overheidsorganisaties.[22] Er blijken echter grote verschillen te zijn in de aard van de individuele PIA's. Bovendien wordt het belangrijkste element ervan, namelijk dat de resultaten publiekelijk toegankelijk moeten zijn, zelden waargenomen. De ICO meldt dat er in sommige organisaties beperkte middelen zijn en een gebrek aan begrip met betrekking tot de bescherming van persoonsgegevens in het algemeen, en PIA's in het bijzonder.

Organisaties zien de bescherming van persoonsgegevens hoofdzakelijk als belangrijk in verband met financiële risico's en hun eigen reputatie. De ICO heeft recentelijk de

18 Consent Country Report UK (2012) p. 4.

19 Bij andere bronnen liggen deze aantallen iets hoger; zie: Consent Country Report UK (2012) p. 4.

20 UK Expert Survey, p. 2.

21 UK Expert Survey, p. 2.

22 Trilateral Research & Consulting (2013), *Privacy impact assessment and risk management Report for the Information Commissioner's Office*, 4 May 2013. https://ico.org.uk/media/1042196/trilateral-full-report.pdf.

bevoegdheid gekregen om geldboetes op leggen tot maximaal £ 500.000 in het geval van ernstige overtredingen van de bescherming van persoonsgegevens. Dit heeft vooral in de publieke sector een aantal opmerkelijke effecten gehad. In de private sector wordt de autoriteit van de ICO echter overschaduwd door de sancties die door andere toezichthouders kunnen worden opgelegd, met name in de financiële sector. Zo lijken bedrijven het niet naleven van de DPA 1998, en hier eventueel op betrapt te worden, te zien als een laag risico met relatief lage kosten.[23] Een veelgehoorde klacht van privacyfunctionarissen is het gebrek aan financiële middelen om hun taken uit te voeren.

Nationaal beleid

Op nationaal niveau zijn privacy en de bescherming van persoonsgegevens belangrijke onderwerpen in het parlementaire debat en deze krijgen extra aandacht wanneer nieuwe wetgeving wordt voorgelegd aan het parlement.[24] Bovendien houdt een aantal parlementaire commissies van beide kamers (House of Commons en House of Lords) zich bezig met privacyvraagstukken. Enkele voorbeelden van zulke commissies die direct of indirect belang hebben bij de bescherming van privacy en persoonsgegevens zijn:

- De Commissie Cultuur, Media en Sport (House of Commons) bewaakt het beleid, de administratie en de uitgaven van het ministerie van Cultuur, Media en Sport (dat verantwoordelijk is voor de bescherming van persoonsgegevens in het Verenigd Koninkrijk) en komt regelmatig bijeen om de kwesties op het vlak van privacy, beveiliging en de bescherming van persoonsgegevens te bespreken (evenals andere zaken binnen de portefeuille). Recent werd bijvoorbeeld een vraag over Cyber Security (de bescherming van persoonsgegevens online) besproken.[25] Deze commissie heeft ook de geschiktheid van de voorkeurskandidaat van de regering voor de post van Informatiecommissaris (hoofd van de toezichthouder ICO) beoordeeld.[26]
- Tot voor september 2015 lag de verantwoordelijkheid voor de bescherming van persoonsgegevens bij het ministerie van Justitie en het controleerde de commissie Justitie (House of Commons) en de EU Data Protection Framework Proposals.[27]
- De Commissie Wetenschap en Technologie (House of Lords) heeft onlangs bewijsvoering gehoord over 'autonome voertuigen' die ook privacyimplicaties met zich meebrengen.
- De Commissie Communicatie (House of Lords) heeft een onderzoek ingesteld naar de toegang tot en het gebruik van internet onder kinderen.
- Hoewel zij verschillende rollen hebben, beoordelen en controleren zowel de commissie Europese controle (House of Commons) en de subcommissies EU (House of Lords) de aanpak van de Britse regering en het belang van EU-wetgeving. De goedkeuring van het nieuwe EU Data Protection Framework heeft de gemoederen

23 UK Expert Survey, p. 3.
24 http://www.parliament.uk/topics/Privacy.htm.
25 http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/inquiries/parliament-2015/cyber-security-15-16/.
26 http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/inquiries/parliament-2015/information-commissioner-pre-appointment-15-16/.
27 http://www.parliament.uk/business/committees/committees-a-z/commons-select/justice-committee/inquiries/parliament-2010/eu-data-protection/.

in deze commissies flink beziggehouden. Verder zijn ze ook zeer alert op de implementatie van EU-wetgeving inzake grenscontroles (SIS II, VIS en EURODAC), douane (CIS) en samenwerking voor wetshandhavingsdoeleinden (EUROPOL).

Ook nodigen deze commissies regelmatig deskundigen uit de industrie, academici, vertegenwoordigers van civil society middenveld of regelgevende instanties en sectorverenigingen uit voor hun vergaderingen en hoorzittingen, vaak als onderdeel van een lopend onderzoek.
Het merendeel van de grotere politieke partijen is een gedeelde mening toegedaan over de rol die gegevens spelen bij de ontwikkeling van de economie en het verbeteren van levens en over de nodige veiligheidsmaatregelen die moeten worden toegepast op de verwerking van persoonsgegevens. Twee bronnen bevatten in het bijzonder veel informatie over de politieke standpunten in het Verenigd Koninkrijk:

- Het Big Brother Watch-manifest, dat in de aanloop naar de verkiezingen in 2015 werd gepubliceerd, is een analyse van de politieke partijprogramma's van 2010. Het manifest onderzoekt specifieke standpunten met betrekking tot burgerlijke vrijheden, waaronder de bescherming van persoonsgegevens.[28]
- In juli 2016 presenteerde de regering een nieuw wetsvoorstel voor de digitale economie aan het parlement.[29] Alvorens het wetsvoorstel aan het parlement voor te leggen, heeft de regering over bepaalde aspecten advies ingewonnen door middel van volksraadplegingen. Voor een van deze volksraadplegingen werd de publieke opinie over een beter gebruik van gegevens bij de overheid (*Better Use of Data in Government)* gepeild. Er werden meer dan 280 reacties ontvangen, onder andere van politieke partijen, met commentaar op het overheidsinitiatief omtrent 'data sharing'.[30]

Media-aandacht
De media tonen steeds meer interesse in verhalen over de bescherming van persoonsgegevens. Dit is tevens een goede afspiegeling van het groeiende bewustzijn onder het publiek op dit vlak. Vooral de kranten zijn erg opmerkzaam over alles wat wordt gezien als overheidssurveillance. Dit blijkt onder andere uit problemen rondom ID-kaarten en, meer recentelijk, het care.data-programma die voorpaginanieuws werden.[31]
Er is een debat gaande op het vlak van privacy en de bescherming van persoonsgegevens, maar dit is nogal eenzijdig: de liberale/linksgeoriënteerde media zijn, niet geheel verrassend, voor meer bescherming van persoonsgegevens, maar ook de rechtsgeoriënteerde, conservatieve media neigen naar meer bescherming van persoonsgegevens. Een voorstander van minder gegevensbeschermingsrechten voor consumenten ontbreekt.[32] De Britse Daily Mail publiceert de meeste verhalen over de bescherming van persoonsge-

28 https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/02/manifesto.pdf.
29 https://services.parliament.uk/bills/2016-17/digitaleconomy.html.
30 https://www.gov.uk/government/consultations/better-use-of-data-in-government.
31 "Het care.data-programma is opgericht door NHS England en het Informatiecentrum voor Gezondheid en Gezondheidszorg, om informatie van verschillende zorginstellingen, zoals huisartsenpraktijken, ziekenhuizen en zorgwoningen, op een veilige manier te bundelen om zo te kunnen zien wat er goed gaat bij de NHS en wat er juist beter kan." https://www.england.nhs.uk/ourwork/tsd/care-data/.
32 UK Expert Survey, p. 3.

gevens, terwijl The Guardian hier vaak over schrijft met betrekking tot nieuwe technologieën (bijvoorbeeld Twitter, Whatsapp, etc.). De BBC publiceert ook veel nieuwsverhalen op dit gebied, vooral online.
Er is over het algemeen veel begrip voor de rol van regulering en toezicht wordt over het algemeen serieus genomen. Het uitdelen van boetes heeft hier zeker aan bijgedragen. Deze boetes hebben veel media-aandacht gekregen en geholpen om meer mensen bekend te maken met het werk van de toezichthouders.[33] In het Verenigd Koninkrijk presenteert de toezichthouder (het *Information Commissioner's Office,* ICO, de Britse toezichthouder voor de bescherming van persoonsgegevens, zie paragraaf 5.5) jaarlijks publiekelijk zijn jaarverslag om de media de gelegenheid te bieden hierover te publiceren.[34]

Datalekken
Hoewel gegevensbeheerders niet wettelijk verplicht zijn datalekken die resulteren in het verlies, de openbaarmaking, vernietiging of corruptie van persoonsgegevens te melden, vindt het ICO dat serieuze datalekken wel gemeld moeten worden (en het staat ook open voor meldingen). In geval van een dergelijke melding zal het ICO de aard van het lek beoordelen en de mate waarin de gegevensbeheerder de Data Protection Act 1998 heeft nageleefd, alvorens te overwegen hoe het de handhavingsbevoegdheden zal gebruiken.[35]
Volgens ICO's jaarverslag 2015/16, is er in de gehele periode 2015/16 één incident binnen het ICO-bureau zelf geweest dat conform de eigen richtlijn omtrent zelfrapportage van incidenten met persoonsgegevens is gerapporteerd aan de handhavingsafdeling van het ICO.[36] Het incident betrof een kleine hoeveelheid persoonlijke informatie van vijf personen uit het ICO-klantenbestand dat per ongeluk werd gedeeld met een klant met dezelfde naam. Een deel van de informatie over een van de vijf personen betrof gevoelige persoonlijke informatie. Volgens het rapport is het incident op dezelfde manier onderzocht en behandeld als elk ander incident dat door een databeheerder aan het ICO gerapporteerd wordt. Er zijn enkele aanbevelingen gedaan om dit proces in de toekomst te verbeteren. Alle aanbevelingen zijn geaccepteerd en geïmplementeerd. Er zijn geen formele stappen ondernomen naar aanleiding van het incident.[37, 38]

Burgerrechtenorganisaties
Wanneer zaken de privacy en de bescherming van persoonsgegevens van burgers beïnvloeden, zorgen de commissies in het parlement ervoor dat de standpunten van

33 UK Expert Survey, p. 3
34 815 Data protection, p. 28.
35 Voor meer informative over hoe ICO datalekken handhaaft, zie ICO's Data Protection Regulatory Action Policy: https://ico.org.uk/media/about-the-ico/policies-and-procedures/1853/data-protection-regulatory-action-policy.pdf.
36 ICO's meest recente jaarverslag is hier terug te vinden: https://ico.org.uk/media/about-the-ico/documents/1624517/annual-report-2015-16.pdf.
37 ICO Annual Report 2015/16, p. 50.
38 Zie voor meer informatie over de door ICO genomen maatregelen n.a.v. datalekken: https://ico.org.uk/action-weve-taken/enforcement/.

burgerrechtenorganisaties naar behoren worden vertegenwoordigd. Het ICO heeft ook regelmatig overleg met belanghebbenden uit verschillende sectoren van de industrie, de lokale en centrale overheden en vertegenwoordigers van de civil society. De grootste burgerrechtenorganisaties zijn de Open Rights Group en de Foundation for Information Policy Research.
De twee burgerrechtenorganisaties die zich meer specifiek bezighouden met privacy en de bescherming van persoonsgegevens zijn Big Brother Watch en Privacy International. Big Brother Watch is opgericht in 2009 en doet onderzoek naar misbruik van bevoegdheden en produceert factsheets waarin complexe wetten en briefings uiteen worden gezet voor het parlement, de pers en het publiek.[39] De groep heeft door de jaren heen campagne gevoerd over een veelheid aan onderwerpen met betrekking tot online privacy, surveillance en burgerrechten in het algemeen.
Privacy International (PI) is een Londense non-profitorganisatie opgericht in 1990, die de wereldwijde bescherming van het recht op privacy wil bevorderen. Haar doelen zijn onder andere het pleiten voor sterke nationale, regionale en internationale wetten ter bescherming van privacy en bewustzijn creëren over technologieën en wetten die privacy in gevaar brengen, om ervoor te zorgen dat het publiek wordt geïnformeerd en betrokken is.[40] Volgens de jaarrekening van 2014-2015 had Privacy International in deze periode £ 1.398.207 aan inkomsten en £ 1.625.947 aan uitgaven.[41] PI wordt gefinancierd door liefdadigheidsfondsen, stichtingen en statutaire instanties. Om de onafhankelijkheid van haar activiteiten te kunnen waarborgen, accepteert zij geen donaties van bedrijven.
Burgerrechtenorganisaties deinzen er niet voor terug zeer kritisch te zijn op de overheid. Volgens de burgerrechtenorganisatie Privacy International kan het Verenigd Koninkrijk worden beschouwd als een endemische surveillancemaatschappij.[42] Volgens haar onderzoek heeft het Verenigd Koninkrijk de slechtste score op het gebied van de bescherming van de privacy van burgers van alle EU-lidstaten.

5.2 Beleid

Nationaal beleid, Privacy Impact Assessments

Experts uit het Verenigd Koninkrijk die zijn geraadpleegd voor dit onderzoek, beschrijven de houding van de Britse regering ten aanzien van de bescherming van persoonsgegevens als "voor verbetering vatbaar".[43] Hoewel de Britse overheid de bescherming van persoonsgegevens lijkt te zien als een noodzakelijk kwaad, zijn er desalniettemin de nodige maatregelen genomen om de wetgeving ten aanzien van de individuele rechten van burgers, de verplichtingen van gegevensbeheerders en ICO's

39 https://bigbrotherwatch.org.uk/about/.
40 https://privacyinternational.org/.
41 Audited Financial Statement 2014-2015, zie: https://privacyinternational.org/sites/default/files/Audited%20Financial%20Statement%202014-2015.pdf.
42 http://observatoriodeseguranca.org/files/phrcomp_sort.pdf.
43 UK Expert survey, pp. 3-4.

bevoegdheden in lijn te brengen met de Europese eisen. Dit lijkt echter wel te zijn beïnvloed door de volgende twee gebeurtenissen:

1. een formele kennisgeving van de Europese Commissie gericht aan de Britse overheid uit 2004 waarin de vermeende tekortkoming van de Britse uitvoering van de Europese richtlijn aan de kaak werd gesteld (de inhoud van de brief is niet bekend gemaakt door de overheid); en
2. een 'met redenen omkleed advies' van de Europese Commissie uit 2010 waarbij onder andere de beperkte bevoegdheden van het ICO, de restricties ten aanzien van het rectificeren of verwijderen van persoonsgegevens en limieten van de vergoeding van immateriële schade als gevolg van schending van de DPA 1998 becommentarieerd werden.[44]

In tegenstelling tot andere Europese landen staat de bescherming van persoonsgegevens in het Verenigd Koninkrijk los van individuele privacyrechten. In plaats daarvan wordt de bescherming van persoonsgegevens vooral gezien in een context van commerciële continuïteit, commerciële risico's en informatiebeveiliging. Deze aanpak is bijvoorbeeld terug te zien in de *Cyber Security Regulation and Incentives Review* gepubliceerd in december 2016.[45] Hoewel de Britse rechtbanken de relatie tussen de bescherming van persoonsgegevens en privacy hebben erkend, zijn achtereenvolgende regeringen huiverig geweest om deze relatie als zodanig formeel vast te leggen.[46]

Met name op het gebied van privacy en nationale veiligheid zijn er zorgen. Het Verenigd Koninkrijk maakt deel uit van de Five Eyes-samenwerking (een alliantie met Australië, Canada, Nieuw-Zeeland en de VS) die bekend staat om de grootschalige verzameling van gegevens en de surveillancemogelijkheden.[47] Gegevens worden onder andere verzameld door middel van grootschalig cameratoezicht in openbare ruimten. In 2011 was het aantal beveiligingscamera's in handen van de lokale overheden ronde de 52.000 in heel het Verenigd Koninkrijk.[48] Als alle beveiligingscamera's (dat wil zeggen: ook de camera's die niet in handen zijn van de overheid) meegeteld worden, telt het Verenigd Koninkrijk zo'n 1,85 miljoen camera's, wat neerkomt op een gemiddelde van 32 burgers per camera.[49] De meeste camera's, rond de 500.000, zijn geïnstalleerd in Londen en de gebieden daaromheen.

Onder de huidige Britse wetgeving zijn risicoanalyses en Privacy Impact Assessments (PIA's) niet verplicht. PIA's zijn echter wel een 'verplichte minimummaatregel' voor

---

44 EU Commission (2010), Data protection: Commission requests UK to strengthen powers of national data protection authority, as required by EU law [press release] (Brussels, 24 June). http://europa.eu/rapid/press-release_IP-10-811_en.htm?locale=en.

45 HM Government (2016), *Cyber Security Regulation and Incentives Review*, Department for Culture Media & Sport, December 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf.

46 UK Expert survey, p. 3.

47 Reuters (2013), British spy agency taps cables, shares with U.S. NSA – Guardian, Reuters, 21 June 2013.

48 Big Brother Watch (2012), 'The Price of Privacy. How local authorities spent £515m on CCTV in four years'. *Big Brother Watch*. February 2012. p. 30.

49 Onderzoek van The Guardian, 'You're being watched: there's one CCTV camera for every 32 people in UK', toont aan dat er 1,85m camera's zijn door heel Groot-Brittanie. De meeste zijn binnen geinstalleerd en privébezit. *The Guardian*, 2 March 2011.

de overheid en de bijbehorende agentschappen.[50] Het ICO heeft richtlijnen opgesteld over de opzet en uitvoering van PIA's.[51]
Een noemenswaardig overheidsinitiatief is het *midata*-programma. Dit is een initiatief dat het vrijgeven van consumentengegevens aan consumenten aanmoedigt, met als doel deze in een herbruikbare vorm terug te leveren aan de betreffende consument. Het idee hierachter is dat consumenten inzicht zouden moeten hebben in de gegevens die bedrijven over hen verzamelen tijdens transacties en zo gemakkelijker verschillende aanbiedingen kunnen vergelijken.[52] Het programma heeft betrekking op specifieke sectoren zoals energie, creditcards, mobiele telefonie en persoonlijke bankrekeningen. Het ICO is actief in haar berichtgeving over de privacyimplicaties van het programma. Een recente ontwikkeling voortvloeiend uit het *midata*-programmais bijvoorbeeld dat klanten nu een bestand van al hun financiële transacties kunnen downloaden bij hun bank en deze zo kunnen gebruiken om een geschikte lopende rekening uit te kiezen. Binnenkort is bij energieverleners hetzelfde mogelijk.[53]

Privacy en de bescherming van persoonsgegevens in nieuw beleid
Het ICO volgt de ontwikkelingen rondom big data nauwgezet. Zo heeft de regering in de begroting van 2014 een budget van £ 42 miljoen voor een periode van 5 jaar toegezegd voor het opzetten van het Alan Turing Institute. Samen met technologiebedrijf IBM financiert zij ook het Hartree Center. Dit centrum heeft de capaciteit om op grote schaal gegevens te verwerken en biedt deze dienst aan bedrijven aan. Er is ook een discussie gaande over de oprichting van een specifieke ethische commissie op dit vlak (*Council of Data Science Ethics*).[54] Ook overheidsgefinancierde onderzoeksraden ondersteunen big data-initiatieven, zoals bijvoorbeeld de steun van de ESRC (Economic and Social Research Council, een van de onderzoeksfinanciers van de Britse overheid) aan het Administrative Data Research Network. Er zijn ook voorbeelden te vinden van overheidssteun aan big data-initiatieven in de *Information economy strategy* van de vorige regering.[55] Het ministerie van Cultuur, Media en Sport, evenals het ICO, overleggen regelmatig met stakeholders en partnerorganisaties (waaronder ook internationale zusterorganisaties) en blijven zo op de hoogte van de laatste ontwikkelingen en de daaraan verbonden risico's.
Wat betreft Privacy by Design moedigt het ICO organisaties aan om vanaf het begin al na te denken over hun wettelijke verplichtingen volgens de DPA. Privacy Impact Assessments (PIA's) zijn een onmisbaar onderdeel van de Privacy by Design-aanpak.

50 Cabinet Office (2008), *Cross Government Actions: Mandatory Minimum Measures*, Sectie I, 4.4: All departments must "conduct privacy impact assessments so that they can be considered as part of the information risk aspects of Gateway Reviews". http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf.
51 ICO (2014), *Conducting privacy impact assessments code of practice*, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.
52 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/327845/bis-14-941-review-of-the-midata-voluntary-programme-revision-1.pdf.
53 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/united-kingdom#chapter-content12.
54 http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/992/992.pdf, paragraph 57.
55 https://www.gov.uk/government/publications/information-economy-strategy.

Er is een gedragscode gepubliceerd waarin de basisprincipes van een PIA worden beschreven en hoe deze kunnen worden toegepast om de privacyrisico's van organisaties te identificeren en te beperken. Verder heeft het ICO een richtlijn voor PIA's uitgebracht in 2014. Zij willen hiermee sectorale groepen die een PIA-methodologie willen ontwikkelen voor hun specifieke sector ondersteunen.

Maatschappelijk debat

Er is er momenteel een actief maatschappelijk debat over de bescherming van privacy en persoonsgegevens gaande waarvoor veel media-aandacht is (zie paragraaf 5.1). Verder maakt de Britse overheid gebruik van online opiniepeilingen om de mening van burgers en bedrijfsleven mee te kunnen nemen bij het ontwerpen van nieuw beleid rondom de bescherming van persoonsgegevens.[56] Een recent voorbeeld hiervan is een peiling naar het delen en het gebruiken van persoonsgegevens binnen de publieke sector[57] die in 2016 gedurende acht weken online toegankelijk was. Het doel hiervan was om een lijst met *good practices* samen te stellen om zo het delen van gegevens binnen instellingen te optimaliseren en tegelijkertijd de beveiliging van gegevens te verbeteren. De peiling heeft burgerrechtenorganisaties, privacygroepen, overheidsambtenaren, academici en vertegenwoordigers van de publieke sector ertoe gebracht om voorstellen van een aantal overheidsdiensten (zoals het ministerie voor Werk en pensioenen of het agentschap van rijbewijzen en voertuiglicenties) omtrent de uitwisseling van gegevens te heroverwegen en vervolgens aan te geven of zij deze passend vinden.[58] De raadpleging werd gezien als een volgende stap in een eenjarig open beleidsontwerpinitiatief dat de overheid in nauwe samenwerking met burgerrechtenorganisaties uitvoerde.[59] De resultaten hiervan werden gepubliceerd op een niet-gouvernementele website, www.datasharing.org.uk, die diende als overzicht van het lopende initiatief.[60]

Informatiecampagnes

De overheid heeft verschillende campagnes op het vlak van privacy en de bescherming van persoonsgegevens gevoerd:

- *Responsible for Information* is een door de overheid ontwikkelde cursus om werknemers en ondernemers te helpen om gegevensbeveiliging en risico's hieromtrent beter te kunnen begrijpen. Ook wordt er ingegaan op hun verantwoordelijkheden met betrekking tot de privacy van gegevens en bescherming tegen fraude en cybercriminaliteit.[61]
- *Cyber Aware* is een website met online tools en informatie om gedragsveranderingen van kleine bedrijven en particulieren te bevorderen zodat zij zich beter kunnen beschermen tegen cybercriminaliteit.[62] Dit is een initiatief van het UK Home Office.

56 https://www.gov.uk/government/publications?publication_filter_option=consultations.
57 https://www.gov.uk/government/news/launch-of-new-data-sharing-consultation.
58 https://www.gov.uk/government/news/launch-of-new-data-sharing-consultation.
59 https://www.gov.uk/government/news/launch-of-new-data-sharing-consultation; http://datasharing.org.uk/.
60 http://datasharing.org.uk/conclusions/index.html.
61 http://www.nationalarchives.gov.uk/sme/.
62 https://www.cyberaware.gov.uk/.

- *Get Safe Online* is een website met een praktische insteek over hoe mensen zichzelf en hun computers, mobiele telefoons en bedrijven kunnen beschermen tegen fraude, identiteitsdiefstal, virussen en andere online problemen. Het initiatief wordt ondersteund door de regering.[63]

Ook heeft het ICO materialen ontwikkeld voor scholen om het bewustzijn van kinderen en studenten over de waarde en het belang van hun persoonlijke gegevens te vergroten.[64] Verder heeft het ICO materialen ontwikkeld om organisaties en hun werknemers te stimuleren om na te denken over hun verantwoordelijkheden krachtens de Data Protection Act 1998.[65]

5.3 Wet- en regelgeving

Implementatie van de EU-richtlijn

De voornaamste wetgeving ter bescherming van persoonsgegevens in het Verenigd Koninkrijk is de Data Protection Act 1998 (DPA) die in 2000 van kracht werd en de EU-richtlijn 95/46/EC op nationaal niveau doorvoert. Verder implementeren de PECR-bepalingen (*Privacy and Electronic Communications Regulations,* PECR), geïntroduceerd in 2003 en gewijzigd in 2011, de eisen van de ePrivacy richtlijn 2002/58/EG. PECR reguleert direct marketing online, het gebruik van cookies en andere soortgelijke technologische middelen. Ook stelt PECR sectorspecifieke eisen aan aanbieders van telecommunicatiediensten met betrekking tot het melden van datalekken.[66]
De DPA 1998 heeft grotendeels de EU-richtlijn gevolgd. Het ICO heeft echter zelf het initiatief genomen om good practices uit andere rechtsgebieden te introduceren, zoals PIA's en Privacy by Design, die, alhoewel niet verplicht, verder gaan dan de in de EU-richtlijn voorziene maatregelen. Sinds de invoering is de DPA gewijzigd naar aanleiding van primaire en secundaire Britse wetgeving, met name de Vrijheid van informatiewet (Freedom of Information Act) 2000.[67]

Sectorale wetgeving

Voor de bescherming van persoonsgegevens is er specifieke wetgeving voor de financiële sector. Gereguleerde organisaties binnen de financiële sector hebben de aanvullende verplichting om hun bedrijfsactiviteiten te verrichten met 'gepaste vaardigheid, zorg en ijver' en 'er zorg voor te dragen [hun] zaken op een verantwoordelijke en effectieve manier te organiseren en te contoleren, met adequate risicomanagementsystemen'.

63 https://www.getsafeonline.org.
64 https://ico.org.uk/for-organisations/education/resources-for-schools/.
65 https://ico.org.uk/for-organisations/improve-your-practices/posters-stickers-and-e-learning/.
66 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/united-kingdom#chapter-content1.
67 Sinds 2002 zijn er 485 amendementen geweest volgens de officiële website over de Britse wetgeving http://www.legislation.gov.uk/.

Gegevensbeheerders in de financiële sector zijn verplicht deze sectorspecifieke wetgeving na te leven. Deze wetgeving functioneert in dit geval als aanvulling op de DPA.[68]
Uit verslagen uit 2010 blijkt dat de Europese Commissie een onderzoeksprocedure heeft ingesteld tegen het Verenigd Koninkrijk, vanwege vermeende tekortkoming bij het implementeren van 11 van de 34 bepalingen van de EU-richtlijn. Er werden veel tekortkomingen gerapporteerd.[69] Het Verenigd Koninkrijk heeft tevens kritiek ontvangen over het ontbreken van speciale wetgeving om de bescherming van werknemers te verbeteren.[70] Naar aanleiding hiervan heeft de toezichthouder voor de bescherming van persoonsgegevens, het ICO, richtlijnen afgegeven om werknemers meer bewust te maken van hun rechten en ze hulp te bieden indien ze bezwaar willen maken.[71]
De DPA verstaat onder 'gevoelige persoonlijke informatie' de standaardcategorieën (etniciteit, ras, politieke of religieuze overtuiging, vakbondslidmaatschap, gezondheid, seksuele oriëntatie), evenals informatie over (vermeende) gepleegde strafbare overtredingen of strafrechtelijke procedures. De categorieën zijn bewust breed gehouden. Als bijvoorbeeld iemand zijn been heeft gebroken, wordt dit gezien als gevoelige persoonlijke informatie, ondanks dat het relatief gemakkelijk is om deze informatie te achterhalen als diegene krukken gebruikt en zijn been in het gips zit.[72] Een relevant voorbeeld hiervan is de zaak *Murray v Big Pictures*, waarbij het hooggerechtshof oordeelde dat een foto gevoelige persoonlijke informatie kan zijn als deze de etnische afkomst van de personen in de foto laat zien.[73]
Gevoelige persoonlijke informatie mag worden verwerkt onder de standaardvoorwaarden[74] voor de verwerking van persoonsgegevens, mits daarnaast nog aan ten minste één van de andere eisen wordt voldaan. Deze andere eisen omvatten onder meer expliciete toestemming van het individu, het bewust publiek maken van de informatie door de betrokkene, de noodzaak om de gevoelige informatie te verwerken in verband met gerechtelijke procedures of het monitoren van gelijke kansen.[75] In de DPA en in een aanvullend bevel (*the Data Protection (Processing of Sensitive Personal Data) Order 2000*) zijn een aantal aanvullende voorwaarden opgenomen voor het verwerken van gevoelige persoonlijke informatie. Hierin wordt onder andere de verwerking van gegevens voor reglementaire inspecties, wetenschappelijk onderzoek of politieke activiteiten gereguleerd.[76]

---

68 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/united-kingdom#chapter-content1.
69 815 Data protection, p. 30.
70 815 Data protection, p. 37.
71 815 Data protection, p. 49.
72 ICO's Guide to Data Protection, p. 7.
73 Linklaters, p. 285.
74 Deze voorwaarden zijn vastgelegd in sectie 2 en 3 van de DPA, en verwijzen naar de toestemming van het individu, de noodzaak van de verwerking door een contractuele relatie of een wettelijke verplichting vanwege levensbelang of legitieme belangen, of voor het uitvoeren van rechtspraak. Zie voor meer informatie https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/#conditions-sensitive-data.
75 https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/#conditions-sensitive-data.
76 http://www.legislation.gov.uk/uksi/2000/417/contents/made.

De toestemming van de betrokkene moet ondubbelzinnig zijn ten opzichte van de gegevensverwerking. De toestemming dient derhalve gebaseerd te zijn op specifieke details over de verwerking, het doel, het informatietype en eventuele bijzondere aspecten die de toestemming zouden kunnen beïnvloeden, zoals eventuele openbaarmaking van de gegevens.

Zelfregulering en gedragscodes

In het Verenigd Koninkrijk is er een lange traditie van zelfregulering.[77] Zelfregulering door de industrie maakt zodoende een belangrijk onderdeel uit van de Britse regelgeving en wordt consequent gesteund door de overheid, zelfs toen dit principe onder druk kwam te staan vanwege vragen rondom de transparantie, publieke aansprakelijkheid en effectiviteit ervan.[78] Diverse zelfregulerende initiatieven zijn al in gebruik, bijvoorbeeld op het gebied van consumentengegevens. Sommige initiatieven staan beschreven in een rapport uit 2015 van de toezichthouder voor competitie en markt over het commercieel gebruik van consumentengegevens.[79] Deze betreffen voornamelijk initiatieven rondom online reclame en direct marketing en bestaan meestal uit een gedragscode of een aantal grondbeginselen, evenals praktische richtlijnen en diverse handhavingsmechanismen voor wanneer men zich niet aan de gedragscode houdt.[80]

Ook het ICO stimuleert en ondersteunt zelfregulering: organisaties worden aangemoedigd om zoveel mogelijk 'zelf te reguleren', bijvoorbeeld door sectorale gedragscodes op te stellen of standaarden vast te stellen voor het verzamelen en verwerken van persoonsgegevens. Het ICO twijfelt er niet aan dat zelfregulering door organisaties en zelfbescherming door goed geïnformeerde individuen steeds belangrijker worden voor een effectief gegevensbeschermingssysteem.[81]

Het ICO heeft zelf ook een reeks richtlijnen en praktische adviezen ontwikkeld om organisaties te helpen bij het implementeren van nieuwe projecten. Sommige hiervan zijn opgesteld in de vorm van een gedragscode die zaken als het delen van gegevens, privacyverklaring en het anonimiseren van gegevens beschrijft.[82]

77 Zie bijvoorbeeld zelfregulering van de pers in de voormalige *Press Complaints Commission* (PCC), nu de *Independent Press Standards Organisation* (IPSO); zelfregulering in de reclame bij de *Advertising Standards Authority*; en zelfregulering van direct marketing bij de *Direct Marketing Association & Commission*.

78 UK Expert survey, p. 5.

79 CMA (2015), *The commercial use of consumer data* (June 2015) at 69-73. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf.

80 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf, p. 71.

81 Zie o.a. ICO (ongedateerd), ICO's antwoord op een vraag van de Europese Commissie over de wetgeving inzake het fundamentele recht op bescherming van persoonsgegevens. http://ec.europa.eu/justice/news/consulting_public/0003/contributions/public_authorities/ico_uk_en.pdf.

82 https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/.

5.4 Implementatie

Sommige bedrijven hebben interne gedragscodes voor intern gegevensverkeer (zogeheten *binding corporate rules*) opgesteld met betrekking tot privacy en de bescherming van persoonsgegevens. Dit zijn echter meestal bedrijven die in meerdere jurisdicties actief zijn en derhalve aanvullende maatregelen moeten nemen om aan verschillende standaarden te voldoen.[83] Het ICO heeft een groot aantal richtlijnen gepubliceerd met betrekking tot privacy, de bescherming van persoonsgegevens en digitale communicatie. Deze publicaties worden regelmatig geactualiseerd in navolging van de laatste technologische en juridische ontwikkelingen.[84] Het ICO voert regelmatig online peilingen uit over conceptgedragscodes en publiceert vervolgens de feedback die hierover is ontvangen. Zo heeft het ICO bijvoorbeeld een peiling over privacyverklaringen gehouden.[85] De ontvangen feedback werd in een rapport op de website gepubliceerd.[86]

Privacyfunctionarissen

Net als in veel andere EU-landen is het voor veel organisaties onder de Britse wetgeving inzake de bescherming van persoonsgegevens niet verplicht om een privacyfunctionaris aan te stellen. In de praktijk blijkt echter dat veel grotere organisaties dit wel doen.[87] Bij overheidsorganisaties worden de werkzaamheden van de privacyfunctionaris vaak gecombineerd met die van een 'vrijheid van informatie'-functionaris (vergelijkbaar met de Wob-functionaris in Nederland, die gaat over de naleving van de Wet openbaarheid van bestuur, Wob).[88]

De aangewezen privacyfunctionaris heeft veelal een achtergrond in gegevensbeheer, IT of gegevensbeveiliging. De privacyfunctionaris mag deel uitmaken van meerdere afdelingen binnen een organisatie. Doordat de wet zich oorspronkelijk beperkte tot persoonsgegevens die bewaard worden op een computer, waren privacyfunctionarissen destijds voornamelijk werkzaam op IT-afdelingen, maar tegenwoordig is dit alles veel complexer geworden en houden ze zich ook bezig met het beheer van documenten en juridische zaken, hetgeen meerdere afdelingen aangaat.[89] Hun taken variëren van het beantwoorden van vragen en verzoeken afkomstig van personen, het ICO, de financiële toezichthouder (*Financial Conduct Authority, FCA*) of de bedrijfseconomische toezichthouder (*Prudential Regulatory Authority, PRA*) tot het ontwikkelen van intern beveiligingsbeleid en bijbehorende procedures, het opleiden van personeel, het adviseren over de naleving van wetgeving op dit gebied, het recenseren van en adviseren over nieuwe

83 Chapter 8, Empirical Findings, United Kingdom, p. 149.

84 Een volledige lijst met ICO-richtlijnen is te vinden op: https://ico.org.uk/for-organisations/guidance-index/data-protection-and-privacy-and-electronic-communications/.

85 https://ico.org.uk/about-the-ico/consultations/privacy-notices-transparency-and-control-a-code-of-practice-on-communicating-privacy-information-to-individuals.

86 https://ico.org.uk/media/about-the-ico/consultations/1625139/ico-privacy-notices-code-of-practice-consultation-summary-20161006.pdf.

87 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/united-kingdom#chapter-content6.

88 UK Expert Survey, p. 6.

89 UK Expert Survey, p. 6.

producten of procedures, het identificeren van risico's en het adviseren over juridische ontwikkelingen die belangrijk kunnen zijn voor de betreffende organisatie.[90] Eenmaal benoemd, hoeft een privacyfunctionaris niet geregistreerd te worden bij de toezichthouders voor de bescherming van persoonsgegevens, maar kan deze wel als contactpersoon voor het ICO worden aangewezen.

Beveiligingsmaatregelen

Privacy by Design is geen vereiste van de toezichthouder,[91] maar wordt door het ICO wel aangemoedigd. Het ICO pleit voor meer aandacht voor privacyafwegingen in project- en risicomanagement, zowel in uitvoering als beleid.[92] In deze context heeft het ICO een gedragscode ontwikkeld voor het uitvoeren van Privacy Impact Assessments (PIA's).[93] De gedragscode gaat in op hoe PIA's effectief kunnen worden gebruikt en bevat bijlagen die kunnen dienen als basis voor een eigen PIA. Deze bevatten onder andere vragen en sjablonen die makkelijk digitaal bewerkt kunnen worden. Het ICO heeft tevens een rapport laten opstellen over het gebruik van PIA's en het potentieel om deze verder te integreren in project- en risicomanagementinstrumenten.[94]

Het ICO verplicht organisaties die persoonsgegevens verwerken om passende technische en organisatorische maatregelen te nemen tegen verlies, vernietiging, schade of enige andere vorm van onwettige verwerking van persoonsgegevens. De beveiliging moet passend zijn gezien de aard van de gegevens (gevoelige persoonsinformatie vereist een hoger beveiligingsniveau) en het potentiële risico op persoonlijk schade (en de ernst hiervan) in het geval er een datalek ontstaat.[95] Specifieke normen zijn in dit verband echter niet in de wet of in bindende richtlijnen vastgelegd. Desalniettemin verwacht het ICO wel dat organisaties interne controles uitvoeren, met inbegrip van een passend gegevensbeschermingsbeleid, gegevensbeschermingsprocedures, toegangscontroles, personeelstraining en technische controles. Dit omvat ook het gebruik van beveiligde apparatuur, encryptie en de veilige verwijdering van software en hardware.[96]

De Data Protection Act (DPA) bevat geen specifieke verplichtingen met betrekking tot het melden van datalekken. Het ICO heeft hier echter wel richtlijnen voor opgesteld en verwacht geïnformeerd te worden indien er ernstige datalekken optreden.[97] Nalatigheid in het melden van ernstige datalekken wordt meegenomen in het vaststellen van

90 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/united-kingdom#chapter-content6.

91 De DPA 1998 vereist dat "passende technische en organisatorische maatregelen worden genomen tegen ongeoorloofde of onrechtmatige verwerking van persoonsgegevens, en tegen verlies, vernietiging of schade aan persoonsgegevens." Er wordt ingegaan op wat er 'passend' wordt geacht in welke context. Het wordt echter vaak geïnterpreteerd als maatregelen die voldoen aan de huidige standaarden van de sector. Zie ook UK Expert survey, p. 6.

92 https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/.

93 https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

94 https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/.

95 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/united-kingdom#chapter-content12.

96 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/united-kingdom#chapter-content12.

97 Linklaters, p. 286.

een passende geldboete. Daarnaast wordt er van organisaties verwacht dat zij betrokkenen over de eventuele risico's zullen informeren, vooral wanneer betrokkenen zelf actie kunnen ondernemen om (verdere) schade te voorkomen.[98] Verplichting tot kennisgeving van datalekken is opgenomen in de PECR-bepalingen (die EU-richtlijn 2009/136/EG inzake gebruikersrechten omtrent elektronische communicatienetwerken en -diensten implementeren) en geldt bovendien voor gegevensbeheerders in de financiële sector die de financiële toezichthouder (*Financial Conduct Authority*) op de hoogte moeten stellen van datalekken.[99]
Het ICO ontwikkelt momenteel een certificaat voor het beschermen van privacy (*privacy seal certification*). Organisaties die het certificaat hebben ontvangen, kunnen dit gebruiken om aan de buitenwereld te laten zien dat ze voldoen aan de meest recente voorwaarden voor het verwerken van persoonsgegevens. Dit zal fungeren als een keurmerk. Het ICO werkt samen met de Britse *Accreditation Service* en andere belanghebbenden om criteria vast te stellen voor de selectie van uitvoeringsorganisaties tot wie instanties zich kunnen wenden voor certificering.[100]

Transparantie
De experts die zijn ondervraagd ten behoeve van dit onderzoek geven aan dat de huidige ideeën over transparantie uiteenlopen, waardoor het lastig is om een algemene conclusie te trekken.[101] De enigszins uiteenlopende uitkomsten van een aantal officiële verslagen bevestigen deze verklaring tot op zekere hoogte.
Het merendeel van de Britten geeft aan nooit of zelden daadwerkelijk het privacybeleid (63%, EU-gemiddelde 54%) te lezen.[102] Als het privacybeleid al gelezen wordt, lezen zij zelden de hele tekst (6%, EU-gemiddelde 11%). Ondanks deze lage aantallen zijn de Britten redelijk vol vertrouwen de tekst – indien ze deze wel lezen – grotendeels of helemaal te begrijpen (58%, EU-gemiddelde 64%).
Tegelijkertijd suggereert een onderzoek van het ICO dat privacy policies niet voldoende begrepen worden. Uit hun focusgroepenonderzoek bleek dat het bewustzijn omtrent privacyverklaringen zelfs extreem beperkt is.[103] In het beste geval konden de respondenten termen herkennen, maar slechts een klein aantal kon uitleggen wat deze termen betekenen en hoe die hen en hun gegevens beschermen.
Bovendien blijkt uit een rapport uit 2015, getiteld *The commercial use of consumer data,* opgesteld door de competitie- en markttoezichthouder (*Competition and Markets Authority*), dat de consument het gevoel heeft dat privacy policies niet doen wat zij moeten doen, namelijk het vergroten van begrip en het waarborgen van een eerlijke

98 UK Expert survey, p. 7.
99 Linklaters, p. 286.
100 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/united-kingdom#chapter-content12.
101 UK Expert survey, p. 7.
102 Consent Country Report UK (2012), p. 36.
103 ICO (2015), *Data protection rights. What the public want and what the public want from Data Protection Authorities.*

verzameling van persoonsgegevens.[104] Respondenten hebben de indruk dat dit soort beleid, vol met ingewikkeld juridische jargon, is ontworpen om bedrijven te dienen in plaats van consumenten. Volgens hen is de macht over het verzamelen en het gebruik van persoonsgegevens van de consument naar bedrijven verschoven.[105] In hetzelfde rapport komt ook de houding aan bod van private organisaties ten opzichte van het verzamelen van informatie terwijl gebruikers zich hier niet bewust van zijn door de verandering van het zogenoemde 'vrijwillig geven van informatie' (gegeven door een vakje aan te kruisen of een formulier in te vullen) naar 'passieve' dataverzameling (door het gebruik van cookies).[106] Naar aanleiding hiervan hebben overheidsgroepen gepleit voor ICO's betrokkenheid bij het versimpelen van de inhoud van privacyvoorwaarden en privacy policies, en hebben zij de overheid gevraagd om actieve betrokkenheid van de burgers gedurende het hele proces te faciliteren.[107]

5.5 Toezicht en handhaving

Toezichthouders

Het Informatiecommissariaat (ofwel *Information Commissioner's Office,* ICO, de Britse toezichthouder voor de bescherming van persoonsgegevens) controleert en handhaaft de DPA en PECR in het Verenigd Koninkrijk. De commissaris wordt benoemd door de koningin. Het ICO is een onafhankelijk lichaam en rapporteert direct aan het Britse parlement. De huidige Informatiecommissaris is Elizabeth Denham, benoemd in juli 2016. ICO's hoofdkantoor is gevestigd in Londen, maar er zijn ook kantoren in Schotland, Wales en Noord-Ierland. Het budget voor 2015/16 was ruim 23 miljoen pond, waarvan meer dan 18 miljoen afkomstig was van gelden die in rekening werden gebracht bij de meldplicht. Deze gelden vloeien rechtstreeks in het budget van het ICO.[108] Het ICO telt momenteel 442 medewerkers waarvan er 409 full-time in dienst zijn.[109] Gegevensbeheerders binnen de financiële dienstensector vallen tevens onder het toezicht van de bedrijfseconomische toezichthouder (*Prudential Regulatory Authority, PRA*) en de financiële toezichthouder (*Financial Conduct Authority, FCA*)

Taken en bevoegdheden

Het ICO stimuleert openheid door overheidsinstanties en bescherming van persoonsgegevens voor particulieren. Zij tracht organisaties en burgers bewust te maken van de bescherming van persoonsgegevens en relevante wetgeving op dit gebied. Zoals hierna

104 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf, p. 170.

105 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf, pp.104-105.

106 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf, p. 169.

107 http://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf, p. 22.

108 Gegevensbeschermingsactiviteiten in het Verenigd Koninkrijk worden bijna geheel gefinancierd door de opbrengst van boetes opgelegd aan gegevensbeheerders die verzuimen hun verwerking van persoonsgegevens te melden (wat wel verplicht is volgens de DPA).

109 https://ico.org.uk/about-the-ico/our-information/key-facts/.

beschreven, kan het ICO ook specifieke maatregelen nemen om deze wetgeving af te dwingen. In het jaarverslag 2015/16 heeft ICO de volgende doelstellingen als hoofdprioriteiten voor de komende jaren geïdentificeerd:

- het ondersteunen van organisaties om hun verplichtingen inzake informatierechten beter te begrijpen;
- het passend aanwenden van handhavingsbevoegdheden om een betere naleving van informatierechten te waarborgen;
- burgers een evenredig, eerlijk en efficiënt antwoord geven op hun vragen rondom informatierechten;
- personen in staat stellen hun informatierechten te gebruiken;
- alert zijn op veranderingen die informatierechten beïnvloeden.[110]

Het ICO heeft een aantal instrumenten ter beschikking om het gedrag van gegevensbeheerders te kunnen beïnvloeden. Hieronder vallen niet alleen civiele en administratieve handhavingsmaatregelen, maar ook strafrechtelijke vervolging. De maatregelen sluiten elkaar niet uit en worden regelmatig gecombineerd.[111] Het ICO heeft de bevoegdheid om informatie en documentatie bij organisaties op te vragen op het terrein van de bescherming van persoonsgegevens.[112] Verder kan het ICO op verzoek van gegevensbeheerders audits uitvoeren. Ook is het ICO bevoegd om verplichte audits te doen om te kunnen controleren of de betrokken organisatie gegevens op de juiste manier verwerkt.[113] De uitkomsten van deze audits worden via een beschikking gecommuniceerd.[114]
Het ICO kan organisaties tevens een openbare kennisgeving geven en daarmee bedrijven verzoeken een specifieke maatregel te nemen om zo te voldoen aan de gegevensbeschermingsregels. Hoewel deze kennisgevingen juridisch niet bindend zijn, is het niet opvolgen ervan niet bevorderlijk voor de reputatie van de organisatie.[115] Bovendien geldt dit als schulderkenning indien er later datalekken optreden. Deze methode wordt regelmatig toegepast.[116]
De ICO-commissaris kan verder een waarschuwing tot handhaving of een 'stop nu'-bevel geven wanneer er een datalek heeft plaatsgevonden. Hiermee vereist het ICO dat organisaties specifieke stappen (niet meer) ondernemen om zo persoonsgegevens te beschermen.[117] Het niet naleven van deze waarschuwingen of bevelen is een strafbaar feit, strafbaar met (onbeperkte) boetes, maar niet met een gevangenisstraf. Aangezien het ICO geen strafrechtelijke bevoegdheden heeft, moet de feitelijke vervolging van een strafbaar feit voor de Britse strafrechter worden gebracht. Hiervoor werkt het ICO samen met het Britse Openbaar Ministerie (*Crown Prosecution Service)*.
Het ICO heeft de bevoegdheid om geldboetes van maximaal £ 500.000 op te leggen in het geval er een ernstig datalek of schending van de bescherming van persoonsgegevens

110 ICO Annual Report 2015/16, p. 13.
111 https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/.
112 815 Data protection EN, p. 21.
113 https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/.
114 http://search.ico.org.uk/ico/search/decisionnotice.
115 Linklaters, p. 287.
116 https://ico.org.uk/action-weve-taken/enforcement/.
117 https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/.

is geweest dat opzettelijk of door roekeloosheid heeft plaatsgevonden en waarschijnlijk ernstige schade of leed zal veroorzaken.[118] In 2015 werden enkele wetwijzigingen doorgevoerd om het gemakkelijker te maken om een geldboete op te leggen voor schending van de regels voor direct marketing via e-mail, telefoon of fax. Het ICO kan nu schendingen van de bescherming van persoonsgegevens beboeten zonder aan te hoeven tonen dat deze ernstige schade of leed zullen veroorzaken.[119]
Bovendien ondersteunt het ICO, hoewel hij niet direct beslist over de gegrondheid van een klacht, burgers bij hun inspanningen om kwesties rondom de bescherming van persoonsgegevens bij de verantwoordelijke organisaties aan te kaarten. De rol van het ICO is om mensen te helpen om beter te begrijpen hoe zij het best met de organisatie kunnen interacteren om het betreffende probleem op te lossen. Hij biedt checklists en informatie met stappen die in dit proces overwogen kunnen worden. Het ICO deelt dergelijke kwesties in op de volgende zes categorieën: overlast door telefoontjes of berichten, zoekresultaten op het internet, toegang tot of hergebruik van informatie, cookies, de behandeling van persoonsgegevens en klachten over het ICO zelf.[120] Zodra een burger de betreffende organisatie heeft gecontacteerd en deze niet in staat is of niet bereid is om de kwestie aan te pakken, verwacht het ICO dat de betrokkene de uitkomst bij het ICO zal melden. Het ICO gebruikt deze informatie om te beslissen of de kwestie een kans biedt om de bescherming van persoonsgegevens te verbeteren. Als dit het geval is, neemt het ICO de maatregelen zoals hiervoor beschreven.[121]
Het ICO wordt niet stelselmatig geraadpleegd door de wetgever bij het opstellen van wetgeving die privacy en de bescherming van persoonsgegevens kan beïnvloeden. De wetgever is niet verplicht om dit te doen.[122]

Gebruik van bevoegdheden
In het jaarverslag van 2015/16 is terug te vinden dat het ICO een toename heeft gezien van het aantal kwesties rondom de bescherming van persoonsgegevens. Ruim 16.300 zaken werden er in deze periode behandeld, waarvan het ICO er 15.700 heeft opgelost waarvan meer dan 90% binnen drie maanden. In de meeste gevallen heeft het ICO maatregelen opgesteld die de betreffende organisaties geacht wordt te nemen.[123] Ook het aantal klachten over de toegang tot informatie van overheidsinstanties is toegenomen. In dezelfde periode heeft het ICO meer dan 5.100 klachten geregistreerd waarvan er 5.068 zijn afgehandeld. Meer dan 70% van de gevallen is binnen drie maanden afgehandeld en bij 90% hiervan is er binnen zes maanden een beslissing genomen. Het ICO heeft verder nog 1.376 beschikkingen afgegeven. Er zijn 275 beroepen ingediend bij het *Information Tribunal*, waarvan in 80% van de gevallen de beslissing van ICO onderschreven werd.[124]

118 Linklaters, p. 287.
119 Linklaters, p. 287.
120 https://ico.org.uk/concerns/.
121 https://ico.org.uk/for-the-public/raising-concerns/.
122 815 Data protection, p. 42.
123 ICO Annual Report 2015/16, p. 18.
124 ICO Annual Report 2015/16, p. 18.

De ICO-hulplijn heeft in de periode 2015/16 in totaal 204.700 gesprekken ontvangen, hetgeen vergelijkbaar is met de voorgaande jaren. De helft van de geregistreerde oproepen kwam van burgers. 80% van de oproepen had betrekking op de bescherming van persoonsgegevens, 15% ging over PECR en 4% ging over kwesties omtrent de vrijheid van informatie. Het ICO heeft zelf een onderzoek uitgevoerd naar de klanttevredenheid met de hulplijn. Gevraagd naar hoe behulpzaam de hulplijn was, vond 95% van de bellers deze behulpzaam tot zeer behulpzaam. Negen van de tien gesprekken werden al tijdens het eerste telefoontje afgehandeld.[125]

Reputatie

Het ICO geeft jaarlijks opdracht tot enquêtes en rapporten over hun klanttevredenheid. De resultaten worden vervolgens op de website geplaatst.[126] Dit geeft inzicht in het niveau van bewustzijn van burgers over hun rechten, en van de instellingen die zijn aangewezen om deze te beschermen.

Uit de statistieken van 2016 (*Annual Track statistics*),[127] die tegelijk met een jaarlijks rapport (*Annual Track report*) en een klantevredenheidverslag (*Customer Satisfaction report*)[128] uitgebracht worden, blijkt dat een grote meerderheid van de Britten de DPA 1998 kent. 97% van de Britten heeft er wel eens van gehoord en 75% is er (in meer of mindere mate) bekend mee. Veel minder mensen zijn echter bekend met hun rechten onder de DPA en het bestaan van het ICO in het algemeen. Slechts 35% heeft evan gehoord, terwijl slechts 5% daadwerkelijk weet heeft van wat het ICO doet. Meer informatie over hoe men over het ICO denkt, is verkrijgbaar uit de *ICO stakeholder perception studies* uitgevoerd in 2008[129] en 2012.[130] Deze studies gaan dieper in op de relaties die verschillende doelgroepen met het ICO hebben ontwikkeld en behandelen tevens de ervaringen van zowel organisaties als individuen. De doelgroepen van beide studies zijn overheidsinstellingen, bedrijven, academici of belanghebbenden die hiervoor uitgenodigd zijn (studie 2012).[131] Burgers zijn in beide gevallen niet ondervraagd. Van het onderzoek uit 2012 is het niet bekend wie de 'uitgenodigde belanghebbenden' zijn. Van de kwesties die uit de studie uit 2008 naar voren kwamen, waren 'de snelheid van het aanpakken van een probleem' en 'de consistentie van het advies van het ICO' het meest problematisch.[132] Uit de studie uit 2012 blijkt dat men wil dat het ICO zijn handhavingsactiviteiten meer openbaar maakt.[133]

125 ICO Annual Report 2015/16, p. 18.
126 ICO (ongedateerd), *Information rights research* [webpage], https://ico.org.uk/about-the-ico/our-information/research-and-reports/information-rights-research/.
127 https://ico.org.uk/media/about-the-ico/documents/1624382/ico-annual-track-2016.pptx.
128 ICO (ongedateerd), *Information rights research* [webpage], https://ico.org.uk/about-the-ico/our-information/research-and-reports/information-rights-research/.
129 Jigsaw Research (2008), *ICO Stakeholder Perceptions Study* (May 2008), https://ico.org.uk/media/1042339/ico-stakeholder-perception-study-research-report.pdf.
130 Ipsos MORI (2012), *Stakeholder Perceptions 2012. Prepared for the ICO* (March 2012). https://ico.org.uk/media/about-the-ico/documents/1042371/stakeholder-perceptions-2012.pdf.
131 UK Expert survey, p. 8.
132 https://ico.org.uk/media/1042339/ico-stakeholder-perception-study-research-report.pdf, p. 5.
133 https://ico.org.uk/media/about-the-ico/documents/1042371/stakeholder-perceptions-2012.pdf, p. 2.

Het ICO heeft een goede reputatie onder gegevensbeheerders omdat hij over het algemeen bereid is hen tegemoet te komen in het vinden van oplossingen.[134] Het feit dat het ICO tot voor kort beperkte handhavingsbevoegdheden had, heeft hier wellicht aan bijgedragen. Sinds 2010 is het mandaat van het ICO uitgebreid en heeft hij een grotere bevoegdheid om boetes uit te delen.[135] De ondervraagde bedrijven vinden de regels rondom boetes van het ICO transparant en makkelijk te begrijpen.[136] Het opleggen van geldboetes aan gegevensbeheerders is echter nog steeds een laatste redmiddel voor het ICO. Het ICO lijkt, indien mogelijk, de voorkeur te geven aan het treffen van een schikking.[137]

134 UK Expert survey, p. 8.
135 Chapter 8, Empirical Findings – United Kingdom, p. 155.
136 Chapter 8, Empirical Findings – United Kingdom, p. 155.
137 UK Expert survey, p. 9.

6. Ierland

6.1 Algemene situatie

Ierland heeft een *common law*-rechtsstelsel met een geschreven grondwet. Het rechtsstelsel is tot op zekere hoogte te vergelijken met dat van het Verenigd Koninkrijk, met name door de historische banden tussen de twee landen. De Ierse grondwet bevat een hoofdstuk met grondrechten, inclusief bepalingen betreffende het huisrecht (artikel 40.5), het familieleven (artikel 41.1) en individuele rechten (artikel 40.3). Een recht op eerbiediging van het privéleven wordt niet specifiek genoemd, maar de rechtbanken erkennen dat de individuele rechten in de grondwet het recht op privacy als zodanig impliceren.[1]

Ierland is een ondertekenaar van de Universele Verklaring van de Rechten van de Mens (*Universal Declaration of Human Rights, UDHR*) en heeft het Internationaal Verdrag inzake burgerrechten en politieke rechten (*International Covenant on Civil and Political Rights, ICCPR*) geratificeerd. Beide zijn juridische instrumenten die een recht op privacy bevatten. Ierland is sinds 1973 lid van de EU en ondersteunt het Europees Verdrag voor de Rechten van de Mens (*European Convention on Human Rights, ECHR*), dat in de nationale wetgeving is verwerkt. Als het gaat om zaken die binnen het EU-recht vallen, is Ierland gebonden aan het Handvest van de grondrechten van de Europese Unie (*Charter of Fundamental Rights of the European Union*), waarin het recht op privacy en de bescherming van persoonsgegevens beschreven worden in artikel 7 en 8. Bovendien heeft Ierland het verdrag van de Raad van Europa geratificeerd voor de bescherming van individuen met betrekking tot de automatische verwerking van persoonsgegevens (Council of Europe Convention 108, ook wel het Verdrag van Straatsburg genoemd).

Met het oog op problemen op het vlak van privacy en de bescherming van persoonsgegevens is het vermeldenswaardig dat de Europese hoofdkantoren van verschillende grote technologiebedrijven, zoals Google, Facebook, Apple, Adobe, Airbnb en LinkedIn, in Ierland gevestigd zijn. De lage belastingtarieven en milde standaarden ten aanzien van de bescherming van persoonsgegevens[2] in combinatie met de aanwezigheid van een jonge, goed opgeleide, Engels sprekende beroepsbevolking kunnen hieraan hebben bijgedragen.[3] Eventuele geschillen tussen Europeanen en deze bedrijven beginnen

1 *McGee/Attorney General*, (1974), IR 284; *Kennedy and Arnold/Attorney General*, (1987), IR 587.

2 http://thesovereigninvestor.com/asset-protection/ireland-sets-big-tech-internet-privacy-policies/.

3 https://www.quora.com/Why-have-Google-and-Facebook-chosen-Dublin-for-their-European-headquarters. Zie ook https://qz.com/124133/the-reason-american-tech-firms-like-ireland-isnt-just-the-low-taxes/.

gewoonlijk in Ierland. In de afgelopen jaren werden er enkele interessante zaken in Ierse rechtbanken gehouden tegen deze technologiebedrijven. Het meest opmerkelijke in dit opzicht was een uitspraak van het Europese Hof van Justitie (HvJ EU) in 2015 in de *Schrems*-zaak, waarin de zogenaamde Safe Harbor-beschikking (een overeenkomst tussen de EU en de VS over een vrijwillige gedragscode die werd beschouwd als voldoende bescherming voor de overdracht van persoonsgegevens van de EU naar de VS) ongeldig werd verklaard.[4] Deze zaak werd in 2011 in Ierland gestart door de Oostenrijkse privacyactivist Max Schrems. Een andere opmerkelijke uitspraak was de uitspraak van het HvJ EU in 2014 die de EU-Dataretentierichtlijn (EU-richtlijn 2006/24/EG) ongeldig verklaarde.[5] Deze zaak werd gestart door Digital Rights Ireland, een Ierse burgerrechtenorganisatie, tegen de Ierse autoriteiten.

Internetgebruik

Ierland heeft een bevolking van 4,7 miljoen inwoners, waarvan in 2015 naar schatting 85% toegang had tot internet thuis.[6] De Ieren lijken goed overweg te kunnen met online diensten. 66% van de Ierse bevolking (EU-gemiddelde 57%) maakt minimaal één keer per week gebruik van online sociale netwerken.[7] Ook wordt er veel gebruikgemaakt van online bankieren (59% gebruikt online bankieren eens per week).[8] Verder blijkt dat een groot deel van de Ierse bevolking gebruikmaakt van online (video) bellen (43%, EU-gemiddelde 27%) en regelmatig iets via internet bestelt (23%, EU-gemiddelde 17%). Ook scoren de Ieren hoog wat betreft het gebruik van peer-to-peer-software of websites om films of muziek uit te wisselen (24%, EU-gemiddelde 18%).[9] Ierse internetgebruikers zijn doorgaans geïnteresseerd in netwerken (29%, EU-gemiddelde 31%) en wereldwijd-webgebruik (13%, EU-gemiddelde 15%).[10]

(Gevoel van) controle

Ongeveer 52% van de Ieren heeft het gevoel gedeeltelijk in eigen hand te hebben welke informatie ze online delen, 26% van de ondervraagden heeft het gevoel hier totaal geen controle over te hebben en 20% heeft juist het gevoel van absolute controle.[11] Deze cijfers lijken erop te wijzen dat er in Ierland een bovengemiddeld aantal mensen het gevoel heeft van gedeeltelijke controle (EU-gemiddelde 50%) of totale controle (EU-gemiddelde 15%) en juist een lager dan gemiddeld aantal mensen het gevoel heeft helemaal geen controle te hebben (EU-gemiddelde 31%). De Ieren lijken zich over het algemeen veel zorgen te maken over het gebrek aan controle wat betreft online privacy. Rond de 83% van de mensen geeft aan bezorgd te zijn, tegenover een EU-gemiddelde van 69%. Over het algemeen lijken de Ieren nogal bezorgd te zijn over het gebrek aan

4 CJEU 6 October 2015, case C-362/14, *Facebook/Schrems*, ECLI:EU:C: 2015:650.
5 Zaak C-293/12. Court of Justice of the European Union. 8 April 2014.
6 http://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2015/.
7 Eurobarometer 431 (2015), p. 109.
8 Eurobarometer 431 (2015), p. 110.
9 Eurobarometer 431 (2015), p. 113.
10 Consent Country Report Ireland (2012), p. 3.
11 Eurobarometer 431 (2015), p. 10.

complete controle. Ongeveer 79% van de mensen geeft aan zich zorgen te maken, in vergelijking met een EU-gemiddelde van 67%.
Onder de Ierse bevolking beschouwt 81% het verstrekken van persoonsgegevens als een steeds groter onderdeel van het moderne leven, hetgeen duidelijk hoger ligt dan het EU-gemiddelde van 71%.[12] In dit verband geeft ongeveer 44% aan dat het verstrekken van persoonsgegevens geen groot probleem is, terwijl 49% zich hier wel zorgen over maakt.[13] Op de vraag of men het erg vindt om persoonlijke informatie te verstrekken in ruil voor gratis online diensten, geeft 46% van de Ieren aan dit inderdaad een probleem te vinden.[14] Deze bevinding wordt bevestigd door een andere recente enquête, waarbij ongeveer 52% van de respondenten aangeeft dat zij liever voor een online dienst betalen dan toestemming verlenen aan de leverancier voor het gebruiken van hun persoonlijke gegevens voor commerciële doeleinden.[15]

Bewustzijn
In vergelijking met de rest van EU lijken de Ieren zich over het algemeen niet erg bewust te zijn van het gebruik van hun persoonlijke informatie door website-eigenaren.[16] Als het echter aankomt op de details ligt het percentage Ieren dat niet gediend is van het gebruik van hun persoonlijke informatie voor doeleinden als het afstemmen van website-inhoud en advertenties net iets hoger dan gemiddeld. Nog minder gediend zijn de Ieren van het gebruik van hun persoonlijke gegevens voor e-mailcontact, het verzamelen van deze gegevens of het doorverkopen of beschikbaar maken van deze gegevens aan derden. Dit soort praktijken wordt over het algemeen gezien als onacceptabel. Commerciële afwegingen op dit gebied worden evenmin geaccepteerd. De Ieren wijken hiermee nauwelijks af van het EU-gemiddelde (Ierland 73%, EU-gemiddelde 74%).[17] Het gevoel dat er daadwerkelijk een inbreuk op de privacy plaatsvindt, is in Ierland gemiddeld laag. De Ieren scoren 2,63 (totaal in steekproef 2,89) op een zevenpuntsschaal (1 = nooit, 7 = regelmatig).[18]
Er zijn relatief weinig mensen in Ierland (37%, EU-gemiddelde 47%) die zich er ooit van hebben laten weerhouden een website te gebruiken wegens hun ontevredenheid over het privacybeleid van die website. Meer dan de helft van de Ieren leest zelden of nooit de voorwaarden of het privacybeleid van een website (beide 70%).[19] Als de Ieren het privacybeleid wel doorlezen, dan lezen zij net als andere EU-burgers zelden de hele tekst (Ierland 6%, EU-gemiddelde 11%). Desondanks is er een hoge mate van vertrouwen dat zij de tekst – als ze deze doorlezen – grotendeels of volledig begrijpen (54%, EU-gemiddelde 64%).[20]

12 Eurobarometer 431 (2015), p. 29.
13 Eurobarometer 431 (2015), p. 32.
14 Eurobarometer 431 (2015), p. 40.
15 Vodafone Survey on Big Data (2016), p.79.
16 Consent Country Report Ireland (2012) p. 4.
17 Consent Country Report Ireland (2012) p. 33.
18 Consent Country Report Ireland (2012) p. 4.
19 Consent Country Report Ireland (2012) p. 4.
20 Consent Country Report Ireland (2012) p. 4.

Vertrouwen

Wat betreft de mate van vertrouwen valt het op dat de Ieren grotendeels overeenkomen met de rest van de EU als het gaat om sectoren als de gezondheidszorg (73%, EU-gemiddelde 74%) en banken en financiële instellingen (59%, EU-gemiddelde 56%). Deze percentages liggen echter aanmerkelijk hoger dan het EU-gemiddelde wanneer men kijkt naar vertrouwen in overheidsinstellingen (72%, EU-gemiddelde 66%), vertrouwen in winkels (54%, EU-gemiddelde 40%) en vertrouwen in telecom- en internetproviders (48%, EU-gemiddelde 33%). Dezelfde tendens is zichtbaar als het gaat om vertrouwen in online bedrijven zoals zoekmachines (39%, EU-gemiddelde 24%). Gevraagd naar de algemene risico's verbonden aan het verstrekken van persoonsgegevens op sociale media, lijkt de Ierse bevolking in het algemeen iets minder risico te zien dan de doorsnee EU-burger. In dit opzicht scoren ze lager dan het totale gemiddelde wanneer het gaat om specifieke risico's (zoals het in gevaar brengen van persoonlijke veiligheid of informatie die gebruikt wordt voor het ongewenst toesturen van commerciële aanbiedingen of zonder toestemming van de gebruiker). Er zijn echter ook vlakken waarop de Ieren hoger scoren dan de gemiddelde EU-burger. Zo ervaren ze een hoger risico met betrekking tot de waarschijnlijkheid of het risico om slachtoffer te worden van fraude (34%, EU-gemiddelde 32%) of discriminatie (28%, EU-gemiddelde 23%) en het risico op reputatieschade (29%, EU-gemiddelde 25%).[21]

Beschermingsmaatregelen

Het aantal Ieren dat ooit heeft geprobeerd privacyinstellingen op hun socialemediaprofielen aan te passen is 62% (EU-gemiddelde 57%).[22] Een totaal van 81% (EU-gemiddelde 64%) vindt het makkelijk om de genoemde veranderingen te maken.[23] Mensen die de privacyinstellingen niet wijzigen, geven aan erop te vertrouwen dat de website gepaste instellingen hanteert (29%), niet te weten hoe de instellingen aangepast kunnen worden (23%), zich geen zorgen te maken over hun online persoonsgegevens (14%), geen tijd te hebben om naar de opties te kijken (19%) of er niet van op de hoogte te zijn dat de instellingen veranderd kunnen worden (15%).[24] Uit een ander onderzoek blijkt dat Ieren vaak of altijd de privacyinstellingen van hun persoonlijk profiel op sociale media aanpassen, hetgeen met 62% boven het EU-gemiddelde van 54% ligt. Van de mensen die hun privacyinstellingen aanpassen, maakt 84% (in vergelijking met het EU-gemiddelde van 80%) deze instellingen strikter, zodat anderen minder informatie over hen te zien krijgen.[25]

Op het niveau van specifieke technische maatregelen om persoonlijke internetbeveiliging te handhaven of te verbeteren, worden alle maatregelen (zoals het blokkeren van pop-ups, het aanvinken van opt-in- en opt-outopties, het controleren op spyware, het verwijderen van de zoekgeschiedenis en het blokkeren van bepaalde e-mailadressen) gebruikt. Deze cijfers liggen duidelijk boven het EU-gemiddelde.[26] Ondanks het feit

21 Consent Country Report Ireland (2012), p. 4.
22 Eurobarometer 431 (2015), p. 92.
23 Eurobarometer 431 (2015), p. 95.
24 Eurobarometer 431 (2015), p. 98.
25 Consent Country Report Ireland (2012), p. 4.
26 Consent Country Report Ireland (2012), p. 3.

dat er doorgaans een gebrek aan informatie over de meest recente activiteiten van socialemediawebsites is, lijkt de mate van bekwaamheid inzake bovenstaande technische maatregelen toch te wijzen op een bepaald niveau van internetervaring.[27]

Nationale politiek

Bescherming van persoonsgegevens is vrijwel nooit onderwerp van debat in het nationale parlement. Het delen van gegevens tussen overheidsinstanties is wel eens ter discussie gesteld, maar niet met betrekking tot de bescherming van persoonsgegevens.[28] De discussie die plaatsvond in verband met de *Cyberbullying Bill* in 2013[29] was iets uitgebreider, maar deze en andere soortgelijke maatregelen[30] zijn niet geslaagd.[31] De Fianna Fáil partij had het wetsvoorstel aangedragen en leiders van andere partijen, zoals de Fine Gael[32] partij en de Labour Party[33], hebben alternatieve regelingen voorgesteld om cyberpesten te bestrijden.

Geen van de vier grootste partijen (gebaseerd op het aantal zetels) – waaronder Fine Gael,[34] Fianna Fáil,[35] Sinn Féin,[36] en de Labour Party[37] – zien de bescherming van persoonsgegevens als een vooraanstaand beleidsprobleem. In plaats daarvan wordt de focus gelegd op algemene onderwerpen, zoals gezondheid, huisvesting, banen en kinderopvang.[38] Dit gezegd hebbende, heeft Fianna Fáil vele persberichten over bescherming van persoonsgegevens uitgebracht[39] en het manifest van de Labour Party bevat een toezegging tot het hanteren van een streng beleid omtrent de bescherming van persoonsgegevens wanneer er gegevens tussen overheidsinstanties worden gedeeld.[40]

---

27 Consent Country Report Ireland (2012), p. 39.

28 "Deputy Terence Flanagan asked the Minister for Public Expenditure and Reform Information on Brendan Howlin Zoom on Brendan Howlin if there are service level agreements between Government Departments regarding the sharing of data, for example, between the the Revenue Commissioners and the Department of Social Protection; and if he will make a statement on the matter." http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/(indexlookupdail)/20131120~WRO?opendocument#WRO00800.

29 http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/(indexlookupdail)/20131106~W?opendocument#W03000.

30 http://www.independent.ie/irish-news/politics/labour-brings-two-separate-bills-targeting-online-bullying-31149776.html.

31 Een van de meest recente initiatieven is een rapport van de Law Reform Commission met bijbehorend wetsontwerp. http://www.irishexaminer.com/ireland/new-laws-to-combat-online-abuse-such-as-cyberbullying-and-revenge-porn-422963.html.

32 https://www.thejournal.ie/cyber-bullying-ireland-1162881-Nov2013/.

33 http://www.independent.ie/irish-news/politics/labour-brings-two-separate-bills-targeting-online-bullying-31149776.html.

34 https://www.finegael.ie/our-priorities/.

35 https://www.fiannafail.ie/the-issues/.

36 http://www.sinnfein.ie/policies.

37 https://www.labour.ie/manifesto/.

38 Zie vorige voetnoten voor de primaire beleidsvraagstukken van elke partij.

39 https://www.fiannafail.ie/?s=data+protection.

40 Labour Party Manifesto, p. 101, available at https://www.labour.ie/download/pdf/labour_manifesto_2016.pdf.

Naast het jaarlijks verhogen van het budget van de commissaris voor gegevensbescherming (*Data Protection Commissioner*)[41] en het *Government Data Forum*-initiatief afkomstig van het ministerie van de *Taoiseach* (de premier)[42] lijken er geen direct beleid, initiatieven of informatiecampagnes door de overheid gelanceerd te zijn die zich specifiek richten op de problemen omtrent de bescherming van persoonsgegevens. Het lijkt er dus op dat zelfregulering grotendeels de voorkeur krijgt ten opzichte van regelgeving.

Media-aandacht

In de regel is er uitgebreide media-aandacht voor privacy en de bescherming van persoonsgegevens, met name in de afgelopen drie jaar. Dit is te herleiden tot de Snowden-openbaringen en de beslissingen van het HvJ EU omtrent de rechtszaken *Digital Rights Ireland* en *Schrems*.[43] De media hebben aandacht besteed aan een verscheidenheid aan problemen, waaronder Snowden en internationaal toezicht, nationaal toezicht, de Schrems-zaak, Safe Harbor en Privacy Shield, Ierland als data hub, de effectiviteit van de Data Protection Commissioner, de procesvoering van Microsoft Ierland, de bescherming van persoonsgegevens (van zowel kinderen als volwassenen), de impact van de 'Google Spanje'-zaak en de komende Algemene Verordening Gegevensbescherming (AVG, in het Engels *General Data Protection Regulation*) van de EU.[44] Er heeft een groot debat plaatsgevonden over de omstreden kwesties. Niet alleen in de kranten, maar ook op televisie en in radioprogramma's is er regelmatig en veel aandacht aan besteed.[45] Over het geheel genomen, zijn de media voorstander van meer rechten op het vlak van privacy en de bescherming van persoonsgegevens.[46]

---

41 https://www.dataprotection.ie/docs/13-10-2016-Data-Protection-Commissioner-welcomes-Budget-2017-increase-in-funding/1601.htm.

42 http://www.taoiseach.gov.ie/eng/publications/publications_2015/government_data_forum.html. Binnen het departement van Taoiseach is er een afdeling Data Protection, maar het is niet duidelijk wat de verantwoordelijkheden zijn. De website heeft alleen links naar de notulen van de vergaderingen van het Forum voor Overheidsgegevens. Zie http://www.taoiseach.gov.ie/DOT/eng/Work_Of_The_Department/Data_Protection_Division/Data_Protection_Division.html.

43 Expert survey, p. 1.

44 Expert survey, p. 2-5. Expert survey v. 2, p. 2-4.

45 Expert survey, p. 1-2. Expert survey v. 2, p. 2 and 5.

46 Expert survey, p. 1. Zie bijvoorbeeld T. J. McIntyre, 'Why Ireland Must Protect Privacy of Irish Emails and Internet Usage from Surveillance', *The Irish Times*, 20 December 2014, http://www.irishtimes.com/opinion/why-ireland-must-protect-privacy-of-irish-emails-and-internet-usage-from-surveillance-1.2044384; T.J. McIntyre, 'The State Must Be More Mindful of Your Private Data', *Independent.ie*, 21 August 2014, http://www.independent.ie/opinion/the-state-must-be-more-mindful-of-your-private-data-30524449.html; T.J. McIntyre, 'Europe Has Failed in Duty to Protect Citizens over Web Privacy Threat', *Independent.ie*, 7 October 2015, http://www.independent.ie/opinion/comment/europe-has-failed-in-duty-to-protect-citizens-over-web-privacy-threat-31589481.html; Karlin Lillington, 'Strong Data Protection Laws Better for EU than Sniping', *The Irish Times*, 23 April 2015, http://www.irishtimes.com/business/technology/strong-data-protection-laws-better-for-eu-than-sniping-1.2185370; Adrian Weckler, 'Safe Harbour Is Gone but Europe Is Still Afraid to Tackle the US on Privacy', *Independent.ie*, 8 October 2015, http://www.independent.ie/business/technology/safe-harbour-is-gone-but-europe-is-still-afraid-to-tackle-the-us-on-privacy-31591450.html; en 'Data Office Still Underfunded despite €1m Boost in Budget', *Independent.ie*, 21 October 2015, http://www.independent.ie/business/technology/news/data-office-still-underfunded-despite-1m-boost-in-budget-34126722.html.

Datalekken

Er hebben meerdere significante datalekken en privacyschendingen omtrent de bescherming van persoonsgegevens plaatsgevonden. Naast internationale datalekken, zoals bij de websites Ashley Madison en Yahoo waarvan Ierse gebruikers het slachtoffer werden, zijn er ook aanzienlijke binnenlandse datalekken geweest. Het bekendste voorbeeld stamt uit 2013, toen promotiebedrijf LoyaltyBuild een datalek had waardoor de persoonsgegevens van ongeveer 1,5 miljoen mensen uit heel Europa, waaronder 90.000 Ierse gebruikers, werden gecompromitteerd.[47] LLoyaltyBuild had in 2013 een winst van 1 miljoen euro geboekt. Na de bovengenoemde overtreding heeft het bedrijf echter in het opvolgende jaar een verlies van 18 miljoen euro gerapporteerd en 500.000 euro geïnvesteerd in nieuwe beveiligingssystemen.[48]

Andere grootschalige datalekken vonden plaats bij de gevestigde gasleverancier Bord Gáis (in 2009 verloor het 75.000 bankgegevens van klanten),[49] Bank of Ireland (31.000 klantenverzekeringen en hypotheekgegevens in 2008)[50] en bookmaker Paddy Power (649.000 klantengegevens verloren, waaronder 120.000 klanten in Ierland).[51] Ook op kleinere schaal zijn er talrijke datalekken geweest[52] en in een recent onderzoek heeft meer dan de helft van de deelnemende bedrijven aangegeven dat ze het afgelopen jaar in een of andere vorm met datalekken te maken hebben gehad.[53] Het lekken van data heeft slechts tot enkele rechtszaken geleid,[54] maar dit blijft een domein dat onderhevig is aan ontwikkeling.[55] Deze incidenten hebben niet geleid tot georganiseerde protesten, maar burgers hebben wel hun zorgen geuit over de bescherming van persoonsgegevens

47 Elaine Edwards, 'Loyaltybuild Reopens for Business after Huge Data Breach', *The Irish Times*, 12 March 2014, http://www.irishtimes.com/news/consumer/loyaltybuild-reopens-for-business-after-huge-data-breach-1.1722266.

48 Gordon Deegan, 'Cyber attack victim firm Loyaltybuild in Clare has €18m loss', *Irish Examiner*, 2 February 2016, http://www.irishexaminer.com/business/cyber-attack-victim-firm-loyaltybuild-in-clare-has-18m-loss-379472.html.

49 Paul Cullen, 'Bord Gáis Failed to Say Stolen Laptop Data Not Encrypted', *The Irish Times*, 19 June 2009, http://www.irishtimes.com/news/bord-g%C3%A1is-failed-to-say-stolen-laptop-data-not-encrypted-1.787045.

50 Edel Kennedy, 'Victims of BoI Laptop Theft Treble to 31,500', Independent.ie, 29 April 2008, http://www.independent.ie/irish-news/victims-of-boi-laptop-theft-treble-to-31500-26442003.html.

51 John Mulligan, 'Massive Data Breach at Paddy Power Bookmakers', *Independent.ie*, 31 July 2014, http://www.independent.ie/business/irish/massive-data-breach-at-paddy-power-bookmakers-30474614.html.

52 Bijvoorbeeld Elaine Edwards, 'Civil Service Payroll System to Be Audited Following Data Breach', *The Irish Times*, 20 June 2016, http://www.irishtimes.com/news/ireland/irish-news/civil-service-payroll-system-to-be-audited-following-data-breach-1.2691360.

53 Expert survey, p. 6.

54 *Collins v FBD Insurance Plc*, IEHC 137 (14 March 2013), beschikbaar via http://www.bailii.org/cgi-bin/format.cgi?doc=/ie/cases/IEHC/2013/H137.html&query=(fbd). In deze zaak werd een schadevergoeding toegekend van €15,000 in relatie tot bescherming van persoonsgegevens. Echter, de schadevergoeding werd teruggedraaid door het hooggerechtshof. *Mc Keogh v John Doe 1 & Ors* [2012] IEHC 95 (26 January 2012), beschikbaar via http://www.bailii.org/cgi-bin/for-mat.cgi?doc=/ie/cases/IEHC/2012/H95.html&query=(mc)+AND+(keogh). Deze zaak werd geschikt.

55 Expert survey v2, p. 4.

en problemen omtrent het bewaren van gegevens en hebben zich ingezet om deze kwesties prioriteit te geven in de openbare discussie.[56]

Burgerrechtenorganisaties

In Ierland zijn er weinig mensenrechtenorganisaties actief op het gebied van databescherming. Twee van de meer vooraanstaande organisaties zijn Digital Rights Ireland en The Irish Council for Civil Liberties. Digital Rights Ireland bestaat uit vrijwilligers en beschikte over een budget van 51.762 euro in 2014 en 124.888 euro in 2015.[57] De organisatie heeft geprocedeerd over zaken als databescherming en tegen de toezichthouder DPC.[58] Ook is zij voor een commissie verschenen over online pesten en neemt zij deel aan informatiecampagnes of organiseert deze zelf.[59] Digital Rights Ireland wordt ook in het Government Data Forum vertegenwoordigd via de voorzitter, dr. TJ McIntyre,[60] maar het is niet duidelijk in hoeverre deze vergaderingen invloed hebben op het overheidsbeleid dat hierna nader wordt besproken.

Hoewel digitale problemen niet de voornaamste focus van de onafhankelijke, niet-gouvernementele Irish Council for Civil Liberties zijn, creëren ze wel publieke bewustwording ten aanzien van gegevensbeschermingsvraagstukken. De Irish Council for Civil Liberties heeft onlangs een symposium over dit onderwerp georganiseerd.[61] Digital Rights Ireland is in de eerste plaats bekend op dit gebied door bijdragen aan radio, drukwerk en online publicaties.[62] Ook de zaak die zij bepleitten en wonnen voor het HvJ EU[63] kreeg aanzienlijke aandacht van de pers.

6.2 Beleid

Nationaal beleid, Privacy Impact Assessments

De regering van Ierland lijkt geen algemeen of sectoraal beleid te hebben omtrent de bescherming van persoonsgegevens. Beleid ten aanzien van wanneer Privacy Impact Assessments (PIA's) plaats moeten vinden, wordt gedelegeerd aan de toezichthouder, de Data Protection Commissioner (DPC). De DPC heeft gewezen op het belang van PIA's en risicoanalyses in grootschalige overheidsgegevensprojecten.[64] De verwachting is dat beide instrumenten gebruikt worden voor technologieën die impact hebben op privacy, zoals camera's die op het lichaam gedragen worden door de politie[65] of het

56 Expert survey v2, p. 5. Zie ook Expert survey, p. 7.
57 Digital Rights Ireland Limited, Income and Expenditure Account for the year ended 31 December 2015.
58 These cases are mentioned in more detail below.
59 https://www.digitalrights.ie/about/.
60 http://www.taoiseach.gov.ie/eng/Work_Of_The_Department/EU_Division/Membership_of_the_Government_Data_Forum.html.
61 http://www.iccl.ie/articles/surveillance--democracy-privacy-rights-in-the-digital-age-symposium-.html.
62 https://www.digitalrights.ie/about/.
63 http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=196677.
64 Annual Report of the Data Protection Commissioner of Ireland, p. 3, zie https://www.dataprotection.ie/docimages/documents/DPC%20AR2015_FINAL-WEB.pdf.
65 Annual Report of the Data Protection Commissioner of Ireland, p. 13, zie https://www.dataprotection.ie/docimages/documents/DPC%20AR2015_FINAL-WEB.pdf.

gebruik van camerabewaking.[66] Afgezien van deze indicaties is het niet duidelijk of en wanneer PIA's uitgevoerd moeten worden, zelfs als deze verplicht zijn. Ook heeft de DPC geen model ontwikkeld en biedt het geen richtlijnen voor het uitvoeren van PIA's. Onlangs heeft de DPC een rapport uitgegeven over de komende Algemene Verordening Gegevensbescherming (AVG) waarin wordt aangegeven dat Data Protection Impact Assessments (DPIA's) verplicht zullen worden voor risicovolle verwerkingen.[67]

Privacy en de bescherming van persoonsgegevens in nieuw beleid
Het schijnbaar enige middel dat de overheid kan gebruiken om te anticiperen op nieuwe ontwikkelingen op het gebied van de bescherming van persoonsgegevens, is het Forum voor Overheidsgegevens (Government Data Forum) dat in 2015 onder het ministerie van de Taoiseach (de premier) is opgericht. Het is echter onduidelijk of de overheid rekening houdt met deze discussies wanneer het nieuwe beleidsmaatregelen ontwikkelt. Ook is het niet zeker of principes zoals Privacy by Design gebruikt worden bij het opstellen van nieuw beleid. De DPC heeft gesteld dat Privacy by Design van belang is voor alle data controllers die werken met complexe productaanbiedingen, die zich richten op grote en internationale doelgroepen en voornamelijk waar technologie een belangrijk onderdeel is in de levering van producten. Dit lijkt te impliceren dat Privacy by Design volgens de DPC vooral bruikbaar is voor bedrijven.[68]

Maatschappelijk debat
De nationale regering van Ierland lijkt een actieve houding aan te nemen in het maatschappelijk debat over de bescherming van persoonsgegevens. Een goed voorbeeld hiervan is het eerdergenoemde Government Data Forum dat een verscheidenheid aan opinies verzamelt, inclusief van actoren in de industrie, de burgermaatschappij, universiteiten en de publieke sector, om zodoende de bescherming van persoonsgegevens in de digitale economie te verbeteren.[69] Sinds de oprichting hebben er zes forums plaatsgevonden.[70] Het meest recente forum werd in mei 2017 gehouden en ging over de rol die data in de moderne maatschappij spelen, het vergroten van het bewustzijn van de gegevensbeschermingsrechten van individuen en het promoten van Ierland als gedachteleider op het gebied van data en de bescherming van persoonsgegevens.[71] Afgezien van dit initiatief lijkt de overheid niet het voortouw te nemen in het maatschappelijk debat over de bescherming van persoonsgegevens.

---

66 https://www.dataprotection.ie/docs/Data-Protection-CCTV/m/242.htm.

67 The GDPR and You, General Data Protection Regulation, Preparing for 2018, Data Protection Commissioner of Ireland, p. 9-10, zie https://www.dataprotection.ie/docimages/documents/The%20GDPR%20and%20You.pdf.

68 Annual Report of the Data Protection Commissioner of Ireland, p. 15, available at https://www.dataprotection.ie/docimages/documents/DPC%20AR2015_FINAL-WEB.pdf.

69 http://www.taoiseach.gov.ie/eng/publications/publications_2015/government_data_forum.html; http://merrionstreet.ie/en/News-Room/Releases/Minister_Murphy_launches_Government_Data_Forum_.html.

70 http://www.taoiseach.gov.ie/DOT/eng/Work_Of_The_Department/Data_Protection_Division/Data_Protection_Division.html.

71 http://www.taoiseach.gov.ie/eng/Taoiseach_and_Government/About_the_Ministers_of_State/Minister/MoS_Murphy_s_Press_Releases/Dara.html.

Informatiecampagnes
De overheid maakt informatie openbaar en publiceert rapporten over de bescherming van persoonsgegevens, maar het belangrijkste aandachtsgebied is de online veiligheid voor kinderen.[72] De *Office for Internet Safety* (OIS), onderdeel van het ministerie van Justitie en Gelijkheid, biedt educatief materiaal aan dat gericht is op ouders,[73] maar verstrekt ook meer gespecialiseerde informatie over onderwerpen als nieuwemediatechnologieën,[74] filtertechnologieën,[75] sociale media[76] en cyberpesten.[77] De DPC verspreidt informatiemateriaal en verwijzingen naar informatie over de bescherming van persoonsgegevens. Beknopte algemene informatie over de kaders voor gegevensbescherming[78] en onderwijsmateriaal[79] is op de website te vinden, evenals aanvullende informatie voor zowel individuen[80] als organisaties.[81] De DPC en andere autoriteiten hebben zo nu en dan burgers via openbare bewustmakingscampagnes geïnformeerd over de bescherming van persoonsgegevens en technische beveiligingsproblemen.[82]

6.3 Wet- en regelgeving

Implementatie van de EU-richtlijn
De belangrijkste wet in Ierland die zich richt op de bescherming van persoonsgegevens is de Data Protection Act 1988. Deze is gewijzigd door de Data Protection Act 2003 (samen de DPActs) om EU-richtlijn 95/46/EC op nationaal niveau te implementeren. De wetgeving wordt aangevuld door de European Communities Regulations 2011 (2011 Regulations) voor de uitvoering van de EU-ePrivacy richtlijn 2002/58/EC. Deze wetgeving schenkt aandacht aan gegevensbeschermingsvraagstukken die verband houden met het gebruik van elektronische communicatieapparatuur en stelt beperkingen ten aanzien van directe marketingdoeleinden.[83]
De DPActs voldoen doorgaans aan de minimumvoorschriften voor de tenuitvoerlegging van richtlijn 95/46/EC, maar er zijn gebieden waar de DPActs, zoals deze door de Ierse rechtbanken worden toegepast, niet aan de minimumeisen van de richtlijn voldoen. Zoals bijvoorbeeld:

- Artikel 23 van de richtlijn bepaalt dat de lidstaten zelf bepalen dat eenieder die schade heeft geleden ten gevolge van een onrechtmatige verwerking of van een daad die onverenigbaar is met de krachtens deze richtlijn vastgestelde bepalingen, het recht heeft de voor de verwerking verantwoordelijke vergoeding van de geleden schade te verkrijgen. Deze bepaling vereist dat een schadevergoeding kan worden toegekend

72 http://www.internetsafety.ie/website/ois/oisweb.nsf/page/safety-en.
73 http://www.internetsafety.ie/website/ois/oisweb.nsf/page/safety-guideparents-en.
74 http://www.internetsafety.ie/website/OIS/OISWeb.nsf/page/EJST-A9FDX61194628-en.
75 http://www.internetsafety.ie/website/OIS/OISWeb.nsf/page/EJST-A9FF9312165228-en.
76 http://www.internetsafety.ie/website/OIS/OISWeb.nsf/page/EJST-A9FFC512214628-en.
77 http://www.internetsafety.ie/website/OIS/OISWeb.nsf/page/EJST-A9FFEQ12255628-en.
78 https://www.dataprotection.ie/docs/Guidance-Material-Menu-Page/m/219.htm.
79 https://www.dataprotection.ie/docs/Training-and-Public-Awareness/b/805.htm.
80 https://dataprotection.ie/docs/A-guide-to-your-rights-Plain-English-Version/r/858.htm.
81 https://dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm.
82 Expert survey v. 2, p. 9.
83 https://www.dataprotection.ie/docs/Law-On-Data-Protection/m/795.htm.

voor immateriële schade, zoals nood of angst. In *Collins v. FBD Insurance*[84] heeft de High Court echter geoordeeld dat de bepaling, zoals geïmplementeerd in de Ierse DPActs, beperkt was tot compensatie voor 'speciale schade' (zoals financieel verlies of reeds gemaakte kosten) en stond het niet toe dat een schadevergoeding werd toegekend voor immateriële verliezen.

- Persoonsgegevens die bestaan uit informatie die de persoon die de gegevens bijhoudt door de wet verplicht is om ter beschikking van het publiek te stellen, zijn uitgesloten van het toepassingsbeleid van de DPActs.[85] Dit wijst er in wezen op dat het toegestaan is om gegevens uit openbare registers te verzamelen en zonder enige beperking te hergebruiken. EU-richtlijn 95/46/EC staat dit echter niet toe. Ook het standpunt van de Artikel 29 Werkgroep is dat de EU-richtlijn voor de bescherming van persoonsgegevens gewoon van toepassing is op persoonsgegevens die openbaar gemaakt zijn.[86]
- In *EMI/Data Protection Commissioner*[87] oordeelde de High Court dat logs van IP-adressen bijgehouden voor de muziekindustrie niet als persoonsgegevens beschouwd kunnen worden, omdat betrokken individuen niet geïdentificeerd kunnen worden zonder verdere informatie. Deskundigen hebben destijds vragen gesteld bij deze beslissing omdat ze dit in strijd achtten met de richtlijnen van de Artikel 29 Werkgroep. Nu blijkt het ook in tegenspraak te zijn met een recente HvJ EU-beslissing in *Patrick Breyer/Bundesrepublik Deutschland*.[88]

De DPActs vereisen ook dat de DPC eerst reageert op klachten door te proberen te komen tot een minnelijke regeling tussen de partijen die betrokken zijn bij de klacht.[89] Deze bepaling is bekritiseerd voor zijn open, soft-law benadering en voor het veroorzaken van procedurele vertraging in gevallen waar het duidelijk is dat er een meer formele bepaling nodig is.[90]

Er lijkt een significante spanning te bestaan tussen enerzijds richtlijn 95/46/EC en anderzijds bepaalde Ierse wetgeving, zoals de Health Identifiers Act 2014. Deze wetgeving staat grootschalige gegevensuitwisseling binnen de Ierse regering toe, zonder de mogelijkheid dit te weigeren en op een manier die inbreuk lijkt te maken op een recente uitspraak van het HvJ EU in *Bara*.[91] In deze zaak werd namelijk bevestigd dat als een overheidsinstantie van plan is persoonsgegevens te verstrekken aan een andere overheidsinstantie, de betrokkenen van tevoren ingelicht moeten worden over de overdracht

84 [2013] IEHC 137.

85 Section 1(4).

86 Denis Kelleher, *Privacy and Data Protection Law in Ireland*. Haywards Heath: Bloomsbury Professional, 2015 (2nd ed.), p. 91.

87 *[2012] IEHC 264.*

88 Case C-582/14.

89 Section 10(1)(b)(ii).

90 Adrian Weckler, 'German Jeers at Irish Data Privacy May Help Us', *Independent.ie*, 31 May 2015, http://www.independent.ie/business/technology/news/german-jeers-at-irish-data-privacy-may-help-us-31266778.html.

91 Expert survey, p. 9. Case C 201/14, *Bara and others v. Preşedintele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Asigurări de Sănătate and Agenţia Naţională de Administrare Fiscală (ANAF).*

van hun persoonsgegevens en ook op de hoogte gebracht moeten worden van het doel van de verwerking ervan.
Het Ierse rechtssysteem bevat nog meer algemene voorschriften die gerelateerd zijn aan de bescherming van persoonsgegevens. De Freedom of Information Act 2014 voorziet mensen van het recht tot het verkrijgen van informatie waarover een instantie beschikt waarop de wet van toepassing is. Ook biedt het de mogelijkheid om officiële informatie over henzelf te wijzigen, indien deze onvolledig, onjuist of misleidend is. Verder maken S.I. No. 337 of 2014 – Data Protection Act 1988, (Commencement) Order 2014 en S.I. No. 338 of 2014 – Data Protection (Amendment) Act 2003, (Commencement) Order 2014 het illegaal voor werkgevers om van werknemers of werkzoekenden te verlangen dat zij kopieën van persoonsgegevens indienen, zodat deze aan de werkgever of toekomstige werkgever ter beschikking gesteld kunnen worden. De regeling is van toepassing op iedereen die een andere persoon benadert om diensten te verlenen.[92]

Sectorale wetgeving
Er is ook een aantal sectorspecifieke bepalingen die betrekking hebben op de bescherming van persoonsgegevens. Zo is er bijvoorbeeld S.I. No. 83/1989 Data Protection (Access Modification) (Social Work) Regulations 1989, waarin specifieke beperkingen voor persoonsgegevens uit de maatschappelijke dienstverlening zijn vastgelegd. Volgens S.I. No. 421 uit 2009 – Data Protection Act 1988 (Section 5(1)(D)) (Specification) Regulations 2009 zijn de DPActs niet van toepassing op het gebruik van persoonsgegevens bij de uitvoering van bepaalde functies van de Director of Corporate Enforcement en inspecteurs aangewezen door de High Court of Director of Corporate Enforcement. S.I. No. 687/2007 Data Protection (Processing of Genetic Data) Regulations 2007 legt beperkingen op aan de verwerking van genetische gegevens op het gebied van werkgelegenheid. S.I. No. 95/1993 Data Protection Act 1988 (Section 5 (1) (D)) (Specification) Regulations 1993 sluit het gebruik van persoonsgegevens bij de uitvoering van bepaalde functies van de Central Bank, de National Consumer Agency en diverse functies uitgevoerd door auditeurs in het kader van de Companies Acts uit van het toepassingsgebied van de DPActs. S.I. No. 81/1989 Data Protection Act, 1988 (Restriction of Section 4) Regulations 1989 beperkt het recht op toegang tot informatie over geadopteerde kinderen en informatie die de Public Service Ombudsman tijdens een onderzoek verkrijgt. Ten slotte heeft S.I. No. 82/1989 Data Protection (Access Modification) (Health) Regulations 1989 betrekking op het recht op toegang tot gezondheidsdata en de bijbehorende beperkingen.[93]
Wat betreft categorieën van gevoelige persoonsgegevens behandelen de DPActs zowel 'standaard' gevoelige gegevens (zoals informatie over de raciale of etnische afkomst van een persoon, politieke meningen, religieuze of filosofische overtuigingen, vakbondlidmaatschap, gezondheid of seksleven) als informatie over strafbare feiten of strafrechtelijke procedures.[94] Toestemming voor de verwerking van dergelijke gegevens dient door de betrokkenen op expliciete wijze schriftelijk of mondeling gegeven te worden, voordat

92 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/ireland#chaptercontent1.
93 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/ireland#chaptercontent1.
94 See the list in S.1 [*No.* 25.] DPActs.

de verantwoordelijke begint met de verwerking van de gegevens. Het wordt als onvoldoende beschouwd wanneer de betrokkene alleen wordt gevraagd of hij of zij bezwaar maakt tegen de verwerking.[95] De DPActs stellen ook aanvullende voorwaarden vast met betrekking tot de rechtmatige verwerking van gevoelige persoonsgegevens. Daartoe behoren verwerkingen van gegevens die noodzakelijk zijn voor statistische doeleinden, politieke activiteiten, belastinginning, beoordeling van het recht op sociale uitkeringen en verwerking die is toegestaan door verordeningen van de minister van justitie vanwege enig zwaarwegend algemeen belang.[96]

Zelfregulering en gedragscodes

Artikel 13 van de Data Protection Act 1988 schrijft voor dat representatieve handelsassociaties rechtstreeks invloed moeten hebben op de totstandbrenging van gegevensbeschermingsnormen binnen hun sectoren en dat de toezichthouder de opzet van de gedragscodes moet bevorderen.[97] Wanneer een dergelijke code door de toezichthouder (DPC) naar behoren is goedgekeurd, kan deze in de desbetreffende sector in gebruik genomen worden. Als een vertegenwoordiger het opstellen van een gedragscode op gang wil brengen, wordt deze aangemoedigd om contact op te nemen met de toezichthouder voor de bescherming van persoonsgegevens om (discussie)bijeenkomsten te verzorgen waarin de te volgen handelwijze besproken kan worden. De toezichthouder geeft praktisch advies over zaken die aan bod moeten komen en geeft aan hoe er omgegaan moet worden met specifieke omstandigheden en verwachtingen in bepaalde sectoren.

Daarnaast heeft de DPC het recht om op eigen initiatief een gedragscode op te stellen. Zo heeft de DPC in 2010 een Personal Data Security Breach Code gepubliceerd[98] die aanzienlijke gevolgen heeft voor entiteiten die te maken hebben met een datalek. Hoewel de code zelf vrijwillig is, beschouwt de DPC deze als aanvulling op de veiligheidsvoorschriften onder de DPActs.[99] De door de DPC opgestelde codes kunnen bindende rechtsgevolgen hebben indien deze door de wetgever worden goedgekeurd.

6.4 Implementatie

De DPActs van 1988 en 2003 schrijven geen specifieke beveiligingsmaatregelen voor waaraan een gegevensbeheerder of gegevensverwerker moet voldoen, maar de 2011 Regulations verwijzen wel naar enkele eisen die specifiek zijn voor de sector elektronische communicatiediensten. De DPActs verplichten de gegevensbeheerders in plaats daarvan 'adequate beveiligingsmaatregelen' in te voeren om privacyincidenten en datalekken te voorkomen. De DPActs wijzen op een aantal factoren waarmee bij de beoordeling van de 'geschiktheid' van de gegevensbeveiligingsinstrumenten rekening gehouden moet worden. Organisaties moeten het volgende overwegen:

95 S. 2B DPActs.
96 Linklaters 2015, p. 126.
97 https://www.dataprotection.ie/docs/Self_Regulation_and_Codes_of_Practice/m/98.htm.
98 https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.
99 Linklaters 2015, p. 127.

- de stand van de technologische ontwikkeling;
- de kosten voor de tenuitvoerlegging van de maatregelen;
- de schade die veroorzaakt kan worden;
- de aard van de gegevens.[100]

Gegevensbeheerders en -verwerkers moeten er ook voor zorgen dat hun werknemers op de hoogte zijn van het beveiligingsbeleid van het bedrijf en zich hieraan houden. De wettelijke verplichting om persoonsgegevens op passende wijze te beveiligen is van toepassing op elke gegevensbeheerder en gegevensverwerker, ongeacht hun omvang. De DPC ondersteunt het ontwerpen van intern beveiligingsbeleid door niet-bindende begeleiding te geven ten aanzien van zaken als toegangscontrole, toegangsverlening, encryptie, antivirus software, firewalls, het bijwerken van software en toegang op afstand.[101]
Tot op heden heeft een aantal organisaties ervoor gekozen om een sectorale gedragscode te ontwikkelen. De toezichthouder heeft formeel ingestemd met dergelijke gedragscodes voor de politie (*Garda Síochána*), de Injuries Board, de verzekeringssector, het ministerie van Onderwijs en Vaardigheden, de Revenue Commissioners, het comité voor de beroepsopleiding, de reclasseringsdienst en het ministerie van Volksgezondheid.[102]

Privacyfunctionarissen
De Ierse wetgeving bevat geen bepalingen inzake de voorschriften voor de aanwijzing van privacyfunctionarissen (DPO's), maar gegevensbeheerders en -verwerkers moeten wel informatie verstrekken over een 'compliance person' bij het registreren bij de DPC. De aanstelling van een privacyfunctionaris is daardoor optioneel. In de afgelopen jaren is er echter een toename geweest van vrijwillige afspraken, aangezien deze niet alleen gunstig bleken te zijn voor klantenrelaties en reputaties, maar ook voor het opbouwen van een relatie met de DPC via een gecentraliseerd kantoor.[103] Aangezien het geen vereiste is om een privacyfunctionaris aan te wijzen, worden er ook geen specifieke eisen aan de kennis of deskundigheid van de privacyfunctionaris gesteld. Dit lijkt te hebben geleid tot de opkomst van verenigingen van privacyfunctionarissen. Deze verenigingen bieden een platform om inzichten en best practices te delen, duidelijkheid over wetgeving te krijgen en zorgen te bespreken.[104]
Nadat privacyfunctionarissen benoemd zijn, verzekeren ze doorgaans dat de organisatie de gegevensbeschermingsbepalingen naleeft en functioneren ze als contactpunt voor alle aangelegenheden die hier betrekking op hebben. Zij ondersteunen, begeleiden, adviseren en trainen de werknemers van de organisatie op het gebied van de bescherming van persoonsgegevens en dragen bij aan de risicobeheersingsprocessen.[105]

100 https://www.dataprotection.ie/docs/Data-security-guidance/1091.htm.
101 https://www.dataprotection.ie/docs/Data-security-guidance/1091.htm.
102 Zie voor de volledige lijst https://www.dataprotection.ie/docs/Self_Regulation_and_Codes_of_Practice/m/98.htm.
103 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/ireland#chaptercontent6.
104 Zie bijvoorbeeld the Association of Data Protection Officers, https://dpo.ie/about.
105 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/ireland#chaptercontent6.

Beveiligingsmaatregelen

Organisaties gebruiken maatregelen om persoonsgegevens te beschermen, maar sommige maatregelen zijn nog niet volledig ten uitvoer gebracht.[106] Er zijn een aantal gevallen geweest waarbij persoonsgegevens werden prijsgegeven of door onbevoegde officiële organisaties, zoals de politie, werden opgevraagd.[107] Dit heeft geleid tot aangescherpte beleidsmaatregelen en een toename in het aantal vervolgingen in verband met ongeoorloofde toegang tot gegevens en het openbaar maken hiervan.[108] De DPC heeft jarenlang Privacy by Design (PbD) gepromoot, maar dit concept heeft echter pas recent meer bekendheid vergaard. Het is onduidelijk hoeveel organisaties het als beleid zullen aannemen.[109] Het 'need to know'-beginsel wordt steeds vaker toegepast, met name door grotere organisaties. De verschillende niveaus van toegang worden gescheiden in beleid en door technische maatregelen.[110] Organisaties zijn bereid om technische beveiligingsmaatregelen en internationale normen te implementeren en interne en externe beveiligingswerkers in dienst te nemen om een bevredigende mate van veiligheid en gegevensbescherming te bereiken. De omvang van de genomen maatregelen hangt doorgaans af van de omvang van de organisatie.[111]

Transparantie

Hoewel de meeste organisaties in Ierland een privacybeleid hanteren, worden er steeds meer cookies op Ierse websites gebruikt, die over het algemeen niet erg gebruiksvriendelijk zijn.[112] De DPC heeft sinds 2013 deelgenomen aan de jaarlijkse 'Privacy Sweep', georganiseerd door het Global Privacy Enforcement Network. Uit dat onderzoek bleek dat 63% van de Ierse websites informatie bevatte over privacy die moeilijk te lezen of te begrijpen was, dat het op 13% van de websites moeilijk was om informatie over privacy te vinden en dat 5% van de sites helemaal geen privacybeleid had.[113] Het Privacy Sweep-onderzoek besteedde ook aandacht aan apps en vond in 2014 dat voor 55% van de Ierse apps de privacyinformatie die wordt verstrekt slechts gedeeltelijk inzicht geeft in het verzamelen, het gebruik en het openbaar maken van persoonlijke informatie, hetgeen vragen oproept met betrekking tot gevraagde toestemmingen.[114]

Aan de andere kant lijkt een groot aantal Ieren (70%) zelden of nooit de voorwaarden te lezen alvorens deze te accepteren.[115] Van degenen die privacyvoorwaarden doornemen, leest ongeveer 89% niet de hele tekst. 54% claimt doorgaans het grootste deel of alles van het privacybeleid te begrijpen. Verder blijkt dat ongeveer 37% op een bepaald moment heeft besloten om een website niet te gebruiken wegens ontevredenheid over

106 Expert survey v2, p. 5.
107 Expert survey v2, p. 5.
108 Expert survey v2, p. 5.
109 Expert survey v2, p. 6.
110 Expert survey v2, p. 6.
111 Expert survey v2, p. 6.
112 Expert survey v2, p. 7. Expert survey, p. 10.
113 Expert survey, p. 10.
114 Data Protection Commissioner, 'Global Privacy Sweep Raises Concerns about Mobile Apps', 2014, https://www.dataprotection.ie/docs/10-09-14-Global-Privacy-Sweep-raises-concerns-about-mobile-apps/i/1456.htm.
115 Consent Country Report Ireland (2012) p. 37.

de privacyvoorwaarden, hetgeen aanzienlijk lager ligt dan het EU-gemiddelde (47%).[116] Gepersonaliseerde privacyinstellingen zijn niet gebruikelijk en worden doorgaans alleen gepromoot door technologische multinationals en technologische websites.[117]

6.5 Toezicht en handhaving

Toezichthouders

Het Office of the Data Protection Commissioner (DPC) is opgericht onder de Data Protection Act 1988 en bestaat sinds 1989. Het is de toezichthoudende instantie die waakt over de naleving van de wetgeving inzake de bescherming van persoonsgegevens in Ierland. De commissaris die aan het hoofd staat van het bureau van de DPC wordt benoemd door de regering en is onafhankelijk in de uitoefening van zijn/haar bevoegdheden.[118]

De begroting van het bureau van de DPC wordt vastgesteld door het Ierse ministerie van Justitie en Gelijkheid. In 2016 is dit bedrag aanzienlijk gestegen van 3,65 miljoen euro naar 4,7 miljoen euro. De recent gepubliceerde begroting stelt dat meer dan 7,5 miljoen euro wordt toegekend aan het bureau van de DPC voor het jaar 2017. Dit heeft deels tot doel de verdere werving van medewerkers, momenteel een van de prioriteiten van het bureau van de DPC, te ondersteunen.[119] Er zijn momenteel 60 mensen in dienst van de DPC,[120] maar de verwachting is dat dit binnen aanzienlijke termijn zal verdubbelen.[121] De boetes die het bureau van de DPC via de wettelijke meldplicht int, vloeien direct terug naar de staatskas.[122]

Taken en bevoegdheden

Bij het uitoefenen van zijn bevoegdheden, voert de DPC onderzoeken en privacyaudits uit, biedt begeleiding aan particulieren en organisaties met betrekking tot hun rechten en plichten inzake de bescherming van persoonsgegevens, stelt gedragscodes op[123] en publiceert jaarverslagen over de werkzaamheden van het bureau. Op grond van artikel 10 van de DPActs is de DPC gerechtigd om een onderzoek naar een bepaalde gegevensbeschermingszaak te starten wanneer het een individuele klacht ontvangt. De DPC heeft de wettelijke verplichting om eerst te proberen in onderling overleg tot een oplossing te komen. Indien dit niet mogelijk is, kan de DPC beslissen of er sprake is van een overtreding van de bepalingen van de DPActs. Zowel de klager als de gegevensbeheerder hebben het recht om tegen de beslissing van de DPC in beroep te gaan bij de rechter, te weten het Circuit Court.

116 Consent Country Report Ireland (2012) p. 37.
117 Expert survey v2, p. 7.
118 https://www.dataprotection.ie/docs/About-the-office-of-the-DPC/b/1032.htm.
119 https://www.dataprotection.ie/docs/13-10-2016-Data-Protection-Commissioner-welcomes-Budget-2017-increase-in-funding/i/1601.htm.
120 DPC AR2015, p. 1.
121 https://www.dataprotection.ie/docs/13-10-2016-Data-Protection-Commissioner-welcomes-Budget-2017-increase-in-funding/i/1601.htm.
122 DPC AR2015, p. 4.
123 Zie 6.3.

De DPC kan ook op eigen initiatief een onderzoek starten indien hij van mening is dat er sprake is van een schending van de regels inzake de bescherming van persoonsgegevens of als deze het passend acht zich ervan te verzekeren dat er wordt voldaan aan de DPActs. Dit laatste type onderzoeken wordt gewoonlijk uitgevoerd in de vorm van privacyaudits, waarvan de gegevensbeheerder van tevoren op de hoogte wordt gebracht. Indien een individu of een organisatie niet aan een onderzoek meewerkt, kan de DPC dergelijke medewerking vereisen door een 'informatiekennisgeving' uit te geven in het kader van artikel 12 van de DPActs. Tegen deze kennisgeving kan bij het Circuit Court beroep worden ingesteld. Het niet naleven van deze informatiekennisgeving zonder geldig excuus is een overtreding.[124]
Op grond van artikel 10 van de DPActs is de DPC ook gemachtigd om alle noodzakelijke stappen te nemen om ervoor te zorgen dat gegevensbeheerders en -verwerkers voldoen aan de voorwaarden van de DPActs. Dergelijke stappen kunnen betrekking hebben op het corrigeren of blokkeren van gegevens, het aanvullen van de gegevens met een verklaring die door de DPC is goedgekeurd of zelfs het wissen van gegevens. De DPC oefent deze bevoegdheden uit door middel van een 'handhavingsbericht' aan de gegevensbeheerders en -verwerkers. Tegen dit handhavingsbericht kan ook beroep worden aangetekend en het niet naleven hiervan zonder geldig excuus is eveneens een overtreding.[125]
Schendingen van de door de DPActs vastgelegde gegevensbeschermingsbepalingen worden doorgaans niet bestempeld als overtredingen en de DPC heeft geen directe bevoegdheid om boetes op te leggen. Indien men echter een handhavingskennisgeving, een informatiekennisgeving of een verbodsbepaling uitgegeven door de DPC negeert, heeft de DPC het recht om een procedure in te leiden voor de Ierse rechtbanken wegens overtreding van de DPActs. Artikel 31 stelt dat de boetes tot maximaal 3.000 euro kunnen oplopen bij een lichte overtreding en tot 100.000 euro bij een zware overtreding. Dit staat in contrast met de 2011 Regulations, die betrekking hebben op telecommunicatiebedrijven en waarvoor de DPC eveneens verantwoordelijk is. In deze 2011 Regulations worden alle overtredingen als afzonderlijke strafbare feiten gezien.[126] Deze hebben voornamelijk betrekking op het elektronisch verzenden van ongevraagd marketingmateriaal (zogeheten spam). Deze feiten zijn strafbaar gesteld met een boete van maximaal 5.000 euro voor elk ongevraagd bericht (on summary conviction – zonder jury) en 250.000 euro volgende op een veroordeling na tenlastelegging (conviction on indictment – met jury). De 2011 Regulations machtigen de DPC onder S.I. 336 van 2011 om zonder tussenkomst van een jury strafrechtelijke boetes voor een overtreding op te leggen.
Naast het ondersteunen van organisaties bij het opstellen van gedragscodes,[127] biedt de DPC ook op vrijwillige basis adviezen aan entiteiten en individuen aan om de naleving van de bescherming van persoonsgegevens te waarborgen. Om die reden heeft de DPC een helpdesk die per telefoon, e-mail of post kan worden bereikt. Een adviesteam

124 https://www.dataprotection.ie/docs/Powers-of-the-Data-Protection-Commissioner/e/96.htm.
125 https://www.dataprotection.ie/docs/Powers-of-the-Data-Protection-Commissioner/e/96.htm.
126 http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/ireland#chaptercontent14.
127 Zie paragraaf 6.3.

behandelt de meer diepgaande onderzoeken. Ten slotte moet worden geconstateerd dat de DPC slechts een raadgevende functie heeft als het gaat om de ontwikkeling van nieuwe wetgeving aangaande de bescherming van persoonsgegevens. Het advies is dus facultatief voor de wetgever.

Gebruik van bevoegdheden

In 2015 werden er door de DPC onderzoeken geopend naar aanleiding van 932 klachten. Er werden meer dan 30.000 vragen ontvangen.[128] Het merendeel van deze vragen (60%) was gerelateerd aan toegangsrechten, terwijl klachten over online marketing de tweede grootste categorie vormden. Individuele klachten lijken benadeeld te worden door de huidige DPC.[129] Volgens het jaarverslag van de DPC werd voor het overgrote deel van de klachten een minnelijke schikking gevonden. Formele besluiten werden slechts in 52 gevallen genomen, waarvan 43 klachten als gegrond werden verklaard.[130] De DPC heeft in 2015 3 wettelijke handhavingskennisgevingen uitgegeven.[131] De DPC heeft op grond van de DPActs geen bevoegdheid om zelf geldboetes of administratieve sancties op te leggen aan overtreders (zie hiervoor), maar is wel in staat om preventieve en corrigerende maatregelen te nemen, zoals handhavingskennisgevingen.[132]

De DPC heeft ook de mogelijkheid om zaken aan de rechtbank voor te leggen als het gaat om overtredingen die verband houden met de bescherming van persoonsgegevens en ongevraagde marketing.[133] In 2015 zijn er procedures gestart tegen 4 organisaties, samen goed voor 24 overtredingen in het kader van de 2011 Regulations. De 4 organisaties werden succesvol vervolgd voor marketinggerelateerde overtredingen betreffende ongewenste sms-berichten en (herhaalde) ongevraagde telefoongesprekken, hetgeen resulteerde in boetes die varieerden van 1.000 tot 35.000 euro.[134] Er is weinig informatie beschikbaar over succesvolle vervolging op grond van de Data Protection Acts, alhoewel een privé-onderzoeker onlangs een boete van 7.500 euro opgelegd heeft gekregen voor het onrechtmatig verkrijgen van persoonsgegevens van het ministerie van Sociale Bescherming.[135] De mogelijkheid van de DPC tot het instellen van vervolging is echter beperkt tot wat wordt bestempeld als een overtreding onder de Data Protection Acts. De roekeloze verwerking van persoonsgegevens wordt bijvoorbeeld niet gezien als een

128 Data Protection Commissioner, 'Annual Report 2015', 2016, https://www.dataprotection.ie/docimages/documents/DPC%20AR2015_FINAL-WEB.pdf.

129 Zie ook

130 DPC AR2015, p. 5.

131 Gerelateerd aan datalekken bij Telefonica Ireland Limited, Arizun Services Ireland Limited en Aer Lingus. Zie DPC AR2015, p.7.

132 Expert survey, p. 11. "Such measures may include [...] correcting the data, blocking the data from use for certain purposes, supplementing the data with a statement which the Commissioner approves, or erasing the data altogether". Zie *Powers of the Data Commissioner*, Data Protection Commissioner of Ireland, available at https://www.dataprotection.ie/docs/Powers-of-the-Data-Protection-Commissioner/e/96.htm#The Commissioner's Power to Enforce Compliance with the Act.

133 Id p. 12.

134 DPC AR2015, p. 21-22.

135 https://www.irishtimes.com/news/ireland/irish-news/private-investigator-fined-7-500-over-data-protection-breaches-1.2824210.

overtreding, waardoor er geen strafrechtelijke aansprakelijkheid voor dergelijke acties mogelijk is.[136]
Er zijn relatief weinig rechtszaken op het gebied van de bescherming van persoonsgegevens waarin de DPC geen rol speelt.[137] Voorbeelden van uitzonderingen zijn de zaken *Collins/FBD Insurance Plc*.[138] en *Digital Rights Ireland Ltd/Minister for Communication & Ors.*[139] Als het gaat om geschillen tussen particulieren spelen verzoeken om gegevensbescherming veelal een aanvullende rol in plaats van de belangrijkste rol.[140] De Ierse wet staat groepsclaims niet toe, hetgeen het gebrek aan rechtszaken naar aanleiding van datalekken kan verklaren.[141]

Reputatie
Zowel burgers als bedrijven zijn over het algemeen op de hoogte van de toezichthouder en diens activiteiten, maar dit bewustzijn is in de commerciële sector hoger dan in de publieke sector.[142] De DPC is bekritiseerd voor het bevoordelen van bedrijven en overheidsinstanties.[143] Een niet-gouvernementele organisatie, Digital Rights Ireland, heeft een rechtszaak aangespannen tegen de staat bewerende dat de DPC niet voldoende onafhankelijk is van de overheid.[144]
Tijdens de *Schrems*-zaak heeft een rechter van het HvJ EU zich afgevraagd of de DPC opzettelijk onvoldoende gefinancierd werd door de rijksoverheid met als doel het toezicht te belemmeren.[145] Een voormalig commissaris van de autoriteit heeft verklaard dat het bureau zicht richt op correctie en begeleiding in plaats van strengere strafmaatregelen.[146] Hierdoor zijn bedrijven niet bang voor de DPC[147] en uit recent onderzoek[148] onder leidinggevenden bleek dat 82% (van de in totaal 200 geconsulteerde bedrijven) de DPC als 'goed tot uitstekend' beoordeelde.[149]

---

136 Expert survey, p. 12.
137 Expert survey, p. 12.
138 *Collins/FBD Insurance Plc* [2013] IEHC 137 (14 March 2013), available at http://www.bailii.org/cgi-bin/format.cgi?doc=/ie/cases/IEHC/2013/H137.html&query=(fbd),
139 *Digital Rights Ireland Ltd/Minister for Communication & Ors* [2010] IEHC 221 (05 May 2010). [2010] 3 IR 251, [2010] IEHC 221, op http://www.bailii.org/cgi-bin/for-mat.cgi?doc=/ie/cases/IEHC/2010/H221.html&query=%28digi-tal%29+AND+%28rights%29+AND+%28ireland%29.
140 Expert survey, p. 12. Zie bijvoorbeeld *Collins/FBD Insurance Plc* [2013] IEHC 137 (14 March 2013), op http://www.bailii.org/cgi-bin/format.cgi?doc=/ie/cases/IEHC/2013/H137.html&query=(fbd).
141 Expert survey, p. 12.
142 Expert survey v2, p. 9.
143 Expert survey, p. 12.
144 Expert survey, p. 12.
145 Expert survey, p. 12.
146 Expert survey, p. 12-13. Billy Hawkes, 'The Irish DPA and Its Approach to Data Protection', in *Enforcing Privacy*, ed. David Wright and Paul De Hert (Cham: Springer International Publishing, 2016), 446 and 454, http://link.springer.com/10.1007/978-3-319-25047-2_18.
147 William McGeveran, 'Friending the Privacy Regulators', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 5 August 2016), https://papers.ssrn.com/abstract=2820683.
148 William Fry and Forbes, 'Europe for Big Data', November 2016, http://www.williamfry.com/docs/default-source/reports/william-fry-europe-for-big-data-report.pdf?sfvrsn=0.
149 Expert survey, p. 13.

7 Frankrijk

7.1 Algemene situatie

De geschiedenis van de mensen- en burgerrechten in Frankrijk begint met de Verklaring van de Rechten van de Mens en Burger, een document dat in 1789 tijdens de Franse Revolutie is opgesteld. In deze verklaring staat dat de rechten van de mens overal ter wereld gelden en de verklaring vormt nog steeds de basis voor de huidige grondwet. De Franse grondwet bevat geen artikelen over de mensenrechten, maar de preambule van de grondwet bevat deze wel. De Franse grondwet is heel vaak aangepast, het meest recent in 2008. Frankrijk neemt een monistische houding aan ten opzichte van het internationaal recht. Zodoende hoeven internationale verdragen niet in de nationale wetgeving opgenomen te worden voor ze als bindend worden beschouwd.[1]
Frankrijk heeft de Universele Verklaring van de Rechten van de Mens, het Europese Verdrag tot Bescherming van de Rechten van de Mens en het Handvest van de grondrechten van de Europese Unie bekrachtigd. Deze rechtsinstrumenten bevatten het recht op privacy. De Franse grondwet bevat dit recht niet. Het recht op privacy is echter opgenomen in artikel 9 van het Frans Burgerlijk Wetboek middels de parlementaire wet van 17 juli 1970, waarin staat dat "iedereen het recht heeft op respect voor zijn of haar privéleven". Hoewel er geen wettelijke definitie van privéleven bestaat, heeft de rechtbank bepaald dat privéleven het liefdesleven, vriendschappen, de gezinssituatie, vrijetijdsactiviteiten, politieke meningen, vakbondslidmaatschap of de religieuze gezindheid en de gezondheidstoestand van een persoon omvat.[2] Frankrijk was een van de eerste landen ter wereld met een wet inzake gegevensbescherming. De eerste Franse wet inzake gegevensbescherming (Loi informatique et libertés) stamt uit 1978.[3]
Met 67 miljoen inwoners is Frankrijk een van de grotere landen binnen de EU.[4] De duidelijke scheiding tussen werk en privé, met een sterk recht op privacy, maakt onderdeel uit van de Franse cultuur. Onlangs heeft de Franse overheid de ambitie uitgesproken de Algemene Verordening Gegevensbescherming (AVG) aan te willen nemen

1 Zie artikel 26 van de Franse grondwet: "les traités régulièrement ratifiés et publiés ont force de loi sans qu'il soit besoin d'autres dispositions législatives que celles qui auraient été nécessaires pour assurer sa ratification".

2 http://franceintheus.org/spip.php?article640.

3 Loi numéro 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Wet inzake informatietechnologie, bestanden en vrijheid), zie https://www.cnil.fr/sites/default/files/typo/.../Act78-17VA.pdf.

4 http://www.bdm.insee.fr/.

voordat deze officieel van kracht wordt in 2018.[5] Na de terroristische aanvallen in Parijs en Nice werd de noodtoestand afgekondigd, hetgeen leidde tot spanningen tussen de nationale veiligheid en de bescherming van persoonsgegevens.

Het gebruik van internet

Het internetgebruik in Frankrijk is snel toegenomen van 14% van de bevolking in 2000 naar 84% in 2015.[6] Het gebruik van breedbandconnectiviteit is relatief laag (met een gemiddelde van 9,9 Mbps staat Frankrijk op de op vijf na laatste plaats, in vergelijking tot Nederland dat met 17,9 op de vijfde plaats staat).[7]

Frankrijk is een van de vijf EU-landen waar minder dan 50% van de bevolking het internet minstens een keer per week gebruikt voor socialemediadoeleinden: 47% tegen een gemiddelde van 57% in de EU.[8] Met betrekking tot het wekelijkse gebruik van instant messaging en chats komt Frankrijk met 49% dichter bij het EU-gemiddelde van 53%.[9] Met 33% is het gebruik van internet voor online bankieren ook laag ten opzichte van het EU-gemiddelde van 43%. De top drie landen behalen percentages van 75 of hoger (Nederland 75%, Denemarken 79% en Finland 84%). Met betrekking tot het internetgebruik voor het minstens eens per week voeren van telefoon- (of video)gesprekken scoort Frankrijk met 28% net boven het EU-gemiddelde. Frankrijk behoort tot een grote groep EU-landen waar tussen een kwart en een derde van de bevolking minstens een keer per week het internet op gaat om te gamen (16 van de 28 landen, waaronder Frankrijk met 29%).[10] Frankrijk heeft met 76% het hoogste percentage mensen dat *nooit* het internet gebruikt om films en muziek te delen via het internet.[11]

Controle

Frankrijk staat in de top drie van EU-landen waar een gebrek aan controle wordt ervaren met betrekking tot persoonsgegevens die online worden verstrekt (Frankrijk staat, met 34% van de bevolking die aangeeft geen controle te ervaren, op de derde plaats na Spanje met 36% en Duitsland met 45%).[12] Frankrijk behoort ook tot de landen waar men zich het meest zorgen maakt over het feit dat de betalingsactiviteiten worden geregistreerd (62% in vergelijking tot het EU-gemiddelde van 55%).[13]

---

5 Dit is vastgelegd in het wetsvoorstel voor een *République Numérique* dat in 2016 is aangenomen: http://www.economie.gouv.fr/projet-loi-pour-republique-numerique-definitivement-adopte, http://privacylawblog.fieldfisher.com/2016/france-to-adopt-gdpr-provisions-before-it-comes-into-force-in-2018/.

6 http://www.internetworldstats.com/eu/fr.htm.

7 https://www.stateoftheinternet.com/downloads/pdfs/Q4-2015-SOTI-Connectivity-Executive-Summary.pdf.

8 Eurobarometer 431 (2015), p. 109. http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm#431.

9 Eurobarometer 431 (2015), p. 110.

10 Eurobarometer 431 (2015), p. 111.

11 Eurobarometer 431 (2015), p. 113.

12 Eurobarometer 431 (2015), p. 10.

13 Eurobarometer 431 (2015), p. 17.

Bewustzijn

Tijdens een onderzoek bleek dat de mate van bewustzijn bij de Fransen met betrekking tot het gebruik van persoonsgegevens door eigenaren van websites iets onder het gemiddelde ligt en dat, interessant genoeg, Frankrijk het hoogste percentage respondenten heeft dat aangeeft "niet precies te weten wat dit betekent".[14] Als we nauwkeuriger kijken, zien we echter dat dat de mate van het Franse bewustzijn vergelijkbaar is met het EU-gemiddelde en dat de mate van non-acceptatie voor de wijze waarop eigenaren van websites persoonsgegevens gebruiken voor het aanpassen van de inhoud en advertenties die gebruikers zien duidelijk hoger dan het EU-gemiddelde is.[15]

In 2013 richtte de Franse toezichthouder, de *Commission Nationale de L'Informatique et des Libertés* (CNIL), het zogeheten *Le collectif Educnum* op,[16] een platform dat circa 60 lidorganisaties verbindt en dat zicht richt op het vergroten van het bewustzijn bij burgers en bedrijven omtrent de bescherming van persoonsgegevens. Hun website bevat onderzoek en informatie over het gebruik van het internet en de bescherming van persoonsgegevens voor burgers en consumenten.[17]

Vertrouwen

Het vertrouwen van de Franse bevolking in de bescherming van persoonsgegevens door verschillende autoriteiten is relatief hoog ten opzichte van het EU-gemiddelde: 79% tegenover 74%. Dit is een daling van 7% in vergelijking tot 2010. Met name het vertrouwen in overheidsinstanties is relatief hoog (73% in vergelijking tot het EU-gemiddelde van 66%). Enigszins hoger dan gemiddeld is het vertrouwen in banken en financiële instellingen (60% ten opzichte van een EU-gemiddelde van 56%) en EU-instanties (53% ten opzichte van een EU-gemiddelde van 51%).

Frankrijk scoort daarentegen laag bij sommige andere categorieën. Net als in Nederland (31%) is het vertrouwen van de Franse bevolking dat onlinewinkels op een juiste wijze omgaan met persoonsgegevens bijzonder laag (29%), in tegenstelling tot bijvoorbeeld in Ierland (54%, het EU-gemiddelde is 40%). Het vertrouwen in telecommunicatiebedrijven met betrekking tot de bescherming van persoonsgegevens is met 25% ook relatief laag in vergelijking tot andere EU-landen (met een EU-gemiddelde van 33%), net als het vertrouwen in onlinebedrijven (16% ten opzichte van een EU-gemiddelde van 24%).[18]

Beschermingsmaatregelen

Met betrekking tot acties die burgers ondernemen om hun eigen persoonsgegevens te beschermen, benadrukt het CNIL-platform Educnum dat twee van de drie jonge burgers

14 Consent Landenrapport Frankrijk (2012), p. 27.
15 Consent Landenrapport Frankrijk, (2012), p. 4.
16 https://www.educnum.fr/fr/le-collectif-educnum.
17 Antwoorden van Emmanuel Laforet naar aanleiding van ons onderzoek (Adjoint au chef de bureau du droit constitutionnel et du droit public général), emmanuel.laforet@justice.gouv.fr.
18 Eurobarometer 431 (2015), p. 66.

gebruikmaakt van een advertentieblokker.[19] Het CNIL raadt ook aan om gebruik te maken van een cookieblokker.[20]
In 2015 onthulde Google per ongeluk gegevens met betrekking tot aanvragen inzake 'het recht om vergeten te worden' die het had ontvangen.[21] Uit de gegevens bleek hoeveel van de privacyverzoeken (dat wil zeggen verzoeken om bepaalde gegevens te verwijderen) gericht aan Google betrekking hadden op persoonsgegevens. Volgens die gegevens kwam het hoogste percentage aanvragen met betrekking tot persoonsgegevens uit Frankrijk (98% van alle privacyverzoeken aan Google, Nederland stond op de tweede plaats met 98%, Duitsland was derde met 98%, Zweden vijfde met 96%, het Verenigd Koninkrijk had 95% en Italië 85% – In Italië hield 12% van de aanvragen verband met ernstige misdrijven). Google ontving tot maart 2015 in totaal 218.320 verzoeken, waarvan ongeveer de helft werd gehonoreerd. Dit kan worden gezien als een voorbeeld van acties die burgers ondernemen om hun persoonsgegevens en hun online reputatie te beschermen.[22]

Nationale politiek
De traditionele Franse politieke partijen hebben zich niet bewust uitgesproken over de bescherming van privacy en persoonsgegevens, maar de Franse overheid werkt goed samen met de CNIL.[23] De grootste politieke partijen pleiten voor een combinatie van wetgeving en zelfregulering. De politieke partijen zijn in gesprek met burgerrechtenorganisaties. Sommige organisaties worden geraadpleegd door de overheid tijdens openbare raadplegingen, andere worden geraadpleegd door commissies van de Nationale Vergadering (Assemblée National, het lagerhuis van het parlement) of de Senaat. Er worden ook evenementen georganiseerd in de Nationale Vergadering of door de Franse toezichthouders.
In 2014 publiceerde de overheid haar beleid inzake overheidsgegevens dat diende voor de transparantie en controleerbaarheid van de overheid. Het bevat de aanstelling van een State Chief Data Officer (CDO) en de oprichting van een platform inzake overheidsgegevens dat vrij toegankelijk is (Data.gouv.fr).[24]
In september 2015 startte de overheid het *Project de Loi pour une République Numérique*, een proces van drie weken waarbij de overheid samen met burgers (online) een wettekst opstelde met betrekking tot onderwerpen als netneutraliteit, gegevensportabiliteit, vertrouwelijkheid van online privécommunicatie, het recht om vergeten te worden, de transparantie van overheidsgegevens en de toegankelijkheid voor mensen met handicaps. Alle politieke partijen stemden oktober 2016 in met de daaruit voortgekomen wet.[25]

19 https://www.educnum.fr/fr/2-jeunes-sur-3-utilisent-un-adblocker (published 26 sept 2016).
20 https://www.educnum.fr/fr/cookies-les-outils-pour-les-maitriser.
21 https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests.
22 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
23 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
24 http://www.gouvernement.fr/en/public-data-policy.
25 http://www.economie.gouv.fr/projet-loi-pour-republique-numerique-definitivement-adopte, http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/21499.pdf.

Tijdens de nacht van vrijdag 13 op zaterdag 14 november 2015, onmiddellijk na de terroristische aanslagen op het Bataclan theater in Parijs, kondigde de Franse president de noodtoestand af door middel van twee besluiten genomen door de ministerraad. De noodtoestand is momenteel van kracht in heel Frankrijk en heeft geleid tot diverse rechtszaken tegen de gegevensverwerking voor opsporingsdoeleinden[26] en tegen het kopiëren van gegevens tijdens een inval.[27] De balans tussen privacy en veiligheid is opnieuw vastgesteld middels nieuwe regels inzake de noodtoestand[28] en door middel van het aanpassen van de wet inzake nationale veiligheid.[29,30]

Media-aandacht

Zoals al aangeven, zorgen nieuwe wetten ervoor dat het voor veiligheidsdoeleinden toegestaan is om meer persoonsgegevens te verwerken. Dit wordt soms bekritiseerd door de CNIL[31] en de pers.[32] Er wordt een ruim scala aan onderwerpen aangesneden in de media. De CNIL is algemeen bekend bij het grote publiek en ook bij de gespecialiseerde en algemene media,[33] zowel bij de reguliere als de nieuwe media.[34] De Franse privacywetgeving haalde de internationale pers toen de toenmalige Franse president François Hollande zich beriep op het recht op respect voor zijn privéleven met betrekking tot een onderzoek naar een vermeende buitenechtelijke affaire.

Datalekken

De Franse gegevensbeschermingsautoriteit CNIL vaardigt schriftelijke openbare waarschuwingen uit op haar website in geval van grote datalekken.[35] Er hebben zich recentelijk incidenten voorgedaan in de e-commercesector,[36] de telecomsector[37] en in verband met datingsites.[38] De CNIL reageerde op deze incidenten met een openbare waarschuwing, maar ook met een verhoging van de eventuele administratieve sancties in Wet nr. 78-17. Burgers mogen een schriftelijke klacht indienen bij de CNIL en kunnen de

26 http://www.conseil-etat.fr/Actualites/Communiques/Controle-des-techniques-de-renseignement.
27 http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2016/2016-536-qpc/decision-n-2016-536-qpc-du-19-fevrier-2016.146991.html.
28 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032921910&categorieLien=id.
29 Antwoorden van Emmanuel Laforet, uit ons onderzoek.
30 http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/Tables/tables_analytiques.pdf.
31 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318979&dateTexte=&categorieLien=id.
32 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
33 Zoals, volgens Emmanuel Laforet, zou worden aangetoond middels een zoekopdracht in Google: https://www.google.fr/search?q=CNIL&ie=utf-8&oe=utf-8&gws_rd=cr&ei=ogkaWIilFMyeaN-Wxq9AB#q=CNIL&tbm=nws.
34 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
35 https://www.cnil.fr/.
36 https://www.cnil.fr/fr/cdiscount-avertissement-et-mise-en-demeure-pour-de-nombreux-manquements.
37 https://www.cnil.fr/fr/la-societe-orange-sanctionnee-pour-defaut-de-securite-des-donnees-dans-le-cadre-de-campagnes.
38 https://www.cnil.fr/fr/donnees-traitees-par-les-sites-de-rencontre-8-mises-en-demeure.

besluiten van de Franse raad van state aanvechten.[39] Een overzicht van privacygerelateerde rechtszaken is te vinden op de CNIL-website en op andere websites.[40]

Burgerrechtenorganisaties

In Frankrijk zijn veel organisaties die zich bezighouden met privacy- en gegevensbescherming. Een aantal van die organisaties zijn geen burgerrechtenorganisaties, waaronder Conseil national du numérique, Syndicat de la magistrature, Syndicat des avocats de France, Syntec numérique, Tech in France.[41]

La Quadrature du Net[42] is een non-profitorganisatie die de rechten en vrijheden van burgers op het internet beschermt. De organisatie pleit er met name voor dat de Franse en Europese wetgeving aangepast wordt aan de basisprincipes van het internet, voornamelijk de vrije circulatie van kennis. La Quadrature du Net is derhalve betrokken bij de oriënterende debatten omtrent onder meer de vrijheid van meningsuiting, het auteursrecht, de regulering van de telecommunicatie en online privacy. La Quadrature wordt gefinancierd door individuele donaties, maar ook door Franse, Europese en internationale NGO's, waaronder de Electric Frontier Foundation, het Open Society Institute en Privacy International. In januari 2017 berichtte La Quadrature dat de jaarlijkse campagne voor het werven van individuele donaties 245.000 euro heeft opgeleverd, een bedrag dat 77% van het jaarlijkse budget van de organisatie voor 2017 dekt. Hiermee wordt gesuggereerd dat het budget voor 2017 circa 320.000 euro beslaat. Nog eens 11% van het budget wordt gedekt door subsidies van andere stichtingen.[43]

Privacy International gaf, in de stukken die het indiende voor het periodieke verslag over Frankrijk dat het VN Mensenrechtencomité op 1 juni 2015[44] uitgaf, al uiting aan haar bezorgdheid over het al te ruime gebruik van elektronische surveillance door de Franse inlichtingendiensten. Privacy International maakt zich zorgen over het feit dat de huidige wetgeving in Frankrijk onvoldoende bescherming biedt tegen inbreuk op het recht op privacy en geeft aan dat deze situatie verergerd is door het wetsvoorstel inzake inlichtingen van 2015,[45] dat als gevolg van de aanslagen op Charlie Hebdo in januari 2015 is ingediend om "te proberen de praktijken die reeds bestaan onder de inlichtingendiensten te legaliseren en de toezichtbevoegdheden te verruimen onder het mom van terrorismebestrijding." Zij schrijven dat "het gebrek aan rechterlijke toestemming en toezicht op surveillance, met name gezien de in het wetsvoorstel beoogde ruime toezichtbevoegdheden, bijzonder zorgwekkend is."

Andere burgerrechtenorganisaties die actief zijn in Frankrijk zijn Amnesty International France, l'Association des services internet communautaires, Cecil, Creis-Terminal,

39 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
40 https://www.legalis.net/jurisprudences/vie-privee/.
41 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
42 https://www.laquadrature.net/.
43 http://www.laquadrature.net/fr/campagne-dons-2016-merci.
44 https://www.privacyinternational.org/sites/default/files/PI%20submission%20France.pdf.
45 LOI n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=9D17CF9469F7DC1FE559D0DC2C940429.tpdila10v_3?cidTexte=JORF-TEXT000030943133&idArticle=&categorieLien=id.

French Data Network, Génération Libre, Les exegetes amateurs, Ligue des droits de l'Homme, en Fédération des fournisseurs d'accès à Internet associatifs. Deze organisaties faciliteren debatten, dragen bij aan openbare raadplegingen, dienen bezwaren in en gaan in beroep tegen sommige wetgeving bij de Franse raad van state of het constitutionele hof. Zij beïnvloeden ook het wetgevingsproces door op nationaal en Europees niveau te lobbyen en te pleiten voor gegevensbescherming bij leden van het parlement. Deze organisaties zijn zeer bekend.[46]

7.2 Beleid

Nationaal beleid, Privacy Impact Assessments

Het algemene beleid inzake gegevensbescherming is vastgelegd in de wet inzake gegevensbescherming (nr. 78-17). Er bestaat een sectorspecifiek beleid voor de gezondheidszorg met betrekking tot archieven, onderzoek en toegang tot documenten.[47] In artikel 34 van de Franse wet inzake wegevensbescherming is de bepaling opgenomen dat de beheerder van persoonsgegevens "*alle zinvolle voorzorgsmaatregelen dient te treffen met betrekking tot de aard van de gegevens en de verwerkingsrisico's, om de veiligheid van de gegevens te waarborgen…*". De beheerders van persoonsgegevens moeten de risico's identificeren die ontstaan naar aanleiding van het verwerken, zodat ze passende maatregelen kunnen treffen om deze risico's te beperken. De CNIL heeft in 2010 een eerste veiligheidshandboek gepubliceerd[48] om mkb-bedrijven en micro-ondernemingen te helpen. Het handboek bevat eenvoudige voorzorgsmaatregelen om de veiligheid omtrent het verwerken van persoonsgegevens te verbeteren. In juni 2012 publiceerde de CNIL een handboek over het beheren van privacyrisico's dat van toepassing is op complexe verwerkingsmethoden of scenario's met een hoog risico.[49]

In 2015 publiceerde de CNIL drie documenten die beheerders van persoonsgegevens kunnen gebruiken bij het uitvoeren van de Privacy Impact Assessments (PIA's): methoden, instrumenten en goede praktijken.[50] Deze documenten vormen een update van het handboek over Privacy Risk Management dat de CNIL in 2012 uitbracht om de beheerders van persoonsgegevens te helpen de risico's die zich voordoen tijdens de verwerking te begrijpen, opdat ze de benodigde en adequate veiligheidscontroles selecteren. Een PIA kan uitgevoerd worden als er een nieuwe wet wordt opgesteld of als er nieuwe vormen van gegevensverwerking worden ontwikkeld, maar PIA's zijn nog niet verplicht. Ze zullen vanaf 25 mei 2018 in bepaalde gevallen wel verplicht worden (als EU-verordening 2016/679 van kracht wordt).[51]

46 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
47 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
48 https://www.cnil.fr/sites/default/files/typo/document/Guide_Security_of_Personal_Data-2010.pdf.
49 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
50 https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual.
51 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.

Privacy en de bescherming van persoonsgegevens in nieuw beleid
De CNIL wordt geraadpleegd inzake wetsvoorstellen en ontwerpdecreten.[52] De CNIL kan ook nieuwe wetgeving voorstellen. Op deze manier spelen de bescherming van privacy- en persoonsgegevens een rol bij de beleidsvorming.[53] De Franse overheid initieerde een onafhankelijke commissie, Conseil National du Numérique, als denktank over de impact van informatisering en innovatie op de maatschappij. De commissie heeft 30 leden, allen vertegenwoordigers uit verschillende segmenten van de maatschappij (overheidsdiensten, particuliere bedrijven, NGO's, onderwijs). De eerste van de belangrijke thema's waar de denktank zich over buigt, is loyaliteit en vrijheid in een gemeenschappelijke digitale ruimte.[54]
Met de uitvoering van artikel 34 van de Franse wet inzake gegevensbescherming kan er gebruik worden gemaakt van het 'Privacy by Design'-beginsel bij het opstellen van nieuwe beleidsmaatregelen en bij de naleving van uitgangspunten als gegevensminimalisering, doelbinding, etc.[55]
De CNIL heeft het initiatief genomen om een netwerk op te richten van privacydeskundigen en belanghebbenden. De CNIL wil dit netwerk gebruiken om analyses die de technologische ontwikkelingen kunnen voorspellen verder te ontwikkelen en nieuwe toepassingen beter te begrijpen en om te kunnen anticiperen op en een beoordeling te kunnen maken van nieuwe belangrijke kwesties op het gebied van gegevensbescherming. Dit wordt weergegeven in het rapport van de CNIL-verkenningscommissie met de naam Privacy Towards 2020.[56]

Maatschappelijk debat
De overheid houdt rekening met de meningen van burgers en bedrijven bij de ontwikkeling van nieuwe beleidsmaatregelen en wetgeving, bijvoorbeeld middels het platform *Republique Numerique*[57] over de wet inzake de digitale republiek (nr. 2016-1321).[58] De overheid reageert ook op vragen van het publiek.[59] De Franse overheid heeft, meer in het algemeen, de hiervoor genoemde *Conseil National du Numérique*,[60] een onafhankelijke commissie met vertegenwoordigers van tal van belanghebbenden, ingesteld om de impact van digitale technologieën op de maatschappij te bespreken.

Voorlichtingscampagnes
De overheid subsidieert projecten die gericht zijn op het creëren van meer bewustzijn onder zowel burgers als bedrijven. De campagnes worden geïnitieerd door de CNIL en

52 Wet inzake gegevensbescherming, artikel 11 paragraaf 4° gewijzigd in Oktober 2016, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460.
53 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
54 https://cnnumerique.fr/.
55 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
56 CNIL-verkenningscommissie, Privacy Towards 2020. IP Innovation & Foresight Reports Nr 1. Beschikbaar op https://www.cnil.fr/sites/default/files/typo/document/CAHIER_IP_EN.pdf.
57 https://www.republique-numerique.fr/.
58 https://www.legifrance.gouv.fr/eli/loi/2016/10/7/ECFI1524250L/jo.
59 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
60 https://cnnumerique.fr/.

worden gefinancierd vanuit de rijksbegroting. Het hierboven genoemde Educnum-platform is een voorbeeld hiervan.[61] Een van de missies van de CNIL is het informeren van betrokkenen (uit hoofde van artikel 11 paragraaf 1° van de wet inzake gegevensbescherming nr. 78-17). De overheid financiert zowel het Conseil National du Numérique (het budget voor 2016 was ca. 91.000 euro) en de CNIL.[62]

7.3 Wet- en regelgeving

Implementatie van de EU-richtlijn

EU-richtlijn 95/46/EC is in nationale wetgeving omgezet middels de Franse wet inzake gegevensbescherming van 6 januari 1978 (Wet nr. 87-17), gewijzigd door wet nr. 2011-334 van 29 maart 2011, richtlijn nr. 2011-1012 van 24 augustus 2011 (de 'Richtlijn'), wet nr. 2013-907 van 11 oktober 2013 en wet nr. 2014-344 van 17 maart 2014.[63]

Uit hoofde van wet nr. 78-17 omvat het verwerken van persoonsgegevens een geheel van automatische handelingen met betrekking tot persoonsgegevens betreffende het verzamelen, registeren, ontwikkelen, wijzigen, opslaan en vernietigen en een geheel van handelingen van dezelfde aard betreffende het gebruik van bestanden of databanken en interconnecties, raadplegingen of communicatie van persoonsgegevens. De wet bepaalt dat elke automatische verwerking van persoonsgegevens namens partijen die niet de staat zijn, overheidsinstanties, territoriale autoriteiten of een particuliere rechtspersoon die een publieke dienst beheert, moeten worden gemeld bij de CNIL alvorens deze ten uitvoer worden gebracht. Er zijn specifieke bepalingen vastgesteld voor gezondheidsgegevens van kinderen. Zo zijn er bijvoorbeeld specifieke procedures voor de bescherming van kinderen en de beheerders van gezondheidsgegevens moeten worden geautoriseerd voor de opslag van de gezondheidsgegevens.[64]

Sectorale wetgeving

Er zijn een aantal wetten en regelgevingen met betrekking tot de bescherming van persoonsgegevens voor specifieke sectoren, waaronder:[65]

- het Franse wetboek van posterijen en elektronische communicatie (artikel L 34 e.v. en artikel R10 e.v.) (voor publieksgerichte online elektronische communicatiediensten);
- het consumentenwetboek (artikel L 223 e.v.) (over telemarketing);
- het consumentenwetboek (artikel L 224-42 tot L 224-4). Deze artikelen worden op 25 maart 2018 van kracht en zullen een algemeen uitgangspunt bevatten dat bepaalt dat consumenten het recht hebben om al hun gegevens terug te halen;

61 https://www.educnum.fr/.
62 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
63 LinkLaters DataProtected https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx.
64 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
65 http://uk.practicallaw.com/6-502-1481.

- het wetboek betreffende de volksgezondheid (artikel L 1110-4 e.v., L 1111-8 e.v., L 1115-1 e.v., L 1122-1 e.v., L 1435-6, L 1460-1 e.v., R 1111-1 e.v.) (over het verwerken van gezondheidsgegevens).[66]
- het wetboek inzake eigendom (artikel L 212-3) (over het bewaren van persoonsgegevens die opgenomen zijn in openbare archieven).

Deze wetgeving heeft betrekking op meer categorieën dan alleen de categorieën gevoelige persoonsgegevens, zoals bijvoorbeeld in het kader van werkgelegenheid.[67]

Zelfregulering en gedragscodes
De CNIL geeft aanbevelingen omtrent goede praktijken en levert kwaliteitslabels.[68] Er bestaan zelfreguleringsinitiatieven, bijvoorbeeld met gedragscodes.[69] De CNIL neemt actief deel aan het programma *Binding Corporate Rules* (BCRs) van de Europese Commissie.[70] De BCRs worden gebruikt door multinationals voor het garanderen van passende waarborgen voor de bescherming van de privacy en de fundamentele rechten en vrijheden van personen in de zin van artikel 26 (2) van EU-richtlijn 95/46/EC voor elke overdracht van persoonsgegevens beschermd onder een Europese wet. Het overzicht van 88 bedrijven waarvoor de BCR-procedure is afgesloten, bevat 28 Franse bedrijven met CNIL als de leidende autoriteit (in vergelijking tot 16 Nederlandse bedrijven, 8 Duitse bedrijven, 22 Engelse bedrijven en 1 Iers bedrijf).

7.4 Implementatie

Sommige bedrijven gebruiken andere middelen om gegevensbescherming toe te passen, zoals bijvoorbeeld privacyzegels,[71] certificeringen of gedragscodes.[72] In januari 2015 publiceerde de CNIL een standaard om te definiëren wat de aansprakelijkheid met betrekking tot privacy in de praktijk betekent: het CNIL-zegel *Gouvernance Informatique et Libertés.*[73] Deze zou wellicht kunnen gelden als voorbeeld voor een Europese standaard.[74] Het programma omtrent privacyzegels wordt gecoördineerd door de CNIL. Om een privacyzegel te krijgen, moeten bedrijven voldoen aan 25 cumulatieve standaarden. Deze standaarden zijn verdeeld in 3 verschillende categorieën:
- de interne organisatie met betrekking tot het beheer van persoonsgegevens;

66 https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031912641#LEGIARTI000031916294.
67 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
68 https://www.cnil.fr/fr/les-labels-cnil.
69 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
70 http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm.
71 https://www.cnil.fr/fr/les-labels-cnil, https://www.cnil.fr/en/cnil-privacy-seal-privacy-governance-procedures, https://www.cnil.fr/sites/default/files/typo/document/CNIL_Privacy_Seal-Governance-EN.pdf.
72 Antwoorden van Emmanuel Laforet ten behoeve van ons onderzoek.
73 https://www.cnil.fr/fr/un-nouveau-label-cnil-gouvernance-informatique-et-libertes.
74 http://www.hldataprotection.com/2015/01/articles/international-eu-privacy/new-cnil-accountability-standard-may-become-european-model/.

- de methoden om te verifiëren of aan de wet voldaan wordt;
- de afhandeling van klachten en incidenten.

Voor bedrijven, instanties, verenigingen of rechtsgebiedenvormt het programma een passend ethisch en wettelijk kader en hiermee wordt de bereidheid van de organisatie aangetoond om te innoveren en om persoonsgegevens op een verantwoorde wijze te verwerken. Daarnaast bereiden deze privacyzegels organisaties voor op de toekomstige Algemene Verordening Gegevensverwerking (AVG) van de EU, met name middels de introductie van het begrip aansprakelijkheid.[75]
In juni 2016 lanceerde de CNIL ook het initiatief voor een openbare raadpleging in de nieuwe EU-regelgeving inzake de Algemene Verordening Gegevensbescherming (AVG) voor professionals. Het initiatief had ten doel concrete vragen, interpretatieproblemen en voorbeelden van best practices te verzamelen die opgeroepen werden door het lezen van de tekst. De bijdragen zijn nuttig voor de Artikel 29 Werkgroep (WG29), die operationele richtlijnen zal aannemen met betrekking tot de verschillende voor raadpleging voorgelegde onderwerpen.[76]

Privacyfunctionarissen
De CNIL staat toe dat organisaties een privacyfunctionaris (*Correspondants Informatique et Libertés (CIL)* aanstellen op facultatieve basis. Hiermee kan een vrijstelling van de wettelijke meldplicht worden verkregen. De privacyfunctionaris is verantwoordelijk voor het nakomen van de verplichtingen zoals voorzien in de wet inzake gegevensbescherming en voor het bijhouden van een verwerkingsregister (behalve indien er processen mee gemoeid zijn waarvoor toestemming of een advies vereist is, waaronder processen waarbij een gegevensstroom buiten de EU wordt overwogen). Volgens het jaarverslag van de CNIL van 2015 hebben ongeveer 16.400 houders van persoonsgegevens een privacyfunctionaris aangesteld.[77]
De privacyfunctionaris hoeft niet te beschikken over door de wet vereiste specifieke vaardigheden, behalve dat de persoon gekwalificeerd moet zijn voor de baan. Als de organisatie over minder dan 50 personen beschikt die zich bezighouden met gegevensverwerking, mag het een externe privacyfunctionaris zijn, anders moet het bedrijf een privacyfunctionaris aannemen.[78] De verantwoordelijkheden van de privacyfunctionaris die voorgeschreven worden door de wet zijn:
i het opstellen en bijhouden van een overzicht van de gegevensverwerkingsactiviteiten van de organisatie waar hij/zij door aangenomen is;
ii waarborgen van de naleving van de wet inzake gegevensverwerking;
iii het adviseren van de organisatie, met name over nieuwe gegevensverwerkingsactiviteiten die toegevoegd moeten worden aan dat overzicht alvorens ze worden toegepast;

75 https://www.cnil.fr/en/cnil-privacy-seal-privacy-governance-procedure.
76 https://www.cnil.fr/sites/default/files/atoms/files/resultats_de_la_consultation_publique_reglement_0.pdf.
77 https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx.
78 https://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/france.

iv het ontvangen van aanvragen en klachten van betrokkenen die betrekking hebben op deze gegevensverwerkingsactiviteiten;
v het indienen van een jaarverslag over zijn/haar activiteiten bij de organisatie en het beschikbaar stellen van dit verslag aan de CNIL.

In de praktijk bestaan de standaardtaken verder uit: het ontwikkelen van interne beleidsmaatregelen en procedures, het uitvoeren van nalevingscontroles, het voorbereiden en verstrekken van personeelstraining, het controleren van contractuele bepalingen betreffende gegevensbescherming, advies uitbrengen over een passende melding aan de betrokkenen, het bij CNIL aanmelden van de gegevensverwerkingsactiviteiten die eerst goedgekeurd moeten worden, en binnen de hele organisatie bewustzijn creëren, in algemene zin, met betrekking tot gegevensbeschermingskwesties.[79] De CNIL moet worden geïnformeerd wanneer er een privacyfunctionaris wordt aangesteld.[80]

Beveiligingsmaatregelen
De CNIL verstrekt via haar website een aantal richtlijnen en adviezen voor burgers en bedrijven over wetten inzake gegevensbescherming, uitgangspunten en manieren om met de wetten om te gaan. Voor bedrijven is er bijvoorbeeld een apart gedeelte op de website dat gaat over 'Les Outils de la Conformité' (compliance-instrumenten).[81] Hier wordt beschreven hoe bedrijven een privacyfunctionaris (CIL in het Frans) kunnen aanstellen om "gegevensrisico's te verkleinen en investeringen te maximaliseren".[82] Een belangrijke taak van de privacyfunctionaris bestaat uit het adviseren over gegevensbeschermingsmaatregelen en waarschuwen voor gegevensbeschermingsrisico's bij de ontwikkeling van nieuwe diensten. De eerdergenoemde privacyzegels die uitgegeven worden door de CNIL vormen ook een belangrijk instrument voor het stimuleren en ondersteunen van de naleving van de veiligheidsnormen.[83]

Transparantie
Tijdens een openbare toespraak noemde Sophie Nerbonne, hoofd compliance bij CNIL, (het gebrek aan) transparantie als een van de grote problemen betreffende het Internet of Things. Begin 2016 heeft de CNIL een waarschuwing doen uitgaan richting een bedrijf genaamd PROFILS SENIORS over een gebrek aan transparantie.[84] Dit bedrijf probeerde een databank op te stellen met gegevens over senioren met als doel deze te verhuren aan derden voor e-commercedoeleinden. In 2015 werden er tijdens een onderzoek een aantal overtredingen van de wet 'Informatique et Liberté' ontdekt, nadat er in 2013 een klacht was ingediend.

79 https://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/france.
80 https://www.iclg.co.uk/practice-areas/data-protection/data-protection-2016/france.
81 https://www.cnil.fr/fr/les-outils-de-la-conformite.
82 https://www.cnil.fr/fr/le-role-du-cil-et-ses-benefices.
83 https://www.cnil.fr/en/privacy-seals.
84 https://www.cnil.fr/fr/profils-seniors-sanctionne-par-la-cnil-pour-manque-de-transparence.

7.5 Toezicht en handhaving

Toezichthouders

Middels de Franse wet inzake gegevensbescherming nr. 78-17 van 6 januari 1978 over informatietechnologie, gegevensbestanden en burgerlijke vrijheden werd de Franse toezichthouder CNIL (Commission Nationale de l'Informatique et des Libertés) opgericht na een politiek debat in het nationaal parlement. De CNIL heeft sinds 2015 in totaal 192 medewerkers. Het budget voor 2016 beslaat bijna 19 miljoen euro.[85]

De leden van de CNIL houden een keer per week een plenaire vergadering op basis van een agenda die vooraf door de voorzitter is vastgesteld. Het grootste gedeelte van deze vergaderingen wordt gewijd aan de beoordeling van wetsvoorstellen en ontwerpdecreten die de overheid heeft ingediend voor een officieel advies van de CNIL. Daarnaast geeft de CNIL toestemming voor het verwerken van gevoelige gegevens, met inbegrip van, maar niet beperkt tot, die partijen die een aanvraag indienen voor het gebruik van biometrische gegevens. De CNIL analyseert ook de gevolgen van nieuwe technologieën op het privéleven van burgers.[86]

De CNIL was een van de toezichthouders in circa twintig landen die de zogenaamde Privacy Sweep hebben geïnitieerd, een evenement dat gecoördineerd werd door het Global Privacy Enforcement Network.[87] Tijdens dit jaarlijkse evenement wordt een aantal groepen samengesteld volgens een thema,[88] maar de CNIL werkt in het algemeen met alle beheerders van persoonsgegevens, gegevensverwerkers en betrokkenen.[89]

Taken en bevoegdheden

De rol van de CNIL wordt omschreven in artikel 11 van de Franse wet inzake gegevensbescherming. De CNIL geeft advies over voorgestelde wetgeving en decreten en ondersteunt burgers. Verder bevordert de CNIL de discussie tussen de autoriteiten en bedrijven onder toezicht. De autoriteiten stellen een onderzoek in als ze dat willen, normaal gesproken nadat ze een klacht hebben ontvangen van een burger of daarover hebben gelezen in de media. De CNIL legt bijvoorbeeld sancties op in het geval dat een datalek gevolgen heeft voor heel veel burgers, gevoelige data onjuist gebruikt worden of als de beheerder van de persoonsgegevens niet meewerkt na een formele kennisgeving.[90]

De CNIL geeft in haar onderzoeksprogramma voor 2015 aan dat ze het voornemen heeft om circa 550 onderzoeken uit te voeren, zowel op locatie als online. De prioriteit ligt voor deze onderzoeken bij contactloos betalen, het Internet of Things voor de gezondheidzorg en het achteraf inspecteren van bedrijven die toestemming hebben gekregen voor hun BCRs.[91] De nadruk van het programma ligt op genetwerkte auto's,

85 https://www.data.gouv.fr/fr/datasets/budget-de-la-cnil-1/.
86 Antwoorden van Emmanuel Laforet, uit ons onderzoek.
87 https://www.privacyenforcement.net/.
88 https://www.cnil.fr/fr/internet-sweep-day-2016-comment-les-objets-connectes-du-quotidien-impactent-la-vie-privee.
89 Antwoorden van Emmanuel Laforet naar aanleiding van ons onderzoek.
90 Antwoorden van Emmanuel Laforet naar aanleiding van ons onderzoek.
91 LinkLaters bron https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx.

smart cities en de commerciële exploitatie van persoonsgegevens door culturele apparaten zoals e-books, digitale muziekspelers of video-on-demand.
De CNIL heeft de bevoegdheid om handhavend op te treden in Frankrijk. Ze heeft het vermogen om bedrijven te beboeten en de boetes die opgelegd zijn door de CNIL kunnen openbaar worden gemaakt (normaal gesproken via de website) en in kranten worden gepubliceerd op kosten van de nalatige beheerder van de persoonsgegevens. Strafrechtelijke vervolgingen voor een misdrijf worden aan de Franse rechtbank voorgelegd, die bevoegd is om strafrechtelijke boetes en/of gevangenisstraffen op te leggen.[92]

Gebruik van bevoegdheden
In 2014 ontving de CNIL 5.825 klachten met betrekking tot schendingen van de wet inzake gegevensbescherming.[93] Er vonden 421 onderzoeken plaats, die leidden tot 62 formele meldingen (waarvan er 4 openbaar werden gemaakt), 7 waarschuwingen, 18 sancties (waaronder 8 financiële sancties, waarvan er 7 openbaar werden gemaakt).[94]
In 2014 resulteerde 68% van de formele meldingen tot naleving, waarna het onderzoek werd gesloten. Slechts 3 procedures leidden tot een decharge.[95]
In januari 2014 legde de CNIL Google een boete op van 150.000 euro inzake Google's samengevoegde privacybeleid dat 60 van haar diensten omvatte, voor schending van de regels voor het verstrekken van eerlijke verwerkingsinformatie, het verkrijgen van geldige toestemming voor cookies, bewaartermijnen en het samenvoegen van gebruikersgegevens verzameld door al Google's diensten. In augustus 2014 nam de CNIL strafmaatregelen tegen een Frans telecombedrijf voor een datalek dat circa een miljoen klanten trof en dat veroorzaakt werd door een tijdelijke technische storing van een opdrachtnemer. Ondanks dat het lek vrijwillig openbaar werd gemaakt, kreeg het bedrijf een waarschuwing van CNIL.
In 2014 vonden er 333 controles op locatie plaats (88 gericht op CCTV-systemen), waarvan 58 online controles. Door de wet inzake gegevensbescherming aan te passen, heeft de CNIL middels de nieuwe wet inzake consumptie van 17 maart 2014 inderdaad de beschikking over nieuwe onderzoeksmiddelen. Nu is de CNIL uitdrukkelijk bevoegd om online onderzoeken te doen en bijvoorbeeld gegevens van websites te verzamelen, mits deze vrij toegankelijk zijn of toegankelijk worden gemaakt door bijvoorbeeld onvoorzichtigheid, nalatigheid of tussenkomst van een derde partij. Sommige strafrechtelijke geschillen worden geïnitieerd door een overdracht van de CNIL aan de klager (op basis van artikel 11.2° e of Wet nr. 78-17).[96] De CNIL ontving in 2015 in totaal 7.908 klachten.[97]

Reputatie
De toezichthouder (de CNIL) is bekend bij het publiek. Bedrijven werken zowel op nationaal als op Europees niveau goed samen met de CNIL, aangezien de CNIL voor-

92 LinkLaters bron https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx.
93 LinkLaters bron https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx.
94 LinkLaters bron https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx.
95 LinkLaters bron https://clientsites.linklaters.com/Clients/dataprotected/Pages/France.aspx.
96 Antwoorden van Emmanuel Laforet naar aanleiding van ons onderzoek.
97 Antwoorden van Emmanuel Laforet naar aanleiding van ons onderzoek.

zitter is van de Artikel 29 Werkgroep.[98] Een aantal bedrijven probeert door gebruikmaking van privacyzegels,[99] certificeringen of gedragscodes toegevoegde waarde te leveren in hun dienstverlening.[100]

98 Antwoorden van Emmanuel Laforet naar aanleiding van ons onderzoek.
99 https://www.cnil.fr/fr/les-labels-cnil.
100 Antwoorden van Emmanuel Laforet naar aanleiding van ons onderzoek.

8. Roemenië

8.1 Algemene situatie

Roemenië is opgenomen in dit onderzoek als een Oost-Europees land dat geen lange geschiedenis kent op het gebied van de bescherming van privacy en persoonsgegevens. Relatief recent, in 2007, is Roemenië toegetreden tot de Europese Unie. Het recht op privacy bestaat al vanaf 1976 in Roemenië, omdat het land het Internationale Verdrag inzake Politieke en Burgerrechten (IVBPR), dat in artikel 17 een recht op privacy bevat, heeft geratificeerd. Gedurende het Sovjettijdperk werd dit recht op privacy echter regelmatig geschonden door de veiligheidsdiensten.[1] Roemenië heeft ook de Algemene Verklaring van de Rechten van de Mens ondertekend. Roemenië neemt een monistische houding aan ten opzichte van het internationaal recht, wat inhoudt dat bepalingen in internationale verdragen direct van toepassing zijn in de nationale wetgeving, zonder dat verdere omzetting in nationaal recht nodig is.
Na het uiteenvallen van de Sovjet-Unie en het Warschaupakt in 1989 werden grote delen van de communistische grondwet opgeschort en werd er in 1991 een nieuwe grondwet aangenomen in Roemenië, waarin voor de eerste keer een recht op privacy werd opgenomen (in artikel 26). Het doel van Roemenië destijds was om toe te treden tot de Europese Unie en daarom werden de EU-richtlijnen actief toegepast. De EU-richtlijn inzake de bescherming van persoonsgegevens (95/46/EC) stamt uit 1995 en werd nauwgezet gevolgd bij het omzetten in nationale wetgeving voor gegevensbescherming (zie paragraaf 8.3). Aangezien Roemenië geen lange geschiedenis kent op het gebied van de bescherming van privacy en persoonsgegevens, bestond er geen nationale wet inzake gegevensbescherming die aangepast moest worden en bestond er dus de mogelijkheid om een geheel nieuw wettelijk kader op te stellen voor de bescherming van persoonsgegevens.
In bestaand onderzoek (zie hoofdstuk 1) wordt Roemenië aangeduid als een van de minst privacygerichte landen onder de EU-lidstaten. Roemenen zijn weinig gevoelig voor het prijsgeven van persoonlijke gegevens en hebben een lage digitale betrokkenheid.[2]

1 Manolea, B. (2007), Institutioneel kader voor de bescherming van persoonsgegevens in Roemenië, p. 1. Zie https://www.apti.ro/DataProtection_ro.pdf.
2 Consent Doelstelling 13.3, p. 44.

Internetgebruik

Roemenië heeft 22 miljoen inwoners, waarvan circa 9 miljoen mensen toegang tot internetdiensten hebben. Circa 2,6 miljoen inwoners hebben toegang tot breedbandinternetdiensten.[3] Vergeleken met het gemiddelde van de EU lijken Roemenen zeer actief op het internet en zijn ze relatief wegwijs met deze technologie. 59% van de Roemenen gebruikt bijvoorbeeld minstens een keer per week sociale media.[4] Verder maakt 52% minstens een keer per week gebruik van instant messaging of chatsites.[5] 83% van de Roemenen bekijkt meer dan een keer per week het nieuws op internet (het EU-gemiddelde is 72%).[6] Roemenen behoren ook tot de gebruikers die het vaakst muziek luisteren en foto's en video's bekijken via internet. Het gebruik van het internet voor online telefoon- en videogesprekken is gelijk aan het EU-gemiddelde.[7] Circa 40% speelt minstens een keer per week online spelletjes (EU-gemiddelde is 25%).

De Roemenen zijn echter terughoudend met het gebruik van sommige online diensten. 70% van de Roemenen koopt bijvoorbeeld online (vergeleken met het EU-gemiddelde van 87%).[8] 48% koopt nooit online, vergeleken met een EU-gemiddelde van 24%.[9] Daarnaast maakt 65% van de Roemenen ook nooit gebruik van online bankieren. Dit percentage is aanzienlijk hoger dan het EU-gemiddelde van 35%.[10]

(Gevoel van) controle

Desgevraagd blijkt dat Roemenen over het algemeen niet het gevoel hebben dat ze controle hebben over de informatie die ze online verstrekken. Een recent onderzoek heeft uitgewezen dat 14% het idee heeft dat ze controle hebben over de informatie, 53% heeft het idee dat ze slechts gedeeltelijk controle hebben en 30% heeft het idee dat ze helemaal geen controle hebben.[11] Dit komt nauw overeen met de EU-gemiddelden die respectievelijk 15%, 50% en 31% zijn. Tegelijkertijd lijken niet alle Roemenen erg bezorgd te zijn over dit gebrek aan controle. Circa 56% van de mensen geeft aan bezorgd te zijn, in vergelijking tot het EU-gemiddelde van 67%.[12]

Iets minder dan de helft van alle Roemenen (48%) beschouwt het geven van persoonsgegevens als een toenemend deel van het moderne leven. Dit is het laagste percentage in de EU (het EU-gemiddelde is 71%).[13] Overigens lijkt dit percentage nog te stijgen in Roemenië, terwijl het gemiddelde in de EU juist aan het dalen is. Circa 33% geeft aan het verstrekken van persoonsgegevens geen groot probleem te vinden.[14] In antwoord op de vraag of men zich prettig voelt bij het gebruik van persoonsgegevens voor gepersonaliseerde advertenties en diensten, geeft 6% aan zich daar heel prettig bij te

3 Consent Doelstelling D2.1, p. 46.
4 Eurobarometer 431 (2015), p. 109.
5 Eurobarometer 431 (2015), p. 109.
6 Eurobarometer 437 (2016).
7 Eurobarometer 431 (2015), p. 111.
8 Consent Landenrapport Roemenië (2012), p. 3.
9 Eurobarometer 431 (2015), p. 111.
10 Eurobarometer 431 (2015), p. 110.
11 Eurobarometer 431 (2015), p. 10.
12 Eurobarometer 431 (2015), p. 13.
13 Eurobarometer 431 (2015), p. 29.
14 Eurobarometer 431 (2015), p. 32.

voelen, 38% geeft aan zich daar redelijk prettig bij te voelen, 36% voelt zich daar redelijk onprettig bij en 14% voelt zich daar heel onprettig bij.[15]

Bewustzijn

Over het algemeen tonen Roemenen met betrekking tot het gebruik van persoonsgegevens door webeigenaren een mate van bewustzijn die vergelijkbaar is met de rest van de EU.[16] Terwijl de Roemenen in de EU echter de hoogste mate van bewustzijn tonen met betrekking tot het gebruik van persoonsgegevens door eigenaren van websites om via e-mail contact op te nemen met gebruikers (Roemenië 90%, het EU-gemiddelde is 87%), onderscheidt het land zich ook door een vergelijkbaar hoog acceptatieniveau (85%). Vergelijkbare relaties kunnen worden waargenomen bij het bewustzijn omtrent en de acceptatie van het gebruik van persoonsgegevens om advertenties en de inhoud ervan toe te spitsen op de persoon. Hoewel er enige mate van 'balans' lijkt te zijn tussen het bewustzijn en de acceptatie van de gebruiker met betrekking tot deze praktijken, is de mate van acceptatie van zorgvuldige informatieverzameling, de verkoop daarvan of het beschikbaar maken van deze informatie aan anderen, echter beduidend lager. Dergelijke praktijken worden voor een groot deel als onaanvaardbaar beschouwd en een commerciële uitwisseling kan dan ook op weinig acceptatie rekening binnen de gehele EU. Op dit gebied tonen de Roemenen een mate van non-acceptatie die vergelijkbaar is met het EU-gemiddelde (Roemenië 75%, het EU-gemiddelde is 74%). Het aantal Roemenen dat aangeeft daadwerkelijk ervaring te hebben met een schending van de privacy is even laag. De Roemenen scoren hier 3,01 (het EU-gemiddelde is 2,89) op een schaal van 7 (1 = nooit, 7 = heel vaak).[17]

Wat betreft ervaringen met privacybeleidsmaatregelen is het percentage Roemenen dat ooit besloot om geen gebruik te maken van een website wegens onvrede met het privacybeleid van die website gelijk aan het EU-gemiddelde (beide 47%) en circa de helft van de Roemeense bevolking leest nooit of vrijwel nooit de algemene voorwaarden van de website (49%) of het privacybeleid (55%).[18] Wanneer ze het privacybeleid wel lezen, dan lezen de Roemenen, net als andere EU-burgers, vrijwel nooit de gehele tekst (Roemenië 15%, in vergelijking tot een EU-gemiddelde van 11%), hoewel zij er vrij zeker van zijn dat – als ze het privacybeleid lezen – ze de tekst voor het merendeel of volledig kunnen begrijpen (Roemenië 76%, in vergelijking tot een EU-gemiddelde van 64%).

Slechts 22% van de Roemenen weet van het bestaan van de Roemeense toezichthouder op het gebied van de bescherming van persoonsgegevens. Dit is een van de laagste percentages in de gehele EU (het gemiddelde is 37%).[19]

15 Eurobarometer 431 (2015), p. 40.
16 Consent Landenrapport Roemenië(2012), p. 4.
17 Consent Landenrapport Roemenië (2012), p. 4.
18 Consent Landenrapport Roemenië (2012), p. 4.
19 Eurobarometer 431 (2015), p. 52.

Vertrouwen

Het percentage Roemenen dat hun persoonsgegevens toevertrouwt aan overheidsinstanties en particuliere bedrijven is 55%. Dit percentage ligt dicht bij het EU-gemiddelde (51%). Als we echter wat beter kijken naar het vertrouwen, dan hebben Roemenen aanzienlijk minder vertrouwen in specifieke sectoren, zoals de gezondheidssector en de farmaceutische sector (58% in vergelijking tot een EU-gemiddelde van 56%). Het vertrouwen in winkels ligt met 39% dicht bij het EU-gemiddelde (40%).[20] Hetzelfde geldt voor online bedrijven als zoekmachines (24% in vergelijking tot het EU-gemiddelde van 24%). Het vertrouwen in telecommunicatiebedrijven en internetproviders is 41%, een percentage dat beduidend hoger ligt dan het EU-gemiddelde (33%).

De manier waarop de Roemenen aankijken tegen de algemene risico's met betrekking tot het verstrekken van persoonsgegevens op socialemediawebsites, lijkt gelijk te zijn aan het totale EU-gemiddelde.[21] Dit geldt ook voor de specifieke risico's die daarmee in verband worden gebracht, zoals informatie die door eigenaren van websites gebruikt of gedeeld wordt zonder dat de gebruiker daarvan weet of daar toestemming voor heeft gegeven en informatie die gebruikt wordt voor het sturen van ongewenste commerciële aanbiedingen (spam). Wat betreft de manier waarop aangekeken wordt tegen de risico's voor de persoonlijke veiligheid, de reputatie die geschaad wordt en het risico om het slachtoffer te worden van fraude, scoort Roemenië aanzienlijk hoger dan het EU-gemiddelde (de kans om slachtoffer van fraude te worden, wordt in Roemenië gepercipieerd als 54% tegenover een EU-gemiddelde van 32%). Deze hoge mate van risicoperceptie kan het resultaat zijn van recente rapporten over hackers en gevallen van phishing, waarvan enkele gevallen zelfs afkomstig waren uit Roemenië.

Beschermingsmaatregelen

Het percentage Roemenen dat de privacyinstellingen van hun socialemediaprofielen heeft getracht te wijzigen bedraagt 51% (EU-gemiddelde 57%).[22] Roemenen vinden het vrij makkelijk om deze instellingen aan te passen (86%, in vergelijking tot het EU-gemiddelde van 64%).[23] Diegenen die de privacyinstellingen niet aanpassen, geven aan er voldoende op te vertrouwen dat de website passende privacyinstellingen hanteert (17%), niet te weten hoe ze deze instellingen aan moeten passen (16%), zich geen zorgen te maken over hun online persoonsgegevens (25%), geen tijd te hebben om zich te verdiepen in de mogelijkheden (27%) of niet te weten dat ze de instellingen aan kunnen passen (13%).[24] Vergelijkbare resultaten zijn terug te zien in het onderzoek van CONSENT, waarin wordt aangetoond dat om hun privacy te bewaken, 43% van de Roemenen de privacyinstellingen van hun persoonlijke profielen op socialemediawebsites vaak of altijd verandert (EU-gemiddelde 54%). 79% (EU-gemiddelde 80%) van degenen die de privacyinstellingen veranderen, geeft aan deze privacyinstellingen strenger in te stellen, zodat anderen minder informatie over hen kunnen zien.[25]

20 Eurobarometer 431 (2015), p. 66.
21 Consent Landenrapport Roemenië (2012), p. 4.
22 Eurobarometer 431 (2015), p. 92.
23 Eurobarometer 431 (2015), p. 95.
24 Eurobarometer 431 (2015), p. 98.
25 Consent Landenrapport Roemenië (2012), p. 4.

Wat betreft specifieke technische maatregelen die worden genomen om persoonlijke veiligheid op internet te behouden of verhogen, worden sommige maatregelen (zoals pop-upblokkeringen van windows, aanvinken van het opt-in/opt-outvakje, het blokkeren van e-mails) vaker toegepast dan andere (zoals controleren op spyware, het wissen van de browsergeschiedenis). Daarbij liggen de resultaten van de Roemenen meestal lager dan het totale EU-gemiddelde.[26] Het lijkt alsof het vermogen om technische maatregelen te nemen om de persoonlijke veiligheid op het internet te behouden of te verhogen, de hoge gebruiksfrequentie van het internet en sociale media niet bij kan benen.[27] De mate van digitale betrokkenheid is aanzienlijk groter dan de neiging om maatregelen te nemen om de persoonlijke veiligheid te beschermen.[28] Daarnaast is de neiging om persoonlijke gegevens te verstrekken veel sterker dan de neiging om maatregelen te nemen om de persoonlijke veiligheid te beschermen.[29]

Nationale politiek

De bescherming van persoonsgegevens speelt geen belangrijke rol in de nationale of partijpolitiek. Wanneer de huidige programma's van de politieke partijen worden bekeken, wordt de bescherming van privacy en gegevens niet of nauwelijks genoemd. Wanneer wetsvoorstellen worden besproken, kan privacy een punt zijn dat aan de orde wordt gesteld. Een typisch voorbeeld hiervan deed zich voor toen de liberale partij een voorstel voor een cyberbeveiligingswet indiende bij het Roemeense constitutionele hof (RCH).[30] Dergelijke parlementaire debatten of openbare discussies ontstaan meestal als gevolg van wetsvoorstellen met betrekking tot de openbare of nationale veiligheid. Zulke debatten/discussies beginnen meestal doordat er een sterk pro-veiligheidsstandpunt wordt ingenomen in het parlement of door de regering, die een reactie teweegbrengt om te stoppen met de uitbreiding van de beschermingsmaatregelen.

In de veiligheidssector wordt regelgeving vaak als enige mogelijkheid gezien, maar dit is ook gebruikelijk in andere sectoren in Roemenië, waar nauwgezette regelgeving eveneens vaak verkozen wordt boven zachte wetgeving en andere benaderingen. Roemenië kent geen traditie van zelfregulering. Zelfregulering wordt door politici (en soms ook door de bevolking) gezien als de 'doe niets'-benadering, hetgeen als (te) passief wordt beschouwd. Er vindt geen echte dialoog plaats tussen de civil society en de politieke partijen over de problemen omtrent de bescherming van privacy en persoonsgegevens. Evenmin vindt er een dialoog plaats tussen de toezichthouder en de politieke partijen of tussen de toezichthouder en overheidsinstanties. Daarnaast wordt het advies van de toezichthouder soms genegeerd, vooral bij gevoelige kwesties zoals grootschalige surveillancemaatregelen. In 2016 waren er minstens drie wetsvoorstellen over nieuwe

26 Consent Landenrapport Roemenië (2012), p. 3.
27 Consent Landenrapport Roemenië (2012), p. 39.
28 Consent Doelstelling 13.3, p. 52.
29 Consent Doelstelling 13.3, p. 53.
30 Zie https://privacy.apti.ro/2015/01/29/romanian-cybersecurity-law-sent-to-the-constitutional-court/. Het wetsontwerp werd in januari 2015 ongrondwettelijk verklaard; https://pri-vacy.apti.ro/2015/01/29/icing-on-the-cake-romanian-cybersecurity-law-unconstitutional/.

veiligheidsvereisten waarin de argumenten van de toezichthouder en voorgaande besluiten van het Roemeense constitutionele hof werden genegeerd.[31]

Media-aandacht

De media besteden niet vaak aandacht aan privacy- en gegevensbeschermingskwesties. Er vindt geen nationaal debat over privacy en gegevensbescherming plaats. Dit is deels te wijten aan een aantal structurele problemen binnen het Roemeense mediabestel.[32] Daardoor lijkt het alsof de media enkel geïnteresseerd zijn in de tabloid- of sensatiekant van privacyverhalen in plaats van de analyse, het onderzoek of debat omtrent deze kwesties. Ondanks het feit dat met name de sensatiekant van privacyverhalen wordt belicht, hebben de algemene media de afgelopen vijf jaar met name de wetten gevolgd die problemen kunnen opleveren voor de privacy of die zijn aangevochten in het Roemeense constitutionele hof.[33] Op het internet is een grote verscheidenheid aan nieuwsartikelen te vinden, maar slechts een paar van deze artikelen gaan over gegevensbeschermingskwesties. Er lijkt een gebrek aan bewustzijn of interesse te zijn bij journalisten met betrekking tot gegevensbescherming of privacykwesties, zelfs als deze kwesties met hun eigen beroep te maken hebben, bijvoorbeeld wanneer het gaat over de vertrouwelijkheid van hun bronnen.

Datalekken

De afgelopen jaren zijn er geen belangrijke datalekken openbaar gemaakt of in het nieuws geweest. Voor het CONSENT-onderzoek werden de belangrijkse socialemediawebsites in Roemenië onderzocht. Geen van deze sites was betrokken bij juridische conflicten met betrekking tot de bescherming van de consument en diens persoonsgegevens.[34] Er waren echter verschillende privacyincidenten die veel media-aandracht kregen:

De Roemeense fiscale autoriteit ANAF publiceerde op 24 mei 2016 een overzicht met 187.000 particulieren (met volledige gegevens, inclusief naam, adres en burgerservicenummer) die een schuld van meer dan 1.500 RON (circa 333 euro) aan de staat hadden, ongeacht of zij dit bedrag voor de rechtbank hadden aangevochten.[35] Het overzicht werd als 'open data' gepubliceerd op het Roemeense open data-portal. De ANAF kreeg een boete van 16.000 RON (circa 3.500 euro) voor het overtreden van de gegevensbeschermingswetten, maar werd niet verzocht om de gegevens van het internet te halen.

---

31 Inlichtingendiensten krijgen meer toezichtbevoegdheden in Roemenië, zie https://edri.org/intelligence-organisations-get-more-surveillance-powers-in-romania/.

32 Zie ActiveWatch FreeEx report 2015-2016 voor meer details. De organisatie benadrukt de belangrijkste problemen van de Roemeense media: "Overmatige politisering van de media, corrupte financieringsmechanismen, een editorial beleid dat ondergeschikt is aan de belangen van de eigenaar en infiltratie van het personeel door inlichtingendiensten, hebben ertoe geleid dat de media zijn omgevormd tot een politiek propogandamiddel. Dit is vooral duidelijk zichtbaar in verkiezingsjaren." http://activewatch.ro/en/freeex/publications/freeex-report-2015-2016.

33 In 2011-2015 werden vier belangrijke wetten onconstitutioneel verklaard op grond van het recht op privacy – twee wetten inzake het bewaren van gegevens, een wet inzake de verplichte registratie van pre-paid SIM-kaarten en het WiFi-verkeer van internetgebruikers, en de ander inzake cyberveiligheid.

34 Consent Doelstelling 2.1, Bijlage 1.

35 Zie nieuws https://republica.ro/anaf-a-fost-amendata-cu-16-000-de-lei-pentru-lista-rusinii.

ANAF vocht de boete aan in de rechtbank. In september 2016 werd er een tweede overzicht gepubliceerd, met striktere technische beperkingen.[36] Deze zaak kreeg veel media-aandacht en er werd veel over gesproken.
De Roemeense inlichtingendienst SRI kreeg in juli 2016 EU-gelden toegewezen voor een project genaamd SII Analytics, voor de aanschaf van software en hardware voor "het consolideren en waarborgen van de e-overheidsinteroperabiliteit tussen openbare informatiesystemen". Het project lijkt erop gericht alle belangrijke databanken van de staat te verzamelen (bijvoorbeeld burger- en bedrijfsregisters, gegevens van de gezondheidskaart, fiscale gegevens) binnen het speelveld van SRI. De gegevens zullen op één groot systeem worden opgeslagen, waardoor andere openbare instanties mogelijk ongelimiteerde en ongerechtvaardigde toegang tot de verzamelde persoonsgegevens zouden hebben. Het project is er ook op gericht om gegevensverzamelingen van alle belangrijke openbare instanties samen te voegen en geavanceerde zoekopdrachten toe te staan om onderzoeken naar beschikbare informatie over burgers en inwoners mogelijk te maken. Daarnaast bevat de projectomschrijving ook een hoofdstuk over gedragsanalyses. Het systeem zou gecompliceerde analyses mogelijk maken door verbanden tussen databanken te leggen en deze te combineren met andere informatie.[37]
Het project heeft enige aandacht gekregen van de media, maar kreeg met name veel aandacht van NGO's in Roemenië, maar ook daarbuiten.
Er zijn regelmatig beschuldigingen van illegale afluisterpraktijken of grootschalige surveillance van geheime diensten die de aandacht van de media trekken, hoewel opgemerkt moet worden dat deze aandacht vooral afkomstig is van media waarvan de eigenaren in de gevangenis zitten of naar wie een strafrechtelijk onderzoek is ingesteld. Hoewel er voorwaarden bestaan voor geheime afluistersystemen die technisch gezien door de geheime diensten worden beheerd, schijnt de bevolking de werking van deze systemen in de praktijk over het algemeen te wantrouwen. Naar het schijnt is het aantal afluisterpraktijken op grond van 'de nationale veiligheid' twee keer zo groot als dat van de FBI[38] en vele van deze afluisterpraktijken lekken uit naar de pers al voordat de rechtszaak begonnen is. Voor dit laatste probleem is Roemenië al een aantal keren veroordeeld door het EHRM.[39]
Een aantal projecten en wetsvoorstellen met betrekking tot biometrische en elektronische documenten, zoals het biometrische paspoort, de elektronische ID-kaart (nog niet ingevoerd) en het elektronische patiëntendossier, hebben de laatste jaren veel publiciteit getrokken.[40] Deze projecten en voorstellen zijn stevig aangevochten, vooral door religi-

36 Het overzicht is te vinden op: https://www.anaf.ro/restante/. Het is moeilijker om namen op te zoeken in dit overzicht dan in het vorige overzicht.
37 Meer informatie op https://edri.org/romania-mass-surveillance-project-disguised-egovernment/ en http://www.liberties.eu/en/ en http://mediapowermonitor.com/content/eu-helps-romanian-intelligence-agency-officially-become-big-brother.
38 http://coalitiaromanilor.org/a41-romania-stat-politienesc-cu-o-populatie-de-16-ori-mai-mica-decat-sua-sri-asculta-de-2-ori-mai-multe-telefoane-ca-fbi.aspx.
39 Case Casuneanu vs Romania (22018/10) http://hudoc.echr.coe.int/sites/fra/Pages/search.aspx#%7B%22appno%22:[%2222018/10%22]%7D; or Voicu vs Romania (22015/10) or Apostu vs Romania (22765/12).
40 Zie voor voorbeeldartikelen over vergelijkbare onderwerpen: http://asociatialibertatearomanilor.ro/.

euze groeperingen.[41] Sommige acties van deze groeperingen mondden zelfs uit in protestdemonstraties,[42] waarbij zich zo'n 2.000 deelnemers verzamelden.[43]

Burgerrechtenorganisaties

Er zijn een paar burgerrechtenorganisaties in Roemenië die actief zijn op het gebied van privacy en gegevensbeschermingskwesties. ApTI (Vereniging voor Technologie en Internet) is een niet-gouvernementele organisatie gericht op het ondersteunen en bevorderen van een gratis en open internet waar de mensenrechten worden gewaarborgd en beschermd.[44] De Roemeense vereniging voor de verdediging van de mensenrechten APADOR is een niet-gouvernementele organisatie die gericht is op het vergroten van het bewustzijn omtrent mensenrechtenkwesties en het promoten van de mensenrechtennormen in Roemenië en de regio.[45] CRJ (Het centrum voor juridische hulpmiddelen) richt zich met name op bewakings- en geheime diensten met betrekking tot privacy- en gegevensbeschermingskwesties.[46]

Andere NGO's zijn onder meer Activewatch, CJI, CRJI, AMPER, Militia Spirituala en SAR. Zij verdedigen ook de standpunten inzake privacy en gegevensbescherming, met name als er belangrijke wetsvoorstellen worden geïnitieerd. Deze NGO's nemen dezelfde standpunten in met betrekking tot veiligheidswetten. Over het algemeen krijgen ze weinig steun van het grote publiek, maar dat hangt van het onderwerp af. Ze spelen bijna altijd een kritische rol ten opzichte van de overheids- en veiligheidsstandpunten, maar ze nemen veelvuldig deel aan debatten en organiseren deze soms ook. Ze worden soms geconsulteerd tijdens de raadplegingen met betrekking tot de transparantie van de regelgeving. Hoewel ze soms worden uitgenodigd en er dan naar hen wordt geluisterd, wordt er niet altijd rekening gehouden met hun standpunten. Doorgaans komen de NGO's niet alleen in actie wanneer er klachten zijn, maar ook uit eigen beweging. Zo startte ApTI in 2015 een strategische rechtszaak inzake gegevensbescherming, hoewel ze in 6 maanden tijd maar circa 35 klachten hadden ontvangen.

8.2 Beleid

Nationaal beleid, Privacy Impact Assessments

De huidige regering heeft geen algemeen beleid inzake privacy en gegevensbescherming. Evenmin hadden de voorgaande regeringen een dergelijk beleid. Privacy en gegevensbescherming worden meestal vanuit een juridisch oogpunt bekeken (zie paragraaf 8.3 voor het juridische kader) in plaats van een beleidsoogpunt. Daarom zijn de meeste beleidsmaatregelen waarin het juridische kader verder wordt vertaald en uitgewerkt, afkomstig van de toezichthouder en niet van de nationale overheid. Er zijn echter sec-

41 Dit is een eufemisme voor ultraorthodoxe conservatieve bewegingen. Hun meest fundamentele argument is dat al deze eID's het nummer van de duivel, namelijk 66, bevatten. Meer informatie over extreme standpunten is te vinden op https://graiulortodox.wordpress.com/ or http://www.apologeticum.ro.

42 Zie https://www.youtube.com/watch?v=AHq8GemUiC4.

43 Zie http://www.mediafax.ro/social/miting-anticip-in-bucuresti-o-mie-de-persoane-la-protest-10667857.

44 www.apti.ro.

45 www.apador.org.

46 www.crj.ro.

torspecifieke beleidsmaatregelen op verschillende gebieden, waaronder financiën en gezondheidszorg, die verder worden besproken in paragraaf 8.3. Daarnaast keurde de Roemeense overheid in 2015 de nationale strategie inzake de digitale agenda voor Roemenië 2020 goed middels overheidsbesluit 245/2015. In dit beleidsdocument worden aspecten met betrekking tot e-governance, interoperabiliteit, cyberveiligheid, cloud computing, big data en sociale media besproken.
Privacy Impact Assessments (PIA's) maken deel uit van de Roemeense gegevensbeschermingswetgeving. Geen enkele PIA is verplicht en er bestaan geen regels over hoe en wanneer ze uitgevoerd moeten worden.

Privacy en de bescherming van persoonsgegevens in nieuw beleid
De bescherming van de privacy en persoonsgegevens speelt een grote rol op diverse gebieden. In de bankwereld, bijvoorbeeld, zijn er nieuwe financiële instrumenten die moeten worden aangepast om te voldoen aan het hoge veiligheidsniveau dat nodig is om gegevens te beschermen. Op het vlak van personeelszaken bevat de arbeidswet regels voor werkgevers, vooral met betrekking tot de grote bedrijven die elektronische systemen gebruiken voor Enterprise Resource Planning en relatiebeheer. Andere gebieden met informatiebeveiligingsregels zijn de belasting, de gezondheidszorg en marketing.
Concepten zoals Privacy by Design worden soms besproken in beleidsdocumenten, zoals in het document van het ministerie van Communicatie over de digitale agenda van Europa.[47] De Roemeense overheid heeft ook de nieuwe technologische ontwikkelingen in beschouwing genomen bij het aannemen van het beleid inzake cyberveiligheid.[48] Het nationale instituut voor onderzoek en ontwikkeling op het gebied van informatica bespreekt in het project 'Onderzoek, Ontwikkeling en Innovatie in ICT'(2015) een aantal aspecten met betrekking tot big data, het Internet of Things, platforms voor aangesloten intelligente voorwerpen en privacy.

Maatschappelijk debat
Zoals besproken in de voorgaande paragraaf, moeten burgers worden geraadpleegd als nieuwe wetten en regelgeving worden opgesteld. Weliswaar worden de burgers geraadpleegd met betrekking tot de bescherming van persoonsgegevens,[49] de Roemeense overheid acteert vaak reactief in plaats van proactief. Niettemin wordt de ontwikkeling van een samenwerking tussen de publieke en private sector om cyberveiligheid te waarborgen als een prioriteit beschouwd binnen het nationale actieplan, blijkens de hiervoor vermelde nationale strategie inzake de digitale agenda voor Roemenië in 2020.
In augustus 2015 hield het Roemeense ministerie van Economische Zaken, Handel en Toerisme een debat over de bescherming van persoonsgegevens, in antwoord op een verzoek met betrekking tot het debat over het ontwerpbesluit van de Roemeense over-

47 Zie www.mcsi.ro/Minister/Agenda-Digitala/Agenda_Digitala.
48 Zie https://ec.europa.eu/epale/sites/epale/files/strategia-nationala-agenda-digitala-pentru-romania-20202c-20-feb.2015.pdf.
49 Zie bijvoorbeeld http://www.romanialibera.ro/politica/institutii/guvernul-ministerul-economiei-va-avea-consultari-publice-privind-acta--actul-nu-schimba-legea-251870.

heid waarin de implementatie van het geïntegreerde informatiesysteem van toeristengegevens werd goedgekeurd.
De Roemeense gegevensbeschermingsautoriteit (ANSPDCP) wordt heel vaak geraadpleegd door overheidsorganisaties die verantwoordelijk zijn voor het opstellen van nieuwe wetgeving. Een voorbeeld waarbij de toezichthouder geraadpleegd werd, is de wijziging van wet nr. 506/2004.[50] Daarnaast vroeg het ministerie voor de Informatiemaatschappij ook het standpunt van het ANSPDCP met betrekking tot de wijziging van daaraan gerelateerde wetgeving.[51] Het ministerie van Openbare Financiën verzocht om het standpunt van de ANSPDCP betreffende de fiscale wetgeving.[52] Het ministerie van Justitie raadpleegde de ANSPDCP met betrekking tot de openbare overnameprocedure.[53] De Roemeense overheid raadpleegde de toezichthouder met betrekking tot het stemmen via e-mail.[54] Het nationale instituut voor de statistiek vroeg het ANSPDCP om advies omtrent de ontwikkeling van het nationale statistisch stelsel.[55] Het ministerie van Binnenlandse Zaken vroeg de toezichthouder om haar standpunt over het regeringsverordeningsproject met betrekking tot het gebruik van passagiersnamen in verband met de strijd tegen terrorisme.[56] Het nationale toerismebureau raadpleegde de ANSPDCP met betrekking tot de implementatie van het geïntegreerde informatiesysteem voor het bewijsmateriaal van toeristen.[57]
De ANSPDCP neemt vaak deel aan openbare debatten, zoals het debat over de bescherming van persoonsgegevens in verband met nieuwe technologieën (2015), de Europese dag van de gegevensbescherming (2014), cloudcomputinguitdagingen en kansen bezien vanuit het gegevensbeschermingsperspectief (2014) en conferenties (bijvoorbeeld: het voorkomen en bestrijden van cybercriminaliteit (2016), Ro-Direct (2015) en de rechtstaat in het digitale tijdperk (2015)). De ANSPDCP hield ook informatiebijeenkomsten bij diverse openbare kamers voor het notariaat.

Informatiecampagnes
Er vinden voorlichtingscampagnes plaats met betrekking tot de bescherming van privacy en persoonsgegevens die zowel gericht zijn op burgers als op bedrijven. De Roemeense overheid plaatste bijvoorbeeld een handleiding online over de bescherming van persoonsgegevens.[58] Overheidsfunctionarissen presenteren soms nieuwe ontwikkelingen op conferenties of bieden materiaal online aan. Zo sprak een afgevaardigde van de kanselarij van de Roemeense premier tijdens de Computer Show (RoCS, 2016) over de gevolgen van de Algemene Verorderning Gegevensbescherming (AVG).[59]

50 Zie ANSPDCP, Jaarverslag (2015), p. 14-16.
51 Zie ANSPDCP, Jaarverslag (2015), p. 16.
52 Zie ANSPDCP, Jaarverslag (2015), p. 17-22.
53 Zie ANSPDCP, Jaarverslag (2015), p. 23.
54 Zie ANSPDCP, Jaarverslag (2015), p. 24.
55 Zie ANSPDCP, Jaarverslag (2015), p. 25.
56 Zie ANSPDCP, Jaarverslag (2015), p. 26-30.
57 Zie ANSPDCP, Jaarverslag (2015), p. 30.
58 Beschikbaar op http://igi.mai.gov.ro/api/media/userfilesfile/Informare%20publica/Drepturile%20persoanelor/manual.pdf.
59 http://www.agerpres.ro/economie/2016/11/23/cucu-cio-office-romania-va-adopta-regulamentul-general-pentru-protectia-datelor-in-luna-mai-2018-12-54-32.

Het Roemeense nationale computercalamiteitenteam (CERT-RO) bespreekt op zijn website de gevaren van de nieuwe technologische ontwikkelingen[60] en de Roemeense informatiedienst heeft een handleiding over zelfbescherming gepubliceerd.[61] Het ministerie van Openbare Raadpleging en Burgerdialoog heeft informatie over de bescherming van persoonsgegevens online gezet.[62] Verder heeft de Roemeense gegevensbeschermingsautoriteit (ANSPDCP) talrijke persberichten, informatiematerialen en casussen gepubliceerd.[63] Voorbeelden zijn casussen met betrekking tot detailhandelaren, supermarkten, het openbaar ministerie, politieke partijen en banken.[64]

8.3 Wet- en regelgeving

Invoering van de EU-richtlijn

Roemenië had de EU-richtlijn met betrekking tot de bescherming van persoonsgegevens (95/46/EC) al ingevoerd voordat het land toetrad tot de Europese Unie. Dit werd gedaan middels het vaststellen van wet nr. 677/2001 voor de bescherming van personen met betrekking tot het verwerken van persoonsgegevens en de vrije circulatie van dergelijke gegevens.[65] Dit is de wet inzake persoonsgegevens (PDL). Deze wet is niet van toepassing op de nationale veiligheid en defensie.

Deze wet volgt nauwgezet de tekst en het oogmerk van EU-richtlijn 95/46/EC. In 2004, toen Roemenië nog midden in de onderhandelingen over de toetreden tot de EU zat, concludeerde de EU bijvoorbeeld dat de invoering van de gegevensbeschermingsrichtlijn nog achterliep omdat het toezicht en de handhaving niet toereikend waren (zie paragraaf 8.5).[66] In reactie hierop volgde Roemenië de instructies van de gegevensbeschermingsrichtlijn nog nauwgezetter.

Daardoor ligt de nadruk van de PDL op het begrip persoonsgegevens en de OESO-beginselen voor eerlijke verwerking van persoonsgegevens (verzamelingsbeperking, kwaliteit van de gegevens, doelstelling, gebruiksbeperking, veiligheidswaarborgen, transparantie, individuele deelname en verantwoording – deze onderwerpen komen met name aan bod in artikel 4 en 5 van de PDL). Uit hoofde van de PDL hebben burgers het recht om geïnformeerd te worden (art. 12 PDL), het recht op toegang (art. 13 PDL), het recht om hun persoonsgegevens te laten wijzigen of te laten actualiseren (art. 14 PDL), het recht om te verlangen dat hun gegevens verwijderd worden (art. 14 PDL), het recht om bezwaar te maken (art. 15 PDL), het recht om een klacht in te dienen bij de gegevensbeschermingsinstantie (art. 25 PDL) of te verwijzen naar een rechtbank (art. 17 PDL).

Aangezien de gegevensbeschermingsrichtlijn nauwgezet is gevolgd, worden middels de PDL voornamelijk de minimumvereisten van de richtlijn ingevoerd. Er zijn geen aan-

60 https://cert.ro/.
61 Beschikbaar op www.sri.ro/ghid-de-autoprotectie.html.
62 Zie Buletin Informativ (2016), beschikbaar op http://dialogsocial.gov.ro/.
63 Zie op http://www.dataprotection.ro/?page=Materiale_informative&lang=ro.
64 Zie ANSPDCP, Jaarverslag (2013).
65 www.avp.rp/leg677en.html. Zie ook de officiele publicatie in: het Roemeense Staatsblad, Deel I, Nr. 790/12 december 2001.
66 EU 2004, Periodiek verslag over de vooruitgang die Roemenië heeft geboekt op weg naar toetreding.

vullende bepalingen of duidelijk nieuwe of specifieke elementen.[67] De enige bepaling die aanvullend lijkt te zijn op de minimumvereisten vastgelegd in de richtlijn, is art. 28 waarin professionele verenigingen gehouden zijn om gedragscodes op te stellen en voor goedkeuring voor te leggen aan de toezichthoudende autoriteit. Volgens de tekst van de richtlijn is dit niet verplicht (art. 27 van de richtlijn).
De nieuwe bepalingen van de Algemene Verorderning Gegevensbescherming (AVG), zoals het recht op gegevensportabiliteit, het recht om vergeten te worden, Privacy Impact Assessments of meldingen van datalekken, zijn niet meegenomen in de PDL. Hoewel er geen verplichting in de PDL is opgenomen inzake meldingen van datalekken, bestaat er wel een dergelijke verplichting voor aanbieders van elektronische communicatiediensten (art. 3 van de Roemeense wet inzake e-privacy), zie hierna.

Sectorale wetgeving
Roemenië heeft, als lid van de EU, ook andere EU-richtlijnen ingevoerd. De EU-richtlijn voor de privacy inzake telecommunicatie (1997/66/EC) werd in 2001 ingevoerd middels wet 676/2001 inzake het verwerken van persoonsgegevens en de bescherming van privacy in de telecommunicatiesector.[68] Deze wet werd in 2004 vervangen door wet 506/2004[69] waarmee EU-richtlijn 2002/58/EC (de zogenoemde e-privacyrichtlijn) werd ingevoerd. Wet 506/2004 werd uitgebreid met wet 235/2015.[70] Wet 365/2002 dient voor de invoering van EU-richtlijn 2000/31/EC (de zogenoemde e-commercerichtlijn) en bevat bepalingen met betrekking tot de opslag van informatie.
Middels wet 238/2009 wordt de verwerking van persoonsgegevens door de structuren en eenheden van het ministerie van Bestuur en Binnenlandse Zaken gereguleerd. De persoonsgegevens die worden verzameld naar aanleiding van maatregelen gericht op preventie, onderzoek en bestrijding van criminaliteit en bij het handhaven van de openbare orde, worden verwerkt in het kader van het overheidsbeleid.[71] Deze wet geldt niet voor het verwerken van persoonsgegevens binnen het domein van de nationale veiligheid en defensie. Deze wet benadrukt dat de systemen en middelen voor het verwerken van gegevens op het gebied van preventie, onderzoek en bestrijding van criminaliteit moeten worden gebruikt "met inachtneming van de mensenrechten en op dusdanige wijze dat de beginselen van legaliteit, noodzakelijkheid, vertrouwelijkheid en proportionaliteit toegepast worden en alleen als, door het gebruik van deze systemen en middelen, de bescherming van de verwerkte gegevens gewaarborgd wordt".[72] Verder bevat de wetgeving met betrekking tot het werk van politieagenten bepalingen die verband houden met het verzamelen van gegevens. Als wettelijke veiligheidsmaatregel moeten politieagenten informatie over potentiële criminelen op dusdanige wijze verza-

67 Şandru, S. (2013), 'Over het beschermen en bewaren van gegevens in Roemenië', *Masaryk University Journal of Law and Technology*. Vol. 7, Nr. 2, p. 379-399.
68 Gepubliceerd in *Publicatieblad* nr. 800 van 14 december 2001. Zie ook: http://www.armad.ro/eng/legislation/law-no-6762001.
69 Gepubliceerd in M. Of. Nr. 1101/25 nov. 2004.
70 Gepubliceerd in M. Of. Nr. 767/14 okt. 2015.
71 http://www.mai-dga.ro/index.php?l=en&t=9. Gepubliceerd in M.Of. Nr. 405/15 jun. 2009, nogmaals gepubliceerd in M. of. Nr. 474/12 jul. 2012.
72 Art. 3 van Wet Nr. 238/2009.

melen dat zij niet "op illegale wijze schade toebrengen aan of een belemmering vormen voor de fundamentele rechten en vrijheden van burgers, hun privéleven, eer en reputatie".[73] Bovendien wordt er uitdrukkelijk in de wet bepaald dat de politieagent met betrekking tot kwetsbare groeperingen de plicht heeft "zorg en respect" te tonen.[74] Bijzondere persoonsgegevens betreffende ras, geloofs- of politieke overtuigingen of seksueel gedrag mogen door de structuren en eenheden van het ministerie van Binnenlandse zaken worden verzameld, maar alleen voor bepaalde gevallen waarin dergelijke gegevens noodzakelijk zijn voor het uitvoeren van een strafrechtelijk onderzoek of vervolging, als gevolg van een misdaad die heeft plaats gevonden.[75]
Besluit Nr. 1736/2012 van de minister van Financiën en besluit nr. 279/2012 van de minister van Bestuur en Binnenlandse Zaken met betrekking tot de goedkeuring van het kader inzake het samenwerkingsprotocol, dienen voor de uitwisseling van informatie tussen de belastingdienst en overheidsinstanties.[76] Noodverordening 99/2006 van de Roemeense regering met betrekking tot kredietinstellingen en de regulering van de nationale Roemeense bank (NBR 6/2006) hebben geleid tot aanvullende regels voor het verwerken van financiële gegevens. Overtreding van deze regels kan leiden tot een schriftelijke waarschuwing, een boete tussen de 0,05% en 1% van het aandelenkapitaal van de onderneming of het intrekken van exploitatievergunningen. Een schending van de vertrouwelijkheid kan worden beschouwd als een openbaarmaking van het beroepsgeheim, een strafbaar feit dat bestraft wordt met een gevangenisstraf van drie maanden tot twee jaar of een boete.
In de zorgverzekeringswet zijn specifieke regels vastgesteld voor medische persoonsgegevens. In besluit 1123/849/2016 van het ministerie van Gezondheid en de National Health Insurance House worden de procedures vastgesteld met betrekking tot het gebruik van de elektronische patiëntendossiers.[77] Middels wet 46/2003 inzake de rechten van de patiënt, wet 95/2006 met betrekking tot de hervorming van de gezondheidssector en besluit 904/2006 van de minister van Volksgezondheid zijn normen vastgesteld voor de invoering van goede praktische regels. Als zorgverzekeraars iemands gezondheidstoestand vrijgeven, wordt dit, indien de verzekerde persoon hier geen toestemming voor heeft gegeven, beschouwd als een strafbaar feit. In artikel 7-10 van de PDL worden de gevoelige categorieën persoonsgegevens behandeld. Onder deze speciale categorieën persoonsgegevens vallen etnische of raciale afkomst, politieke, religieuze of filosofische overtuigingen of overtuigingen van eenvoudiger aard, vakbondslidmaatschap en persoonsgegevens met betrekking tot de status van de gezondheid of het seksleven. Art. 10 richt zich op persoonsgegevens met betrekking tot strafbare feiten.

Zelfregulering en gedragscodes
De Roemeense ombudsman heeft, met betrekking tot de veiligheid van persoonsgegevens, besluit 52/2002 uitgevaardigd voor de goedkeuring van de minimumveiligheids-

73 Art. 32 van Wet Nr. 218/2002 over de organisatie en het functioneren van de Roemeense politie.
74 Art. 41 van Wet Nr. 360/2002 over de status van de politiemedewerker.
75 Art. 5 van wet 238/2009.
76 Gepubliceerd in M. Of. Nr. 32, 15 jan. 2013.
77 Gepubliceerd in M. Of. Nr. 806/13 okt. 2016.

vereisten voor de verwerking van persoonsgegevens.[78] Middels dit besluit zijn de beheerders van persoonsgegevens verplicht om te voorzien in een correcte identificatie en authenticatie van gebruikers (bijvoorbeeld middels gebruikersnamen en wachtwoorden), verschillende toegangsprofielen (need-to-know),[79] audittrajecten voor toegang tot persoonsgegevens, het gebruik van encryptie, het creëren van back-ups en het trainen van personeel.
De Roemeense gegevensbeschermingsinstantie (ANSPDCP) heeft ook een reeks besluiten gepubliceerd waarmee nadere informatie wordt gegeven over hoe persoonsgegevens verwerkt moeten worden.[80] Een dergelijk besluit bevat bijvoorbeeld passende beschermingsniveaus voor het overdragen van persoonsgegevens aan derde landen (buiten de EU), waaronder Argentinië, Zwitersland en Canada.[81] Sommige besluiten hebben betrekking op specifieke categorieën gegevens (zoals gezondheidsgegevens),[82] of specifieke technologieën, zoals videosurveillance.[83] Besluit 90/18-07-2006 heeft betrekking op de categorieën van verrichtingen die een negatief effect op persoonlijke rechten en vrijheden zouden kunnen hebben. In besluit 91/18-07-2006 worden zaken bepaald waarvoor geen melding gestuurd hoeft te worden met betrekking tot de verwerking van persoonsgegevens en in besluit 162/26-02-2008 worden zaken bepaald waarvoor een vereenvoudigde melding met betrekking tot de verwerking van persoonsgegevens acceptabel is.

8.4 Implementatie

Over het algemeen moeten organisaties zelf bepalen hoe ze willen voldoen aan de gegevensbeschermingswetten. Er zijn, afgezien van een handleiding voor CCVT-systemen geïnstalleerd in appartementenblokken, geen officiële overheidsrichtlijnen van de toezichthouder.[84] De interpretatie van de ANSPDCP van de gegevensbeschermingswetten kan enkel worden afgeleid uit jaarverslagen[85] en andere algemene informatiebronnen,[86] maar doorgaans respecteren zij ook de standpunten van de Artikel 29 Werkgroep.
Art. 28 van de PDL verplicht professionele verenigingen om gedragscodes op te stellen en voor goedkeuring voor te leggen aan de toezichthoudende instantie. Hoewel alle gedragscodes volgens de wet goedgekeurd moeten worden door de PDL, is er echter maar één gedragscode waarin privacy en gegevensbescherming is opgenomen en die is goedgekeurd door de PDL. Dit is de gedragscode van de Roemeense organisatie voor direct marketing.[87] Een aantal grotere bedrijven passen informatiebeveiligingsnormen

78 Gepubliceerd in M. Of. Nr. 383/5 jun. 2002.
79 Het 'need-to-know'-beginsel betekent dat gebruikers alleen toegang kunnen krijgen tot die gegevens die noodzakelijk zijn voor het uitvoeren van hun werkzaamheden.
80 http://www.dataprotection.ro/index.jsp?page=publicated&lang=en.
81 Besluiten 172/2007, 174/2007 en 173/2007.
82 Besluit 101/2008.
83 Besluit 52/2012.
84 Beschikbaar op http://dataprotection.ro/?page=ghiduri&lang=ro.
85 Beschikbaar op http://dataprotection.ro/?page=Rapoarte%20anuale&lang=ro.
86 Beschikbaar op http://dataprotection.ro/?page=Materiale_informative&lang=ro.
87 ARMAD - http://armad.ro/, DPA information - http://www.dataprotection.ro/servlet/ViewDocument?id=622.

toe (ISO 27000 en andere) om te bewijzen dat ze voldoen aan de gegevensbeschermingswetten.

Privacyfunctionarissen

De PDL noemt geen vereisten of kwalificaties voor het aannemen van privacyfunctionarissen. Er staan geen straffen op het in gebreke blijven betreffende het aanstellen van een privacyfunctionaris.[88] Roemeense bedrijven stellen normaal gesproken geen privacyfunctionarissen aan. Het is meer gebruikelijk voor multinationals met dochterondernemingen in Roemenië om een privacyfunctionaris aan te stellen, maar normaal gesproken vinden dit soort aanstellingen plaats bij de moedermaatschappij. Bij veel bedrijven is privacy en gegevensbescherming onderdeel van het takenpakket van de compliance officer of van de juridische afdeling. Het is daarom normaal gesproken geen fulltimebaan. De Roemeense organisaties die een privacyfunctionaris hebben aangesteld, wijzen die doorgaans de volgende taken toe: het adviseren van het bedrijf over de gegevensbeschermingsrechten en plichten en toezicht houden op activiteiten op het gebied van de gegevensverwerking, de wettelijke meldplicht, het gegevensbeheer en het voorkomen van datalekken.[89] Aangezien het niet verplicht is om privacyfunctionarissen te registreren, bestaan er geen officiële statistieken over het aantal privacyfunctionarissen in Roemenië.

Beveiligingsmaatregelen

In verband met de veiligheid van persoonsgegevens, heeft de Roemeense ombudsman besluit 52/2002 uitgevaardigd met betrekking tot de goedkeuring van de minimumveiligheidsvereisten voor de verwerking van persoonsgegevens. Middels dit besluit zijn de beheerders van persoonsgegevens verplicht om te voorzien in een correcte identificatie en authenticatie van gebruikers (bijvoorbeeld middels gebruikersnamen en wachtwoorden), verschillende toegangsprofielen (need-to-know),[90] audittrajecten voor toegang tot persoonsgegevens, het gebruik van encryptie, het creëren van back-ups en het trainen van personeel. Besluit 52/2002 bevat geen verwijzing naar de ISO-normen of -certificaten.

Er zijn specifieke sectoren die zich verder richten op beschermingsmaatregelen. De automatiseringsstrategie van het rechtssysteem voor de periode 2013-2017 is erop gericht de veiligheid van vertrouwelijke gegevens te vergroten en stelt procedures vast voor het monitoren van de veiligheidsbeleidsmaatregelen voor bestaande LAN- en WAN-netwerken en databanken en de ontwikkeling van systemen voor het herstel daarvan na calamiteiten. Het ministerie van Bestuur en Binnenlandse Zaken heeft Instructie 27/2010 uitgevaardigd, die de regels met betrekking tot de organisatorische en technische maatregelen bevat die toegepast moeten worden bij de verwerking van persoonsgegevens die verzameld worden tijdens de preventie, het onderzoek en de bestrijding van criminaliteit en ten behoeve van de continuïteit van overheidsactiviteiten.

88 www.iclg.co.uk.

89 www.iclg.co.uk.

90 Het need-to-knowbeginsel betekent dat gebruikers alleen toegang krijgen tot die gegevens die noodzakelijk zijn voor de uitvoering van hun werkzaamheden.

De gegevensverwerkers zijn, tijdens hun werk, onderhavig aan de controle van de nationale toezichthoudende instantie.[91]
Art. 28 van de PDL verplicht professionele verenigingen om gedragscodes op te stellen en voor goedkeuring voor te leggen aan de toezichthoudende instantie. Het is echter niet verplicht om informatiebeveiligingsmaatregelen op te nemen in deze gedragscodes. Er zijn bovendien verder geen regels of richtlijnen voor het invoeren van toegang op basis van functie of op basis van het need-to-knowbeginsel.
Het 'Privacy by Design'-concept is relatief nieuw.[92] Aangezien Roemenië geen voorloper is op het gebied van privacy en gegevensbescherming, is het niet raar dat Privacy by Design geen onderwerp van debat is in Roemenië.[93] Desondanks wordt er rekening gehouden met het 'Privacy by Design'-concept (en andere concepten zoals Privacy by Default en Privacy Impact Assessments) door de toezichthoudende instanties.[94]

Transparantie
Over het algemeen is het percentage Roemenen dat zich bewust is van het gebruik van persoonsgegevens door eigenaren van websites gelijk aan het gemiddelde van andere EU-burgers.[95] Als het gaat om beleidsmaatregelen inzake privacy heeft een significant aantal Roemenen (47%) ooit besloten om geen gebruik te maken van een website vanwege het privacybeleid. Ongeveer de helft van de Roemenen leest de algemene voorwaarden (49%) of het privacybeleid van een website (55%) nooit of vrijwel nooit. Als ze het privacybeleid wel lezen, lezen ze bijna nooit de hele tekst (slechts 15% vergeleken met het EU-gemiddelde van 11%). Desondanks voelen Roemenen zich vol vertrouwen, als ze de tekst lezen, dat ze de tekst voor het grootste gedeelte of helemaal begrijpen (76% vergeleken met het EU-gemiddelde van 64%).[96]
Gebrek aan informatie of opleiding zou een van de redenen kunnen zijn waarom minder dan de helft van de Roemenen hun privacyinstellingen wijzigt, met name met betrekking tot de beveiliging (bijvoorbeeld toegankelijkheid) van hun persoonlijke profielen en foto's op sociale media.[97]

8.5 Toezicht en handhaving

Op het moment dat de nieuwe grondwet in Roemenië werd vastgesteld in 1991, werd ook de zogenoemde Avocatul Poporului opgericht, de nationale ombudsman. Bescherming van privacy en persoonsgegevens maakte onderdeel uit van het werkveld van deze organisatie. De activiteiten van de Avocatul Poporului gingen pas in 1997 van

91 Gepubliceerd in M. Of. Nr. 98/12 feb. 2010.
92 Cavoukian, A. (2009), *Privacy by Design. The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, Toronto, Ontario, August 2009.
93 Zie ook http://hammond-minciu.com/2016/08/10/new-general-data-protection-regulation/.
94 Zie bijvoorbeeld ANSPDCP, Jaarverslag(2015), p. 28; ANSPDCP, Jaarverslag (2014), p. 27 en p. 107; ANSPDCP, Jaarverslag (2013), p. 14.
95 Consent Landenrapport Roemenië (2012), p. 4.
96 Consent Landenrapport Roemenië (2012), p. 4.
97 Consent Landenrapport Roemenië (2012), p. 39.

start, maar ook toen werden er slechts een paar zaken met betrekking tot de bescherming van privacy en persoonsgegevens behandeld.[98]
In 2004, toen Roemenië nog toe moest treden tot de EU, was er weinig vooruitgang geboekt met betrekking tot de invoering van regelgeving voor de bescherming van persoonsgegevens. De EU stelde vast dat de vooruitgang van de invoering beperkt was en was behoorlijk bezorgd over de regelgevende bevoegdheden en handhaving. Handhavingsmaatregelen bleven duidelijk achter in vergelijking tot andere lidstaten.[99]
Het toewijzen van het toezicht over en de handhaving van de bescherming van privacy en persoonsgegevens aan de Avocatul Poporului lag niet geheel in lijn met EU-richtlijn 95/46/EC, omdat de richtlijn voorschrijft dat het toezicht en de handhaving door een geheel onafhankelijke en autonome organisatie gedaan moet worden, speciaal opgericht voor dit onderwerp. Hoewel de Roemeense ombudsman een onafhankelijke en autonome organisatie is, richt deze zich duidelijk op een veel breder scala aan onderwerpen. In 2004 gaf de Avocatul Poporului al aan niet te beschikken over gespecialiseerde medewerkers en te weinig structuren te hebben om de taken met betrekking tot de bescherming van privacy en persoonsgegevens naar behoren uit te voeren.[100]
In mei 2005 werd er, middels wet 102/2005,[101] een nieuwe instantie opgericht, de nationale instantie voor de controle van en het toezicht op de verwerking van gegevens van persoonlijke aard (ANSPDCP). Op 1 januari 2006 verving deze toezichthouder in feite de Roemeense ombudsman als handhavingsinstantie op het vlak van de bescherming van persoonsgegevens. De president van deze gegevensbeschermingsinstantie heeft de rang van minister en de vice-president heeft de rang van staatssecretaris of vice-minister.[102] Beide worden aangewezen door de Roemeense senaat (het hogerhuis van het parlement) voor een periode van vijf jaar.

Toezichthouders
Op het moment dat de Avocatul Poporului werd opgericht, werden er middels wetgeving 20 vacatures gecreëerd voor medewerkers die aan kwesties zouden werken betreffende de bescherming van privacy en persoonsgegevens. In 2005 waren slechts 15 van deze vacatures gevuld.[103] Toen de ANSPDCP, de nieuwe toezichthouder, werd opgericht, werd er in de wetgeving rekening gehouden met een maximum van 50 medewerkers (de president en vice-president van de ANSPDCP niet meegerekend).

98 Manolea, B. (2007), Het institutionele kader voor de bescherming van persoonsgegevens in Roemenië, p. 1. Zie https://www.apti.ro/DataProtection_ro.pdf.
99 EU (2004), Periodiek verslag over de vooruitgang van Roemenië in aanloop naar de toetreding.
100 Manolea, B. (2007), Het institutionele kader voor de bescherming van persoonsgegevens in Roemenië. Zie https://www.apti.ro/DataProtection_ro.pdf.
101 Gepubliceerd in M. Of. Nr. 391/9 mei 2005.
102 Beide moeten minimaal vijftien jaar ervaring hebben in hun specialisatie en over een goede reputatie en hoge mate van integriteit beschikken. Het is echter niet vereist dat ze een juridische opleiding of een expertise hebben op het gebied van mensenrechten en/of de bescherming van privacy en persoonsgegevens.
103 Manolea, B. (2007), Het institutionele kader voor de bescherming van persoonsgegevens in Roemenië, p. 8. Zie https://www.apti.ro/DataProtection_ro.pdf.

De toezichthouder beschikt over een jaarlijks budget van circa 3 miljoen Lei (bijna 700.000 euro).[104] De afgelopen jaren heeft de ANSPDCP jaarlijks een aanzienlijk aantal vacatures gerapporteerd. In 2015 waren er 9 vacatures (van de maximaal 50 vacatures zoals vastgesteld in de wet). Dit tekort aan personeel, zowel in aantal als in expertise, wordt constant vermeld in de jaarverslagen van de afgelopen paar jaren.[105]
Naast de ANSPDCP is er nog een ander toezichthoudende instantie, namelijk de nationale instantie inzake het beheer en de regelgeving in communicatie (ANCOM), die specifieke bevoegdheden heeft met betrekking tot elektronische communicatiediensten en providers op telecommunicatienetwerken. ANSPDCP heeft echter de bevoegdheid te handhaven in geval van schendingen van de marktwetten.
De Avocatul Poporului, de nationale ombudsman, zou zich ook moeten richten op privacy, maar de organisatie heeft zich nogal rustig gehouden de afgelopen jaren, behalve met betrekking tot twee zaken. De ene is een rechtszaak over de onrechtmatigheid van verplichte registratie van prepaid SIM-kaarten voor het Roemeense constitutionele hof in 2014.[106] De ombudsman heeft deze zaak gewonnen. De andere is een zaak over de regelgeving met betrekking tot elektronische patiëntendossiers die de ombudsman in 2016 voorlegde aan het Roemeense constitutionele hof.[107]

Taken en bevoegdheden
De belangrijkste activiteiten van de toezichthouder staan weergegeven op diens website. De ANSPDCP:[108]

- ontvangt en onderzoekt meldingen over het verwerken van persoonsgegevens;
- geeft toestemming voor het verwerken van de gegevens in situaties die zijn vastgelegd in de wet;
- kan besluiten, als schending van de wet eenmaal is vastgesteld, tot het tijdelijk opschorten of stopzetten van de gegevensverwerking, het gedeeltelijk of geheel wissen van de verwerkte gegevens, het informeren van de strafrechtelijke instanties of procederen;
- informeert de natuurlijke en/of juridische persoon over de noodzaak te voldoen aan de verplichtingen en het uitvoeren van de procedures die zijn vastgesteld in wet nr. 677/2001;
- houdt het register bij waarin de het verwerken van persoonsgegevens wordt vastgelegd en stelt dit openbaar ter beschikking;
- ontvangt klachten, aanschrijvingen of verzoeken van natuurlijke personen, lost deze op en communiceert de geboden oplossing of, afhankelijk van iedere zaak, de aanpak die uitgevoerd is;
- voert voortijdig controles uit indien de gegevensbeheerder persoonsgegevens verwerkt die speciale risico's met zich mee kunnen brengen voor de rechten en vrijheden van de desbetreffende persoon;

104 Jaarverslag van de ANSPDCP (2015), p. 103.
105 Zie de jaarverslagen van de ANSPDCP uit 2013, 2014, 2015.
106 Zie https://edri.org/romania-mandatory-prepaid-sim-registration-ruled-unconstitutional/.
107 Persbericht van 30 november 2016; http://www.avp.ro/comunicate-de presa/comunicate2016/comunicat_30noiembrie2016.pdf.
108 http://www.dataprotection.ro/index.jsp?page=about&lang=en.

- voert onderzoeken uit, op eigen initiatief of naar aanleiding van klachten of aanschrijvingen;
- wordt geraadpleegd wanneer normatieve wetten worden opgesteld met betrekking tot de bescherming van de rechten en vrijheden van burgers in verband met het verwerken van persoonsgegevens;
- kan voorstellen doen met betrekking tot het opstellen van normatieve wetten of het wijzigen van normatieve wetten die van kracht zijn op het gebied van het verwerken van persoonsgegevens;
- werkt samen met overheidsinstanties en -organen, bestudeert hun jaarverslagen met betrekking tot de bescherming van burgers in verband met het verwerken van persoonsgegevens; vervaardigt, op verzoek van enige persoon, aanbevelingen en goedkeuringen over zaken die verband houden met de bescherming van de fundamentele rechten en vrijheden betreffende het verwerken van persoonsgegevens, met inbegrip van overheidsinstanties en -organen;
- werkt samen met vergelijkbare buitenlandse instanties voor wederzijdse ondersteuning en met personen die in het buitenland verblijven of die huizen bezitten in het buitenland, voor de bescherming van de fundamentele rechten en vrijheden die kunnen worden aangetast door het verwerken van persoonsgegevens; en
- voert andere bevoegdheden uit die zijn vastgelegd bij wet.

De ANSPDCP kan ex-officio of naar aanleiding van een klacht starten met een onderzoek. De toezichthouder kan haar onderzoeksbevoegdheden niet uitoefenen in het geval dat een klacht al eerder bij een rechtbank is neergelegd en deze klacht verband houdt met dezelfde partijen en dezelfde kwestie.
In 2004 vond er een aanzienlijke toename van de activiteiten van de toezichthouder plaats. De bescherming van persoonsgegevens werd verbeterd (met de nadruk op het belang van de verplichtingen van de beheerder van de gegevens) middels een reeks seminars gericht op specifieke sectoren, zoals hotels, het toerisme, internetdiensten, gezondheidszorg en de financiële sector.[109]
De toezichthouders van 17 Oost-Europese landen (zowel EU-lidstaten als andere landen) hebben zich verenigd om nauwer samen te kunnen werken. Deze toezichthouders treffen elkaar twee keer per jaar om de ontwikkelingen in hun respectievelijke landen te bespreken. Ze hebben ook een gezamenlijke website opgezet.[110]
De ANSPDCP heeft de volgende bevoegdheden (art. 21 PDL): het uitvoeren van audits bij beheerders van gegevens, het opschorten of stop zetten van de verwerking van persoonsgegevens, het gedeeltelijk of volledig uitwissen van persoonsgegevens, het starten van rechtszaken, het doorverwijzen van zaken naar de politie en juridische organisaties, het onderzoeken van zaken naar aanleiding van klachten of op eigen initiatief en het opleggen van boetes. Er zijn verschillende categorieën van administratieve boetes (hoofdstuk VIII van de wet inzake gegevensbescherming). Indien men verzuimt om gegevensverwerkingsactiviteiten te melden of een onvolledige of kwaadwillige melding

109 Manolea, B. (2007), Het institutionele kader voor de bescherming van persoonsgegevens in Roemenië, p. 11. Zie https://www.apti.ro/DataProtection_ro.pdf.
110 www.ceecprivacy.org.

doet, staat daar een boete op van 120 tot 2.325 euro. Sancties van 232 tot 5.800 euro kunnen opgelegd worden voor het illegaal verwerken van gegevens of het schenden van de rechten van de betrokkene. Het niet nakomen van de regels betreffende veiligheid en vertrouwelijkheid kan leiden tot boetes van 3.500 tot 11.700 euro. Op het niet beantwoorden van vragen van de gegevensbeschermingsinstantie of het niet aanleveren van de gevraagde documenten aan de gegevensbeschermingsinstantie staat een boete van 230 tot 3.500 euro.[111] In 2016 zijn de maximumboetes verhoogd. De maximumboetes bedragen nu, afhankelijk van de aard van de niet-naleving, tussen de 1.100 en 22.000 euro. Voor bedrijven met een jaarlijkse omzet van meer dan 1,11 miljoen euro kunnen de boetes tot 2% van de jaarlijkse omzet bedragen. Overtreders kunnen strafrechtelijk aansprakelijk worden gesteld, niet onder de wet inzake gegevensbescherming, maar onder het strafrecht. De schending van de geheimhouding van correspondentie is bijvoorbeeld een misdrijf, waarop een gevangenisstraf van zes maanden tot drie jaar staat.

Gebruik van bevoegdheden

Uit hoofde van artikel 25 van wet 677/2001, hebben burgers het recht om een klacht in te dienen bij de toezichthouder in het geval zij menen dat hun privacy of de bescherming van hun persoonsgegevens is geschonden. Burgers moeten eerst een klacht indienen bij de beheerder van de gegevens, maar na 15 dagen kunnen zij hun klacht indienen bij de toezichthouder, de ANSPDCP. De toezichthouder kan zowel het verhaal van de betrokkene als van de beheerder van de gegevens, of van vertegenwoordigers van beide partijen, aanhoren. Als de klacht gegrond wordt geacht, is de toezichthouder bevoegd om de tijdelijke opschorting of stopzetting van de verwerking van de persoonsgegevens te gelasten en/of te gelasten dat de verwerkte gegevens gedeeltelijk of volledig worden gewist.[112] De toezichthouder kan ook de strafrechtelijke handhavingsinstanties inlichten of een rechtszaak starten.[113]

In 2013 ontving de toezichthouder circa 7.500 meldingen.[114] Datzelfde jaar werden van de 67 aanvragen voor de overdracht van gegevens buiten de Europese Economische Ruimte in totaal 36 aanvragen goedgekeurd door de ANSPDCP.[115] Verder werden er in 2013 een totaal van 877 klachten en reclamaties ontvangen door de toezichthouder, hetgeen leidde tot 151 onderzoeken. Van de 229 onderzoeken die de ANSPDCP dat jaar in totaal uitvoerde, werd in 190 gevallen een sanctie opgelegd (ongeveer een derde kreeg een boete en ongeveer twee derde kreeg een waarschuwing). Uiteindelijk werd de toezichthouder 1.242 keer om hulp gevraagd bij het interpreteren van wet- en regelgeving.

Onlangs heeft de toezichthouder een reeks onderzoeken afgerond naar de mate waarin bedrijven voldoen aan de wetten inzake de bescherming van persoonsgegevens, met

111 Zie www.uk.practicallaw.com/7-520-9524.

112 Privacy en Mensenrechten 2004: Roemenië, deel van de Privacy en Mensenrechten 2004 door het Electronic Privacy Information Center en Privacy International. Bbeschikbaar op http://www.legi-internet.ro/privacy_ro2004.htm.

113 Manolea, B. (2007), Het institutionele kader voor de bescherming van persoonsgegevens in Roemenië, p. 7. Zie https://www.apti.ro/DataProtection_ro.pdf.

114 Jaarverslag 2013.

115 https://clientsites.linklaters.com/Clients/dataprotected/Pages/Romania.aspx.

name binnen overheidsinstanties, ambassades en consulaten, openbare vervoersmaatschappijen, medische centra en ziekenhuizen, en scholen. De hoogste sancties werden opgelegd voor het onvoldoende invoeren van maatregelen met betrekking tot de veiligheid en vertrouwelijkheid van de gegevens en het onvoldoende informeren van burgers over hoe hun persoonsgegevens worden verwerkt.
De Roemeense toezichthouder publiceert op zijn website elke paar maanden de sancties die zijn opgelegd. Deze publicaties bevatten de vermelding van de naam van de organisatie die een boete heeft gekregen, de hoogte van de boete die is opgelegd en de overtreding die geconstateerd is.[116] Een typerend voorbeeld ziet er als volgt uit: in juli/augustus 2016 werd bij SC Vodafone Romania SA "vastgesteld dat de verplichting vastgesteld in artikel 3, onder de voorwaarden vastgesteld in artikel 3 (3) van wet nr. 506/2004, gewijzigd en aangevuld, niet is nagekomen, aangezien Vodafone Romania SA niet voldoende passende technische en organisatorische maatregelen heeft genomen om de bescherming van de persoonsgegevens van bepaalde abonnees tegen onwettige toegang of verspreiding, te waarborgen. Voor deze overtreding werd een boete opgelegd van 10.000 [Roemeense] Lei."
In 2015 ontving en behandelde de ANSPDCP 1.335 klachten (1.074 klachten en 175 meldingen), hetgeen leidde tot boetes met een totaal bedrag van 679.700 Roemeense Lei (circa 150.000 euro) en waardoor 106 onderzoeken werden opgestart die leidden tot boetes met een totaalbedrag van 441.500 Roemeens Lei (circa 98.000 euro).[117] De aanpak van de ANSPDCP met betrekking tot het opleggen van boetes, is niet heel consistent.

Reputatie
Slechts 22% van de Roemenen weet van het bestaan van hun nationale toezichthouder. Dit is een van de laagste percentages in de gehele EU (het EU-gemiddelde is 37%).[118] Als burgers niet eens weten dat deze toezichthouder bestaat, zijn ze zich natuurlijk ook niet bewust van zijn activiteiten. Bedrijven zijn zich waarschijnlijk meer bewust van het bestaan van de ANSPDCP en diens activiteiten vanwege de bestaande regelgeving met betrekking tot de bescherming van persoonsgegevens. In 2015 was er een aanzienlijke stijging van het aantal petities dat door de toezichthouder werd ontvangen. Dit geeft aan dat de ANSPDCP en diens juridische bevoegdheden al beter bekend zijn dan toen de instantie net opgericht was.

116 Zie bijvoorbeeld:
http://www.dataprotection.ro/index.jsp?page=Sanctiuni_aplicate_august_2016&lang=en.
117 Zie ANSPDCP, Jaarverslag (2015).
118 Eurobarometer 431 (2015), p. 52.

9. Italië

9.1 Algemene situatie

De Italiaanse grondwet, uitgevaardigd in 1947, bevat een reeks van fundamentele beginselen (*principi fondamentali*) en een aantal burgerrechten en -plichten (*diritti e doveri dei cittidani*). In de fundamentele beginselen (artikelen 1-12) wordt de waardigheid van de persoon, zowel als individu als in sociale groepen, erkend en gewaarborgd dat de overheid de vrijheid en gelijkheid van alle burgers moet respecteren. Deze opsomming van burgerrechten en -plichten (artikelen 13-28) vormen de Italiaanse tegenhanger van een Bill of Rights. Deze bepalingen bevatten het recht op onschendbaarheid van de woning en de persoonlijke woonplaats (artikel 14) en de vrijheid en vertrouwelijkheid van correspondentie en van elke andere vorm van communicatie (artikel 15). Enige beperking of begrenzing van deze rechten kan alleen door middel van rechterlijke uitspraken worden opgelegd overeenkomstig de waarborgen die zijn vastgelegd in de wet.
Italië heeft de Universele Verklaring van de Rechten van de Mens (UDHR), het Europese Verdrag tot bescherming van de Rechten van de Mens (EVRM) en het Internationale Verdrag inzake Burger- en Politieke Rechten (IVBPR) ondertekend, drie rechtsinstrumenten die een recht op privacy bevatten (respectievelijk in artikel 12, 8 en 17). Italië heeft ook de Overeenkomst van de Raad van Europa inzake de Bescherming van Personen met Betrekking tot de Geautomatiseerde Verwerking van Persoonsgegevens (het zogeheten Verdrag van Straatsburg), ondertekend. Het constitutionele hof heeft vastgesteld dat het EVRM niet dezelfde status heeft als een grondwet.[1] Dit komt overeen met de Italiaanse dualistische benadering van het internationale recht, waarbij bepalingen uit internationale verdragen overgenomen moeten worden in nationale wetten voordat ze rechtstreeks van toepassing zijn. Italië was in 1958 een van de oprichters van de EEG, de voorloper van de EU. Daardoor is Italië onderhavig aan alle EU-wetgeving, met inbegrip van de EU-richtlijn inzake gegevensbescherming van 1995 (richtlijn 95/46/EC) en het Handvest van de grondrechten van de Europese Unie van 2009, waarvan artikelen 7 en 8 betrekking hebben op respectievelijk het recht op privacy en de bescherming van persoonsgegevens. Verder waarborgt wetsbesluit nr. 196.2003 (de Italiaanse wet inzake bescherming gegevens) het recht op privacy, door vast te stellen dat iedereen het recht heeft op bescherming van de persoonsgegevens die betrekking op hem of haar hebben (artikel 1 van de Italiaanse wet inzake bescherming gegevens).

1 Uitspraken nr. 348 en 349, 2007.

Internetgebruik

Italië heeft meer dan 60 miljoen inwoners, waarvan naar schatting 56% toegang heeft tot internetdiensten. Dit percentage is veel lager dan het Europese gemiddelde (72%). Het lijkt er echter op dat, vergeleken met de algehele situatie in de EU, de Italianen eerder gebruik maken van bepaalde online diensten dan landen waarvan het percentage inwoners dat toegang heeft tot internetdiensten nog lager ligt. Italië staat in de top 10 van landen in Europa waar mensen één keer per week gebruikmaken van online sociale netwerken (63% ten opzichte van het EU-gemiddelde van 57%).[2] Hetzelfde percentage Italianen (63%) maakt regelmatig gebruik van instant messaging of chatsites, waarmee Italië op de vijfde plaats staat in de EU-ranglijst.[3] Percentages die vergelijkbaar of lager zijn dan het EU-gemiddelde zijn die voor het gebruik van online games (28% vergeleken met het EU-gemiddelde van 25%), online bankieren (40% ten opzichte van het EU-gemiddelde van 43%) en het online uitwisselen van films of muziek met leeftijdsgenoten (23% ten opzichte van het EU-gemiddelde van 18%). Dit alles duidt op het gebrek aan een sterke internetinfrastructuur en internetdiensten in Italië.

Hoewel de Italiaanse burgers zich er steeds meer van bewust zijn dat organisaties hun persoonsgegevens verzamelen en exploiteren,[4] handelen ze daar niet naar. Deze waarneming is bevestigd door een aantal statistische gegevens over de activiteiten die de Italiaanse toezichthouder voor de bescherming van persoonsgegevens (*Garante per la protezioni dei dati personali*, hierna de 'Garante' genoemd) in 2015 heeft uitgevoerd.[5] In die periode legde de Garante 25.500 informatieverzoeken vast. Dit is een aanzienlijke daling vergeleken met 2014 toen de Garante 33.201 verzoeken behandelde.[6] Burgers maakten voornamelijk melding van hinderlijke oproepen en ongevraagde e-mails (spam).[7] Zij bleken zich echter wel bewust te zijn van gevoelige kwesties zoals de relatie tussen de bescherming van persoonsgegevens en de vrijheid van meningsuiting en het openbaar maken van foto's – veelal door minderjarigen – op het internet.

Bedrijven maakten zich in die tijd met name druk om het voldoen aan hun nieuwe verplichtingen onder de cookiewet.[8] De experts die voor dit onderzoek ondervraagd werden, gaven aan dat het voldoen aan de gegevensbeschermingswetgeving de grootste zorg was voor de meeste bedrijven.[9] Dit sluit geheel aan bij de zorg om te voldoen aan de cookiewet. Reputatie wordt in Italië zeer belangrijk wordt geacht voor het winnen van het vertrouwen van de klant, en speelt dan ook een belangrijke rol in de nasleep van een datalek of een sanctie die wordt opgelegd door de Garante. Diegenen die hun

2 Eurobarometer 431 (2015), p. 109.
3 Eurobarometer 431 (2015), p. 110.
4 Italiaans deskundigenonderzoek, p. 1.
5 'Relazione annuale 2015' door Garante per la protezione dei dati personali, p. 4.
6 'Relazione annuale 2014' door Garante per la protezione dei dati personali, p. 3.
7 'Relazione annuale 2015' by Garante per la protezione dei dati personali, p. 228, tabel 10.
8 De cookiewet werd in Italië geïntroduceerd samen met wetsbesluit 69 van 28 mei 2012 en de maatregel van Garante van 8 mei 2014 ter uitvoering van EU-richtlijn 2009/136/EC. Het verplicht bedrijven om over verschillende gegevensbeschermende maatregelen te beschikken overeenkomstig de cookiestypologie bij het installeren van dergelijke cookies in de browers van gebruikers. Garante gaf op 5 juni 2015 een toelichting over deze procedure.
9 Italiaans deskundigenonderzoek, p. 2.

reputatie graag intact houden, voldoen aan de meldingsplicht inzake het datalekken en aan, indien nodig, de opgelegde sancties.

(Gevoel van) controle

Een recent uitgevoerd onderzoek toont aan dat circa 53% van de Italianen het gevoel heeft dat ze slechts gedeeltelijk controle hebben over de informatie die zij online plaatsen, terwijl 23% van de ondervraagden aangeeft het gevoel te hebben helemaal geen controle te hebben.[10] Verder heeft 19% het gevoel de volledige controle te hebben. Dit lijkt erop te duiden dat Italië hoger dan het EU-gemiddelde scoort wat betreft gedeeltelijke controle (EU-gemiddelde is 50%) en volledige controle (EU-gemiddelde is 15%) en lager dan het gemiddelde scoort wat betreft geen controle (EU-gemiddelde is 31%). Over het geheel genomen lijken de Italianen zich minder druk te maken over het gebrek aan controle vergeleken met andere EU-landen. Circa 67% geeft aan zich hierover zorgen te maken, hetgeen verhoudingsgewijs weinig is.

69% van de Italianen beschouwt het verstrekken van persoonsgegevens als een steeds groter wordend deel van het moderne leven. Dit percentage ligt iets lager dan het EU-gemiddelde (71%).[11] Circa 40% geeft in dit verband aan dat ze het verstrekken van persoonsgegevens geen groot probleem vindt.[12] Anderszins geeft 44% van de Italianen aan het geen probleem te vinden om persoonsgegevens te verstrekken in ruil voor gratis online diensten.[13]

Vertrouwen

Als we wat nader ingaan op het vertrouwen, scoren Italianen over het algemeen onder het EU-gemiddelde, ook al staan ze nog in de bovenste helft van de ranglijst. Dit klopt voor sectoren als de gezondheidszorg en farmacie (64% ten opzichte van het EU-gemiddelde van 74%), overheidsinstanties (56% ten opzichte van het EU-gemiddelde van 66%) en het bankwezen en financiële instellingen (37% ten opzichte van het EU-gemiddelde van 56%). 40% van de ondervraagden heeft vertrouwen in winkels. Dat sluit perfect aan bij het EU-gemiddelde (40%). Het vertrouwen in online bedrijven als zoekmachines is daarentegen 28%, een percentage dat hoger is dan het EU-gemiddelde van 24%. De Italianen lijken over het algemeen meer te geloven in particuliere instanties dan in overheidsinstanties.

Beschermingsmaatregelen

Het percentage Italianen dat de privacyinstellingen van hun socialemediaprofielen ooit heeft getracht te wijzigen bedraagt 40% (EU-gemiddelde is 57%). Dit is een van de laagste percentages in de EU. Alleen Hongarije heeft ook een dergelijk laag percentage.[14] Desalniettemin vindt 79% van de Italianen het makkelijk om deze instellingen aan te passen (in vergelijking tot het EU-gemiddelde van 64%).[15] Diegenen die de privacyin-

10 Eurobarometer 431 (2015), p. 10.
11 Eurobarometer 431 (2015), p. 29.
12 Eurobarometer 431 (2015), p. 32.
13 Eurobarometer 431 (2015), p. 40.
14 Eurobarometer 431 (2015), p. 92.
15 Eurobarometer 431 (2015), p. 95.

stellingen niet aanpassen, geven aan erop te vertrouwen dat de website passende privacyinstellingen hanteert (20%), niet te weten hoe ze deze instellingen aan moeten passen (26%), zich geen zorgen te maken over hun online persoonsgegevens (27%), geen tijd te hebben om zich te verdiepen in de mogelijkheden (18%) of ze geven aan niet te weten dat je die instellingen aan kunt passen (16%).

Nationale politiek

Debatten omtrent gegevensbescherming vinden regelmatig plaats in het Italiaanse parlement vanwege artikel 154.1.f van de Italiaanse wet inzake gegevensbescherming (wetsbesluit 196/2003, hierna WGB genoemd),[16] waarin de Garante het mandaat krijgt om "de aandacht van het parlement of de overheid te vestigen op de wenselijkheid van de wetgeving, zoals vereist wordt door de noodzaak om de rechten waarnaar wordt verwezen in titel 2, te beschermen, mede in het licht van sectorale ontwikkelingen". Telkens als het verwerken van persoonsgegevens op het spel staat, is de Garante dus verplicht om commentaar te geven (door middel van formele raadplegingen en het indienen van formele standpunten) op de gevolgen van de gegevensbescherming voor een specifiek wetsvoorstel.[17] In 2015 diende de Garante 44 standpunten in over diverse onderwerpen en openbare sectoren, waaronder het verwerken van gegevens door de politie en inlichtingendiensten, de automatisering van openbare administratieve databanken en gerechtelijke procedures, belastingkwesties en gezondheidsgegevens.[18]
De experts die zijn geraadpleegd voor dit onderzoek geven aan dat (nationale) veiligheidsmaatregelen de afgelopen jaren belangrijker werden gevonden door de politiek dan de zorgen omtrent de bescherming van privacy en persoonsgegevens. Dit is te wijten aan de veronderstelde toegenomen dreiging van terroristische aanvallen.[19]
Met betrekking tot de gegevensbeschermingsregels is het Italiaanse parlement geneigd zelfregulering boven wetgeving te verkiezen, zoals blijkt uit het onderbouwde standpunt met betrekking tot het voorstel voor de Algemene Verordening Gegevensbescherming (AVG).[20] De overheid is momenteel bezig, in nauwe samenwerking met de Garante, om maatregelen te nemen om de nationale wetgeving voor gegevensbescherming af te stemmen op de AVG. Verder heeft de Garante informatiecampagnes gelanceerd betreffende dit onderwerp (door middel van richtlijnen en infographics) om het bewustzijn van burgers betreffende de komende wetgeving te vergroten.[21]

16 De wet is via de volgende link beschikbaar in het Engels: http://194.242.234.211/documents/10160/2012405/Personal+Data+Protection+Code+-+Legislat.+Decree+no.196+of+30+June+2003.pdf.
17 Italiaans deskundigenonderzoek, p. 2.
18 Italiaans deskundigenonderzoek, p. 2.
19 Italiaans deskundigenonderzoek, p. 2.
20 https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Reasoned_opinion_Italian_Chamber_of_Deputies.pdf.
21 Door bijvoorbeeld een handboek uit te geven over privacy op school en het verantwoorde gebruik van apps en sociale media. De complete lijst met informatiecampagnes is hier beschikbaar (alleen in het Italiaans): http://garanteprivacy.it/web/guest/home/stampa-comunicazione/vademecum-e-campagne-informative.

Media-aandacht

Er vindt in Italië geen specifiek nationaal debat over de bescherming van privacy of gegevens plaats dat de discussies in de media domineert.[22] Desalniettemin worden incidenten op het vlak van privacy en gegevensbescherming breed uitgemeten in het nieuws. De media houden de kwesties met betrekking tot de bescherming van persoonsgegevens en de activiteiten van de Garante goed in de gaten. De media-afdeling van de Garante bewaart de publicaties betreffende haar mandaat in een databank om zo het publiek uitvoerig te kunnen informeren. In 2015 selecteerde de Garante 57.200 documenten.[23] Hiervan kwamen 14.685 artikelen uit de belangrijkste Italiaanse kranten, landelijke tijdschriften, de belangrijkste lokale kranten, online kranten en blogs waarin geschreven werd over privacykwesties. 4.293 artikelen behandelden uitsluitend de activiteiten van de Garante. In totaal werden er 251 artikelen gepubliceerd in de papieren media over interviews, toespraken en verklaringen door de president en leden van de Garante, terwijl er 343 artikelen online werden gepubliceerd en 34 items betreffende dit onderwerp werden uitgezonden op de nationale en lokale tv en radio.[24] Het laatste privacygerelateerde onderwerp waarover werd bericht in de media is het recente hacken van de e-mails van invloedrijke politici en openbare instellingen.[25] Een ander recent voorbeeld dat de aandacht van de media trok, dateert van september 2016 en ging om een wraakactie betreffende de vrijgave van een pornovideo. Een Italiaanse meisje pleegde zelfmoord nadat een videoclip waarin zij voorkwam viraal ging.[26] Hoewel het debat omtrent dit incident zich meer richtte op de rol van de nieuwe technologieën en sociale netwerken, kwamen de problemen omtrent privacy ook aan de orde.

De zaak betreffende Ashley Madison trok ook veel media-aandacht. Het betrof de diefstal van 25 GB aan gebruikersgegevens van de commerciële website die gefactureerd werden onder de noemer 'het toestaan van buitenechtelijke relaties'.[27] De Garante werkte samen met de bevoegde buitenlandse instanties om na te gaan of de persoonsgegevens van Italiaanse burgers naar behoren waren verwerkt voorafgaand, tijdens en na het datalek.

22 Italiaans deskundigenonderzoek, p. 2.

23 'Relazione annuale 2015' door Garante per la protezione dei dati personali, paragraaf 23.1, p. 187.

24 T also contains procedures to follow in case of data breaches. different time from the main regulation - the the party. 'Relazione annuale 2015' door Garante per la protezione dei dati personali, paragraaf 23.1, p. 187.

25 http://www.bbc.com/news/world-europe-38568881?intlink_from_url=http://www.bbc.com/news/topics/0021de37-b64a-46ac-a4bb-5bdbdf0908ec/italy&link_location=live-reporting-story.

26 'Tiziana Cantone: Zelfmoord na jarenlange online vernedering schokt Italië', http://www.bbc.com/news/world-europe-37380704.

27 https://www.theguardian.com/technology/2015/aug/19/ashley-madison-hackers-release-10gb-database-of-33m-infidelity-site-accounts.

Er ontstonden ook verhitte debatten toen de nieuwe cookiewet van kracht ging in juni 2015.[28] De Italiaanse overheid voerde de Europese richtlijn 2009/136/EC[29] in door wetsbesluit 69 van 28/05/2012 te introduceren en de bepaling van bindende vereenvoudigde richtlijnen over te dragen aan de Garante.[30] De Garante introduceerde vervolgens de maatregel van 8 mei 2015,[31] maar verschillende professionele mediakanalen klaagden dat deze maatregel niet duidelijk genoeg was en geen technologische specificaties bevatte.[32] Dientengevolge gaf de Garante een toelichting op 5 juni 2015[33] met informatiemateriaal en infographics.[34]

Datalekken

Uit het jaarverslag van de Garante over 2015 blijkt dat zij dat jaar 49 meldingen ontving van datalekken, opgesteld door leveranciers van elektronische communicatiediensten die actief zijn in Italië (dit is een stijging van 50% ten opzichte van het voorgaande jaar).[35] Het merendeel van de gemelde datalekken had betrekking op ongeoorloofde toegang tot persoonsgegevens of het onopzettelijk verlies van contractuele documenten. Bijna alle gemelde gevallen betroffen minder dan 100 betrokkenen. Het grootste aantal mensen werd getroffen door vier gevallen (meer dan 2.000 mensen per zaak). In alle onderzochte zaken ging de Garante na of de respectievelijke organisatie gepaste maatregelen had genomen om het incident te verhelpen, bijvoorbeeld door ervoor te zorgen dat, waar nodig, de getroffen personen door de gegevensbeheerders op de hoogte waren gebracht van het incident. In twee gevallen (van 17 april 2015 en 22 december 2015) hadden de beheerders hun plicht om de getroffen personen te informeren verkeerd geïnterpreteerd en zij hadden daardoor verzuimd de betrokken personen te informeren.[36] De Garante stelde voor deze vier grotere zaken zogeheten niet-nalevingsprocedures in als gevolg van de mislukte meldingen inzake een datalek. In een van de gevallen informeerde de gegevensbeheerder de Garante zes maanden nadat het datalek plaats had gevonden. In de andere drie gevallen communiceerde de beheerders zelf helemaal niets.[37] De Garante werd op de hoogte gesteld van het datalek door de getroffen personen.

28 http://garanteprivacy.it/cookie.

29 EU-richtlijn 2009/136/EC van 25 november 2009 van het Europese parlement en van de Raad, waarmee EU-richtlijn 2002/22/EC met betrekking tot de wereldwijde dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken, en Verordening (EC) Nr. 2006/2004 met betrekking tot de samenwerking tussen nationale instanties die verantwoordelijk zijn voor de handhaving van wetten inzake consumentenbescherming, worden gewijzigd, introduceerde de plicht van lidstaten om het gebruik van cookies op de apparaten van gebruikers, te reguleren.

30 Wetsvoorstel nr. 69 van 28/05/2012, artikel 1.5.

31 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884.

32 http://it.ibtimes.com/cookie-law-una-legge-che-non-piace-tra-multe-petizioni-e-tanta-confusione-1404832.

33 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4006878.

34 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3661249.

35 "Relazione annuale 2015" door Garante per la protezione dei dati personali, Paragraaf 11.7, p. 107.

36 "Relazione annuale 2015" door Garante per la protezione dei dati personali, Paragraaf 11.7, p. 108.

37 "Relazione annuale 2015" door Garante per la protezione dei dati personali, Paragraaf 11.7, p. 108.

Burgerrechtenorganisaties
Om richtlijnen en aanbevelingen over specifieke onderwerpen uit te kunnen geven, publiceert de Garante regelmatig 'Mededelingen voor openbare raadpleging', waarin ze om de inbreng vraagt van "iedereen die geïnteresseerd is, ook van organisaties, academici en onderzoekers".[38] Deze inbreng is echter niet bindend voor de besluiten van de Garante. Federprivacy,[39] een organisatie van privacyfunctionarissen en -adviseurs, organiseert jaarlijks bijeenkomsten (een privacydag) om het bewustzijn onder burgers omtrent privacy en kwesties met betrekking tot gegevensbescherming te bevorderen.[40] Deze organisatie wordt gefinancierd via lidmaatschapsgelden (vanaf 60 euro per jaar voor gewone leden tot 800 euro per jaar voor grote bedrijven) en donaties.
Het Italiaanse instituut voor privacy organiseert momenteel bijeenkomsten tussen privacyfunctionarissen van particuliere organisaties en leden van de Garante met als doel een actief debat te voeren over de mogelijke frictie die kan ontstaan gedurende de invoer van de Algemene Verordening Gegevensbescherming (AVG).[41]

9.2 Beleid

Nationale beleidsmaatregelen, Privacy Impact Assessments
De Italiaanse wet voor gegevensbescherming (WGB) en bijlagen daarvan bevatten algemene en sectorspecifieke beleidsuitgangspunten.[42] De bijlagen werden van kracht na de WGB[43] en bevatten de sectorspecifieke aspecten van deze wet. Ze zijn opgesteld door de Garante en vastgesteld als 'maatregelen door de Garante', maar er wordt uitdrukkelijk naar verwezen in een aantal artikelen van de WGB en ze zijn daarom bindend. Er zijn momenteel negen bijlagen, waarvan er zeven bedoeld zijn als gedragscodes (annexes A.1 tot A.7) die sectorspecifieke beleidsmaatregelen bevatten:

- A.1: het verwerken van persoonsgegevens bij journalistieke activiteiten (maatregel door de Garante van 29/07/2998);
- A.2: het verwerken van persoonsgegevens voor historische doeleinden (maatregel door de Garante van 14/03/2001);
- A.3: het verwerken van persoonsgegevens voor statistische doeleinden in de activiteiten van het nationale stelstel voor de statistiek (maatregel door de Garante van 31/07/2002);
- A.4: het verwerken van persoonsgegevens voor statistische en wetenschappelijke doeleinden (maatregel door de Garante van 16/06/2004);
- A.5: het verwerken van persoonsgegevens voor informatiesystemen die beheerd worden door particulieren die zich bezighouden met consumentenkrediet en de

38 Dezelfde methode wordt gebruikt bij iedere mededeling voor openbare raadpleging. Een compleet overzicht is beschikbaar op de website van Garante: http://www.garanteprivacy.it/web/guest/home/ricerca?p_p_id=searchportlet_WAR_labcportlet&p_p_lifecycle=0.
39 http://www.federprivacy.it/fp/chi-siamo.html.
40 http://www.federprivacy.it/attivita/agenda/agenda-privacy/privacy-day-forum-2016.html.
41 http://www.istitutoitalianoprivacy.it/it/.
42 Italiaanse deskundigenonderzoek, p. 3.
43 Bijlagen A.1, A.2 en A.3 vormen een uitzondering hierop. Deze bijlagen werden geïntroduceerd samen met de Italiaanse gegevensbeschermingswet die vooraf ging aan de WGB.

betrouwbaarheid en stiptheid van de betaling (maatregel door de Garante van 16/11/2004);
- A.6: het verwerken van persoonsgegevens voor defensief onderzoek (maatregel door de Garante van 6/11/2008);
- A.7: het verwerken van persoonsgegevens voor commerciële informatiedoeleinden (maatregel door de Garantie van 17/09/2015;
- B: technische specificaties met betrekking tot de minimale veiligheidsmaatregelen;
- C: niet-incidentele verwerking die uitgevoerd wordt voor gerechtelijke of politiedoeleinden.

Bijlage C moet twee verordeningen bevatten: een van het ministerie van Justitie en een van het ministerie van Binnenlandse Zaken volgens artikelen 46 en 53 van de WGB. Deze verordeningen van de overheid zijn echter nog niet goedgekeurd.[44]
Privacy Impact Assessments (PIA's) zijn niet verplicht gesteld in Italië. In artikel 17 van de WGB krijgt de Garante de opdracht om een voorafgaande controle uit te voeren wanneer verwerking van persoonsgegevens plaatsvindt waarbij bepaalde risico's worden gelopen. De Garante brengt bovendien regelmatig advies uit over sectorspecifieke gegevensverwerking, zoals bijvoorbeeld over gegevensverwerking met betrekking tot het internet- en telefoonverkeer.[45]

Privacy en de bescherming van persoonsgegevens in nieuw beleid
In de WGB worden uitgangspunten inzake de bescherming van persoonsgegevens vastgesteld waaraan iedere sector, zowel de particuliere als de openbare sector, moet voldoen. Dientengevolge worden de uitgangspunten inzake de bescherming van persoonsgegevens vaak in beschouwing genomen bij de uitwerking van beleidsmaatregelen met betrekking tot het verwerken van gegevens.
Wat betreft het antiperen op nieuwe technologische ontwikkelingen en de gevolgen daarvan voor de toekomstige beleidsmaatregelen, neemt de Garante een actievere rol in dan de Italiaanse overheid. De Garante is regelmatig betrokken bij de evaluatie van specifieke technologische fenomenen en de gevolgen die deze fenomenen hebben voor de bescherming van persoonsgegevens. Zo werd een eerste evaluatie van de verwerking van big data en de goedkeuring daarvan door de Garante in 2014 gevolgd door een evaluatie door het nationale stelsel voor de statistiek in het kader van energieverbruik. Sindsdien heeft de Garante er een gewoonte van gemaakt om vergaderingen van belanghebbenden die bijdragen aan de evaluatie van de ontwikkelingen omtrent big data te sponsoren.[46]
Dezelfde benadering werd toegepast in verband met initiatieven gericht op het Internet of Things (IoT). In het begin moedigde de Garante een openbare raadpleging over deze zaak aan.[47] Daarnaast startte de Garante, als vervolg op 'de Privacy Sweep Day 2016', een initiatief van het Global Privacy Enforcement Network (GPEN), een 'veegactie'

44 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557209.
45 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1502599.
46 http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5846360.
47 http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3898704.

met betrekking tot de naleving van de wetgeving voor gegevensbescherming door de beheerders van gegevens in het kader van het Internet of Things.[48] Daarnaast organiseerde de Garante specifieke bijeenkomsten om de quantified-self beweging te bespreken.[49]

Maatschappelijk debat

De benadering van de Italiaanse overheid van privacyzaken wordt eerder als reactief dan als proactief beschouwd.[50] Daarom vinden bepaalde dialogen tussen de politieke partijen en burgerrechtenorganisaties over privacygerelateerde zaken niet op een gestructureerde manier plaats. Bewijs voor deze bewering kan gevonden worden in de pogingen van de overheid om de digitalisering van het openbare bestuur te verbeteren en instrumenten voor een e-overheid te bevorderen, terwijl tegelijkertijd bijna geen aandacht wordt besteed aan kwesties met betrekking tot de bescherming van persoonsgegevens.

De overheid maakt pas sinds kort gebruik van internetraadplegingen om het publiek te betrekken. De Vijfsterrenbeweging nam het initiatief voor deze benadering door bij het nemen van haar politieke beslissingen de uitkomst van dergelijke raadplegingen in beschouwing te nemen.[51] Er werden ook internetconsultaties gestart door de Garante om informatie te verzamelen over het gebruik van het Internet of Things.

Informatiecampagnes

Informatiecampagnes met betrekking tot de bescherming van persoonsgegevens die direct of indirect gesteund worden door de Italiaanse overheid, komen niet vaak voor. Een van de bekendste initiatieven die recentelijk werden geïntroduceerd door het ministerie van Binnenlandse Zaken, het ministerie van Onderwijs, Universiteiten en Onderzoeksinstellingen en de Italiaanse politie, is een informatiecampagne over het gebruik van het internet en sociale media en de gevolgen van cyberpesten.[52]

De toezichthouder, op zijn beurt, speelt een belangrijke rol bij het vergroten van het bewustzijn met betrekking tot de bescherming van persoonsgegevens en privacyrechten. Hij probeert dit bewustzijn te vergroten door regelmatig seminars te organiseren en papers te publiceren.[53] Deze zijn er echter vooral op gericht om professionals en de industrie te informeren over hoe voldaan kan worden aan de wetgeving voor gegevensbescherming en richten zich niet rechtstreeks op de zorgen van de burgers. De campag-

48 http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4877134.

49 http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3693403.

50 Italiaans deskundigenonderzoek, p. 4.

51 De Vijfsterrenbeweging is een politieke partij die in 2009 is opgericht door de voormalige komiek Beppe Grillo en de ondernemer Gianroberto Casaleggio. In 2013 werden kandidaten voor de politieke verkiezingen in Italië voor het eerst online gekozen door het lid van de partij; hetzelfde gebeurde in de daaropvolgende Europese en lokale verkiezingen. De partij gebruikte online raadplegingen om een aantal leden uit de partij te zetten, toen bleek dat zij niet voldeden aan de richtlijnen. De officiële website van de partij is: http://www.movimento5stelle.it.

52 http://www.istruzione.it/allegati/2016/Piano_azioni_definitivo.pdf.

53 http://garanteprivacy.it/web/guest/home/stampa-comunicazione/vademecum-e-campagne-informative.

nes die wel gericht zijn op burgers, richten zich met name op de bescherming van minderjarigen.[54]

9.3 Wet- en regelgeving

Invoering van de EU-richtlijn

EU-richtlijn 95/46/EC werd in eerste instantie geïmplementeerd met de wet inzake de bescherming van particulieren en andere betrokkenen met betrekking tot het verwerken van persoonsgegevens (wet nr. 675/96). In 2004 werd deze initiële wet echter vervangen door de geconsolideerde wet met betrekking tot bescherming van persoonsgegevens (wet inzake gegevensbescherming – wetsbesluit nr. 196 van 30 juni 2003, de WGB).[55] In tegenstelling tot de voorgaande wet, die met name gericht was op het reguleren van specifieke gegevensverwerkingen, dient de WGB voor het vastleggen van kaders voor de bescherming van persoonsgegevens. De wet bevat ook gedragsrichtlijnen voor journalistieke, historische, wetenschappelijke en statistische activiteiten.
Daarnaast bevat de WGB regels en maatregelen met betrekking tot de beheerders en verwerkers van de verwerkingsactiviteiten die uitgevoerd worden met behulp van elektronische hulpmiddelen, met het oog op de taken van de beheerders van de verwerkingssystemen.[56] De richtlijn werd derhalve ingevoerd met aanvullende bepalingen.[57]

Sectorale wetgeving

E-Privacy richtlijn 2009/136/EC,[58] waarin lidstaten verplicht worden om nieuwe regelgeving met betrekking tot veilige gegevensverwerking en cookies te introduceren, werd in de loop van 2012 omgezet in een Italiaanse wet, met name door middel van wetsbesluit nr. 69/2012 waarmee het concept 'inbreuk op persoonsgegevens' werd geïntroduceerd in de Italiaanse regelgeving en waarin de plichten waaraan leveranciers van openbare elektronische communicatiediensten moeten voldoen, zijn vastgelegd in geval van een dergelijke inbreuk (zie artikel 32-bis van de WGB).[59] De plicht houdt voor dit type leverancier in dat hij de Garante onmiddellijk op de hoogte moet stellen van het datalek (art. 32-bis 1) en uiteindelijk ook de getroffen gebruikers moet informeren als het lek waarschijnlijk aanzienlijk schade zal toebrengen aan de persoonsgegevens of privacy van een abonnee of persoon (art. 32-bis 2).

---

54 Italiaans deskundigenonderzoek, p. 4.

55 De volledige tekst is beschikbaar in het Engels: http://194.242.234.211/documents/10160/2012405/Personal+Data+Protection+Code+-+Legislat.+Decree+no.196+of+30+June+2003.pdf.

56 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1628774).

57 Italiaans deskundigenonderzoek, p. 5.

58 EU-richtlijn 2009/136/EC van 25 november 2009 van het Europese parlement en de Raad waarin EU-richtlijn 2002/22/EC met betrekking tot de wereldwijde service en gebruikersrechten in verband met elektronische communicatienetwerken en -diensten, EU-richtlijn 2002/58/EC betreffende het verwerken van persoonsgegevens en de bescherming van privacy in de elektronische communicatiesector, en Verordening (C) nr. 2006/2004 over de samenwerking tussen de nationale instanties die verantwoordelijk zijn voor de handhaving van de wetten inzake de bescherming van consumenten, worden gewijzigd.

59 Wetsbesluit nr. 69 van 28/05/2012, artikelen 2, 3 en 4.

De WGB omschrijft gevoelige gegevens in art. 4 als: "persoonsgegevens die speciale voorzorgsmaatregelen behoeven op basis van hun aard. Gevoelige gegevens zijn gegevens die het ras of de etniciteit, de geloofsovertuiging of andere overtuigingen, politieke meningen, het lidmaatschap van politieke partijen, vakbonden en/of verenigingen, de gezondheid of het seksleven van een persoon kunnen onthullen".[60] Verder beschouwt de WGB strafrechtelijke gegevens (art. 4 e) ook als gevoelige gegevens. Strafrechtelijke gegevens worden als volgt omschreven: "persoonsgegevens waarin wordt onthuld dat er bepaalde gerechtelijke maatregelen zijn genomen met betrekking tot een persoon die opgenomen moeten worden in het strafdossier van die persoon (bijvoorbeeld definitieve strafrechtelijke veroordelingen, voorwaardelijke vrijlatingen, verblijfs- of verplaatsingsbeperkingen of andere maatregelen dan inbewaringstelling). Het feit dat iemand een beklaagde is en/of het onderwerp van een strafrechtelijk onderzoek valt ook binnen de werkingssfeer van deze definitie".[61]
In 2015 nam de speciale commissie van de Kamer van Afgevaardigden voor de rechten en plichten op het internet een verklaring van internetrechtenaan die onder andere richtlijnen met betrekking tot de bescherming van persoonsgegevens (art. 5), een recht op eigen beeldvorming (art. 6), een bepaling over anonimiteit (art. 10) en een recht om vergeten te worden (art. 11) bevat.[62] De verklaring is bedoeld als handleiding voor toekomstige wetsvoorstellen.[63]

Zelfregulering en gedragscodes
Het Italiaanse institutionele systeem ondersteunt de gedecentraliseerde regulering van privacy niet. Naast de overheid en het parlement, is de Garante de enige instantie die gerechtigd is om bindende regelgeving en aanbevelingen met betrekking tot gegevensbescherming op te stellen.
Zoals omschreven in artikelen 12 en 154 (1) e van de WGB, stimuleert de Garante de goedkeuring van gedragscodes. In 2010 stelde de voormalige minister van Binnenlandse Zaken, dhr. Maroni, een wet voor waarin de 'zelfregulerende code voor de bescherming van de waardigheid van de mens op internet' was opgenomen naar aanleiding van aanbeveling 2160/2008 van het Europese parlement.[64] De code is er onder andere op gericht om personen te beschermen tegen online raciale, seksistische, sociale en religieuze haat. Hoewel dit niet direct genoemd wordt in de code, was een recht op privacy en vertrouwelijkheid opgenomen in de inleiding van het memorandum van overeenstemming tussen de overheid en de andere partijen.[65] De wet is echter nooit aangenomen

60 http://www.garanteprivacy.it/web/guest/home_en/data-protection-and-privacy-glossary.
61 http://www.garanteprivacy.it/web/guest/home_en/data-protection-and-privacy-glossary.
62 De volledige tekst van de verklaring is beschikbaar op: http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITVO_2015.pdf.
63 Website van de special commissie voor de rechten en plichten op het internet http://www.camera.it/leg17/1174.
64 http://www.ilsole24ore.com/fc?cmd=document&file=/art/SoleOnLine4/Norme%20e%20Tributi/2010/05/bozza-definitiva-codice-autodisciplina.pdf?cmd=art.
65 http://www.ilsole24ore.com/fc?cmd=document&file=/art/SoleOnLine4/Norme%20e%20Tributi/2010/05/bozza-definitiva-Protocollo-Codice-Autodisciplina.pdf?cmd=art.

en de overheid heeft verder geen initiatieven ondernomen om zelfregulering met betrekking tot de bescherming van persoonsgegevens te bevorderen.

9.4 Implementatie

Bij het naleven van de standaarden voor gegevensbescherming binnen organisaties spelen gedragscodes een belangrijke rol. Geheel in lijn met artikelen 12 en 154 (1) e van de WGB, moedigt de Garante de invoering van gedragscodes en professionele praktijken voor specifieke sectoren aan. De Garante ondersteunt organisaties bij het opstellen van processen en zorgt ervoor dat de voorgestelde codes voldoen aan de toepasselijke wetgeving voor gegevensbescherming.
Gedragscodes, ingevoerd door de Garante middels een maatregel overeenkomstig artikelen 12 en 154 (1) e, worden beschouwd als een integraal onderdeel (als bijlages) van de WGB en zijn daarom bindend.[66] Bij het invoeren van maatregel nr. 203 van 17 april 2014, bijvoorbeeld, schreef de Garante bepaalde stappen voor als een integraal onderdeel van het herzieningsproces inzake de gedragscodes. Die stappen zijn met name relevant voor het opstellen van gedragscodes met betrekking tot "de verwerking van persoonsgegevens voor informatiesystemen die beheerd worden door particulieren die zich bezighouden met consumentenkrediet en de vertrouwelijkheid en stiptheid van de betaling".[67] Artikel 12 (3) bepaalt bovendien dat het in acht nemen van de bepalingen vastgesteld in de relevante gedragscode een vereiste is voor de naleving van de wetgeving voor gegevensbescherming. Op de website van de Garante staat een overzicht met alle gedragscodes.[68]
Door de jaren heen heeft het Italiaanse toezichthouder ook tal van besluiten en richtlijnen[69] aangenomen die verduidelijking bieden van de uitgangspunten voor gegevensbescherming en richting bieden voor de concrete toepassing van deze uitgangspunten binnen diverse sectoren.[70] Deze besluiten zijn voornamelijk gebaseerd op de EU-wetgeving voor gegevensbescherming zoals geïnterpreteerd door het HvJ EU (zoals bijvoor-

66 Zie hierboven onder paragraaf 9.2.
67 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3070048.
68 Een lijst met gedragscodes is beschikbaar op de website van Garante http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-italiana. See above under section 9.2.
69 'Besluiten' zijn beslissingen genomen naar aanleiding van verschillende soorten klachten die bij Garante zijn gemeld (zie paragraaf 9.5). 'Richtlijnen' zijn algemene indicaties gegeven door Garante met betrekking tot specifieke verwerkingsvormen om een juiste toepassing van de uitgangspunten van de WGB te kunnen garanderen (een overzicht van de uitgegeven richtlijnen is te vinden op http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1772725).
70 Zie voor een voorbeeld van een dergelijk besluit: http://www.garanteprivacy.it/web/guest/home_en/main-decisions.

beeld in de *Google Spanje*-zaak)[71] en de Artikel 29 Werkgroep.[72] Een voorbeeld van een dergelijke activiteit is het algemene toepassingsbevel met betrekking tot biometrie.[73]

Privacyfunctionarissen

Onder de huidige WGB is er geen wettelijke verplichting tot het aanstellen van een privacyfunctionaris.[74] Hoewel dit niet betekent dat organisaties in de particuliere sector niet vrijwillig een privacyfunctionaris aanstellen, is het moeilijk een schatting te maken van het aantal privacyfunctionarissen dat momenteel als zodanig is aangesteld, aangezien er geen verplichting bestaat om een privacyfunctionaris te registreren en de Garante op de hoogte te stellen na een individuele aanstelling. De privacyfunctionaris hoeft bovendien niet over specifieke kennis of expertise te beschikken. De Garante raadt echter, sinds kort, bedrijven die zich bezighouden met het beheer van patiëntendossiers aan om een privacyfunctionaris aan te stellen.[75]

Grotere bedrijven stellen eerder een privacyfunctionaris aan. Vaak kunnen privacyfunctionarissen hun taken echter niet echt onafhankelijk uitvoeren. Daarnaast zijn hun verantwoordelijkheden in de meeste gevallen slechts onderdeel van hun algehele taken- en activiteitenpakket binnen de organisatie.[76] Er moet ook opgemerkt worden dat recente trends erop wijzen dat grotere Italiaanse organisaties liever een externe adviseur voor gegevensbescherming inhuren als het gaat om de nakoming van de verplichtingen inzake gegevensbescherming.[77]

Beveiligigingsmaatregelen

Organisaties worden geacht volledig te voldoen aan de verplichtingen die zijn vastgesteld in de WGB, met inbegrip van het invoeren van 'Privacy by Design (PbD)'-maatregelen en specifieke beginselen voor gegevensbescherming die zijn goedgekeurd middels de besluiten van de Garante. Aangezien PbD-methodieken niet wettelijk verplicht zijn, hebben ze pas recentelijk de aandacht getrokken van bedrijven en worden nu langzaam ingevoerd.[78]

---

71 http://curia.europa.eu/juris/fiche.jsf?id=C%3B131%3B12%3BRP%3B1%3BP%3B1%3BC2012%2F0131%2FJ&pro=&lgrec=en&nat=or&oqp=&dates=&lg=&language=en&jur=C%2CT%2CF&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&td=%3BALL&pcs=Oor&avg=&mat=or&parties=google%2Bspain&jge=&for=&cid=495953.

72 Italiaans deskundigenonderzoek, p. 5.

73 http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3590114. Het volledige overzicht van algemene besluiten is beschikbaar op: http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3755203.

74 Italiaans deskundigenonderzoek, p. 6.

75 http://194.242.234.211/documents/10160/0/Linee+guida+in+materia+di+dossier+sanitario+-+Allegato+A.pdf.

76 Italiaans deskundigenonderzoek, p. 6.

77 Italiaans deskundigenonderzoek, p. 6.

78 Bedrijven nemen pas sinds kort PbD in overweging door de komende inwerkingtreding van art. 25 van de AVG.

Met betrekking tot specifieke veiligheidsmaatregelen is artikel 31 e.v. van de WGB bijzonder belangrijk.[79] Informatiebeveiliging wordt ingevoerd door middel van ISO-certificaten en gedragscodes.[80] Beheerders van gegevens kunnen worden bestraft in geval ze de minimumveiligheidsmaatregelen zoals omschreven in bijlage B van de WGB niet naleven.[81] In bijlage B, paragraaf 13 wordt toegang op basis van functie bijvoorbeeld voorgeschreven als een verplichte maatregel: "Autorisatieprofielen voor iedere persoon of homogene groep personen die verantwoordelijk is voor de verwerking zullen worden opgesteld en de toegang voor deze persoon of groep personen zal zodanig worden geregeld voorafgaande aan de start van de verwerking dat zij alleen toegang kunnen krijgen tot die gegevens die noodzakelijk zijn voor het uitvoeren van de verwerkingswerkzaamheden.'

Transparantie

Ongeveer de helft van de Italianen leest nooit of bijna nooit de algemene voorwaarden van een website (45%) of het privacybeleid (50%). Diegenen die het privacybeleid wel lezen, lezen bijna nooit de hele tekst (11% in Italië ten opzichte van een EU-gemiddelde van 10%). Niettemin zijn Italianen er vrij zeker van dat, als ze het gelezen hebben, ze de tekst voor het grootste gedeelte of volledig begrepen hebben (Italië 65%, EU-gemiddelde 64%).[82] Verder gelooft het merendeel van de Italianen (83%) dat websites de persoonsgegevens van gebruikers verzamelen zonder dat mede te delen.[83] Dit gevoel wordt bevestigd door de bevindingen van het deskundigenonderzoek, waarin werd aangegeven dat de privacyinstellingen normaal gesproken zijn ingesteld om zoveel mogelijk persoonsgegevens te verzamelen.[84]

Het feit dat organisaties weinig geneigd zijn openheid van zaken te geven over het verzamelen en verwerken van persoonsgegevens uit zich in een bepaalde houding van het publiek. Italianen zijn geneigd zich te richten op de rol van de instanties en negeren hun eigen rol en verantwoordelijkheden grotendeels.[85]

9.5 Toezicht en handhaving

Toezichthouders

De Garante is de onafhankelijke instantie die opgericht is voor de bescherming van de fundamentele rechten en vrijheden in verband met de verwerking van persoonsgegevens en om het respect voor de waardigheid van personen te waarborgen. Hoewel een aantal

79 Bepalingen met betrekking tot de veiligheid van gegevens en systemen bevatten ook procedures die opgevolgd moeten worden in geval van een datalak.

80 Italiaans deskundigenonderzoek, p. 6.

81 Technische specificaties met betrekking tot de minimumveiligheidsmaatregelen: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557184.

82 Consent Landenverslag Italië, p. 4.

83 Il valore della privacy nell'epoca della personalizzazione dei media. Onderzoek door CENSIS, 7/10/2012, p. 6.

84 Italiaans deskundigenonderzoek, p. 6.

85 Il valore della privacy nell'epoca della personalizzazione dei media. Onderzoek door CENSIS, 7/10/2012, p. 10.

van de taken van de Garante zijn overgedragen aan de regio's, zijn er op regionaal niveau geen toezichthouders of toezichthoudende organen. De Garante is een collegiaal orgaan dat bestaat uit vier leden (een president, een vice-president en twee leden) die worden gekozen door het parlement voor een niet te verlengen termijn van zeven jaar. De huidige collegeleden zijn in 2012 gekozen.
De Italiaanse toezichthouder bestaat uit een totaal van 121 medewerkers.[86] Het budget voor 2016 bedraagt circa 19,2 miljoen euro, waarvan de helft afkomstig is van de Italiaanse overheid, terwijl de andere helft, zoals voorgeschreven door de wet, wordt ingebracht door andere onafhankelijke instanties.[87]

Taken en bevoegdheden
De Garante wordt gereguleerd door titel II van de WGB. Haar taken zijn vastgelegd in artikel 153 e.v. van de WGB en bevatten het volgende:
- toezicht houden op de naleving van de wettelijke bepalingen voor gegevensbescherming;
- het afhandelen van vorderingen, meldingen en klachten van burgers;
- het verbieden/stopzetten van verwerkingsactiviteiten die ernstige schade kunnen toe brengen aan individuen;
- het controleren, ook namens de burgers, van gegevensverwerking door de politie en inlichtingendiensten;
- het uitvoeren van controles ter plaatse op de directe toegang van databanken;
- het melden van ernstige overtredingen aan de gerechtelijke autoriteiten;
- het vergroten van het bewustzijn van de burgers omtrent privacywetgeving;
- het stimuleren van de invoer van gedragscodes voor verschillende industriële sectoren;
- het toekennen van algemene machtigingen voor het verwerken van bepaalde gegevenscategorieën; en
- deelname aan internationale activiteiten, speciaal met betrekking tot het werk van de gemeenschappelijke toezichthoudende instanties van Schengen, Europol en het douane-informatiesysteem.

De specifieke bevoegdheden voor onderzoeken en controles van de Garante worden gereguleerd in artikel 157 e.v., terwijl artikel 161 e.v. de sancties opnoemt die gebruikt worden voor de handhaving van de gegevensbescherming. Daarnaast krijgen betrokkenen middels de WGB drie opties voor het indienen van een klacht bij de Garante:
- Formeel bezwaar: dit is een alternatief voor de gewone rechtspraak, die is vastgelegd in artikel 145 tot 151 van de WGB. Er kan geen formeel bezwaar ingediend worden als er over dezelfde kwestie nog een procedure loopt bij de gewone rechtbank. Een formeel bezwaar voorkomt ook dat de betrokkene gebruikmaakt van de gewone rechtspraak voor dezelfde kwestie nadat de Garante erbij betrokken is. Met een formeel bezwaar kan de Garante de verwerking blokkeren en eisen dat de beheerder van de gegevens de kosten van het bezwaar betaalt.

86 http://194.242.234.211/documents/10160/4524990/Dotazione+organica+al+1°+settembre+2016.pdf.
87 2015 Jaarverslag, p. 204.

- Klacht (*Reclamo*): ingebed in artikel 142 en 143 van de WGB. Dit zijn gedetailleerde klachten over onwettige verwerking die op een informele manier ingediend kunnen worden door betrokkenen of hun vertegenwoordigers.
- Meldingen (*Segnalazioni*): dit zijn informele klachten, vastgelegd in artikel 144, die echter opgevolgd kunnen worden door de Garante middels nader onderzoek.

De Garante is gestart in 1997 en heeft met name veel aandacht besteed aan het opstellen van sectorale gedragscodes. De Garante adviseert zowel overheidsinstanties, waaronder het parlement en de rijksoverheid, als burgers en particuliere instanties die behoefte hebben aan verheldering van zaken op het gebied van privacy en gegevensbescherming. Om er zeker van te zijn dat de nieuwe rechtsinstrumenten met uitgangspunten voor gegevensbescherming nageleefd worden, geeft de Garante bindend advies over wetsvoorstellen. Daarnaast kan de Garante, in navolging van artikel 154 van de WGB, de aandacht van de rijksoverheid vestigen op de noodzaak van regelgevende maatregelen op het vlak van de bescherming van persoonsgegevens. De website van de Garante (www.gdpd.it) bevat alle informatie over de besluiten en standpunten die de Garante heeft uitgevaardigd, samen met de primaire en secundaire wetgeving (in het Italiaans). Middels een periodieke nieuwsbrief wordt bericht over de activiteiten van de Garante en de belangrijkste ontwikkelingen op het gebied van gegevensbescherming.[88]

Gebruik van bevoegdheden

In 2015 heeft de Garante zo'n 5.000 aanvragen, vorderingen en meldingen behandeld die verband hielden met verzekeringsmaatschappijen, telemarketing, consumentenkrediet, videosurveillance, het krediet- en bankwezen, internet, journalistiek, gezondheidszorg en welzijnsvoorzieningen.[89] Over 307 klachten werd een besluit genomen. Deze klachten betroffen met name banken en financiële instellingen, marketing, uitgeverijen, administratieve overheidsorganen, de uitbesteding van overheidsdiensten en bedrijfsinformatiediensten. De Garante bracht verder 44 adviezen uit over vragen van de regering en het parlement met betrekking tot diverse kwesties, waaronder het gebruik van persoonsgegevens door politie en inlichtingendiensten, de automatisering van overheidsdatabanken en gerechtelijke procedures, en gezondheidsgegevens.[90] Daarnaast behandelde de Garante 25.600 informatieaanvragen van burgers, die met name betrekking hadden op ongevraagde telemarketing (spam), videosurveillance en gegevensbescherming op de werkplek.

Datzelfde jaar voerde de Garante 303 inspecties uit, waarvan een aantal met behulp van het privacyteam van de Italiaanse financiële politie. Onder de organisaties die geïnspecteerd werden, waren onder andere softwarebedrijven die ondersteuning bieden aan politieonderzoeken en justitie, callcenters in de telemarketingindustrie en bedrijven die zich bezighouden met geldoverdracht. De inspecties van de Garante met betrekking

88 De laatste nieuwsbrief van 14 februari 2017 betrof bijvoorbeeld de willekeurige monitoring van e-mails en smartphones van medewerkers, telemarketing en het elektronisch paspoort. Het archief met alle uitgegevens nieuwsbrieven staat op de website van Garante: http://www.garanteprivacy.it/web/guest/home/ricerca?p_p_id=search-portlet_WAR_labcportlet&p_p_lifecycle=0.

89 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5570645.

90 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5570645.

tot de overheidssector leken met name gericht op de belastingdienst met bijzondere aandacht voor veiligheidsmaatregelen, interne audits en toepassingen voor e-gezondheidszorg.[91]
Er werden in 2015 in totaal 1.700 overheidsovertredingen geconstateerd, wat op het oog drie keer zoveel lijkt te zijn als het voorgaande jaar. Een belangrijk deel van deze overtredingen heeft te maken met het onrechtmatig verwerken van gegevens wegens het ontbreken van toestemming, het verzuim van de leveranciers van elektronische communicatiediensten om datalekken te melden en het niet of foutief informeren van gebruikers over de verwerking van hun persoonsgegevens.[92] De administratieve boetes die werden geheven bedroegen in totaal circa 3,5 miljoen euro.
De Garante diende in 33 gevallen een melding in bij de gerechtelijke instanties, met name in gevallen waar de instanties verzuimd hadden de minimale veiligheidsmaatregelen in te voeren, hetgeen bij 58% van de meldingen het geval was.[93] Er is geen informatie beschikbaar over de uitkomst van deze meldingen. Het is bovendien onmogelijk om exacte cijfers te achterhalen over het aantal rechtszaken met betrekking tot gegevensbescherming in Italië. Door de manier waarop statistische gegevens ingedeeld worden door het ministerie van Justitie, worden deze rechtszaken in dezelfde categorie geplaatst als vele andere rechtszaken.

Reputatie
Aangezien de Garante bevoegd is om sancties op te leggen aan bedrijven, zijn die bedrijven zich meer bewust van de Garante en haar activiteiten dan burgers. Organisaties die de besluiten van de Garante en diens activiteiten nauwgezet volgen, zijn eerder geneigd om de toezichthouder om advies te vragen. Dientengevolge zijn ze, doordat ze in contact staan met de Garante, minder bang voor sancties in vergelijking tot andere organisaties die niet regelmatig en op vrijwillige basis contact hebben met de toezichthouder.[94] Burgers zien de Garante als een onpartijdige scheidsrechter in het geval de verwerking van hun persoonsgegevens beoordeeld moet worden.[95]

91 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5570645.
92 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5570645.
93 'Relazione annuale 2015' door Garante per la protezione dei dati personali, paragraaf 11.7, p. 217, tabel 7.
94 Italiaans deskundigenonderzoek, p. 7.
95 Zie paragraaf 9.1 hierboven.

10. Conclusie

In de vorige acht hoofdstukken is antwoord gegeven op de eerste vijf deelvragen van dit onderzoek. Per land is in kaart gebracht wat op het terrein van de bescherming van persoonsgegevens de algemene situatie is en hoe het zit met beleid, wet- en regelgeving, implementatie en toezicht en handhaving. Zoals aangegeven in hoofdstuk 1 (zie tabel 2.1), zijn binnen deze vijf vergelijkingsaspecten in totaal 23 labels gebruikt om de antwoorden te clusteren. In dit hoofdstuk wordt in paragraaf 10.1 eerst de zesde deelvraag ('wanneer de acht onderzochte landen met elkaar worden vergeleken op bovengenoemde aspecten, wat is dan de positie van Nederland?') beantwoord. In deze paragraaf zal de positie van Nederland worden bepaald voor elk van de vijf vergelijkingsaspecten. Daarna zal in paragraaf 10.2 antwoord worden gegeven op de hoofdvraag van dit onderzoek ('wat is de positie van Nederland met betrekking tot de bescherming van de persoonsgegevens van de burgers in vergelijking met enkele andere landen binnen de Europese Unie?').

10.1 De positie van Nederland

10.1.1 *Algemene situatie*

Alle onderzochte landen zijn aangesloten bij de internationale en Europese verdragen die in een recht op privacy voorzien, waaronder de Universele Verklaring van de Rechten van de Mens (artikel 12), het Internationaal verdrag inzake burgerrechten en politieke rechten (artikel 17), het Europees Verdrag voor de Rechten van de Mens (artikel 8) en het Handvest van de grondrechten van de EU (artikel 7 en 8). In Nederland,[1] Frankrijk en Roemenië is sprake van een monistische benadering van het internationale recht, waarbij internationaal en nationaal recht als één rechtssysteem worden gezien en bepalingen in internationale verdragen direct, zonder verdere omzetting, doorwerken in nationaal recht. In Duitsland, het Verenigd Koninkrijk, Ierland, Zweden en Italië is sprake van een dualistische benadering van het internationale recht, waarbij internationaal en nationaal recht als twee gescheiden rechtssystemen worden gezien en bepalingen in internationale verdragen eerst moeten worden omgezet in nationaal recht.
Afgezien van het Verenigd Koninkrijk, dat geen grondwet heeft, hebben alle onderzochte landen van oudsher grondrechten met betrekking tot het huisrecht en het briefgeheim,

1 In Nederland wordt doorgaans gesproken van een gematigd monistisch systeem, omdat directe werking van bepalingen uit internationaal recht meestal pas geldt onder voorwaarde van voorafgaande bekendmaking.

rechten die gerelateerd zijn aan het privacyrecht. Alleen in Nederland, Zweden en Roemenië is een expliciet recht op privacy in de grondwet terug te vinden. In het Verenigd Koninkrijk en Frankrijk is het recht op privacy terug te vinden in andere wetgeving (in respectievelijk de Human Rights Act en de Code Civil). In de overige landen, Duitsland, Ierland en Italië, wordt het recht op privacy geconstrueerd door rechters op basis van andere grondrechten.

Internetgebruik

Het gebruik van Internet door Nederlanders wijkt nauwelijks af van het gemiddelde van de EU. In tabel 10.1 zijn verschillende vormen van internetgebruik vergeleken met het EU-gemiddelde.[2] Voor het gebruik van sociale media, telefoongesprekken via internet, online gaming en online winkelen zijn de cijfers voor Nederland vergelijkbaar met de rest van de EU. Alleen het gebruik van websites voor chatten ligt in Nederland wat lager. Het gebruik van internetbankieren ligt daarentegen juist aanzienlijk hoger dan het EU-gemiddelde.

	Nederland	**EU-gemiddelde**
Sociale media	59%	57%
Chatting	43%	33%
Internetbankieren	75%	43%
Online telefoongesprekken	24%	27%
Online gaming	27%	25%
Online winkelen	15%	17%

Tabel 10.1 Meer dan wekelijks internetgebruik in Nederland ten opzichte van het EU-gemiddelde[3]

Op basis van deze vergelijking kan worden gesteld dat de Nederlandse bevolking niet voorligt of achterligt wat betreft internetgebruik in vergelijking met andere Europese landen. Er zijn wel bepaalde verschillen te duiden met specifieke landen die in dit onderzoek worden vergeleken, maar het is niet aannemelijk dat verschillen tussen landen in de (mate van) bescherming van persoonsgegevens zouden zijn toe te rekenen aan de uiteenlopende mate waarin het internet wordt gebruikt.

(Gevoel van) controle

Er zijn duidelijke verschillen tussen Nederland en de EU waar te nemen als (het gevoel van) controle over persoonsgegevens nader wordt beschouwd (zie tabel 10.2). Allereerst is de mate waarin Nederlanders een gevoel van (volledige) controle over hun persoonsgegevens hebben duidelijk lager dan het EU-gemiddelde. Bovendien heeft Nederland

2 Voor een duidelijker overzicht van al het cijfermateriaal is Nederland hier niet vergeleken met de zeven andere landen in dit onderzoek maar met het EU-gemiddelde.

3 Gebaseerd op Eurobarometer 431 (2015), p. 109-112.

op dit punt een van de laagste cijfers van de EU. Daarbij dient wel aangetekend te worden dat als cijfers voor een gedeeltelijk gevoel van controle over persoonsgegevens worden meegerekend, de verschillen kleiner zijn.
De mate van bezorgdheid over het gebruik van persoonsgegevens is in Nederland duidelijk lager dan in de EU. Nederland heeft ook op dit punt een van de laagste cijfers van de EU. Wanneer de stelling wordt voorgelegd dat het verstrekken van persoonsgegevens nu eenmaal onderdeel is van het moderne leven (hetgeen iets zegt over de acceptatie van de praktijk van verzamelen en verwerken van persoonsgegevens), is 86% van de Nederlanders het hiermee eens, een cijfer dat aanzienlijk hoger ligt dan het EU-gemiddelde. Nederland heeft hiermee niet alleen een van de hoogste cijfers van de EU, maar het percentage is ook nog eens toegenomen de afgelopen jaren, een trend die tegen die in de EU ingaat.
Wanneer Nederlanders wordt gevraagd of het verstrekken van persoonsgegevens een belangrijk punt is, antwoordt 48% bevestigend, een percentage dat aanzienlijk hoger ligt dan het EU-gemiddelde. Ook hier heeft Nederland weer een van de hoogste cijfers binnen de EU. De mate waarin Nederlanders ongemakkelijk zijn met gepersonaliseerde informatie en advertenties ligt in Nederland ook hoger dan in de EU.

	Nederland	**EU-gemiddelde**
Gevoel van (volledige) controle	9%	15%
Bezorgdheid	47%	67%
Acceptatie	86%	71%
Belang	48%	35%
Ongemakkelijk met personalisering	61%	53%

Tabel 10.2 Gevoel van (volledige) controle over het gebruik van persoonsgegevens, bijbehorende bezorgdheid en acceptatie, de mate waarin belang wordt gehecht aan het verstrekken van persoonsgegevens en ongemakkelijkheid met personaliseren van informatie en advertenties in Nederland vergeleken met de EU[4]

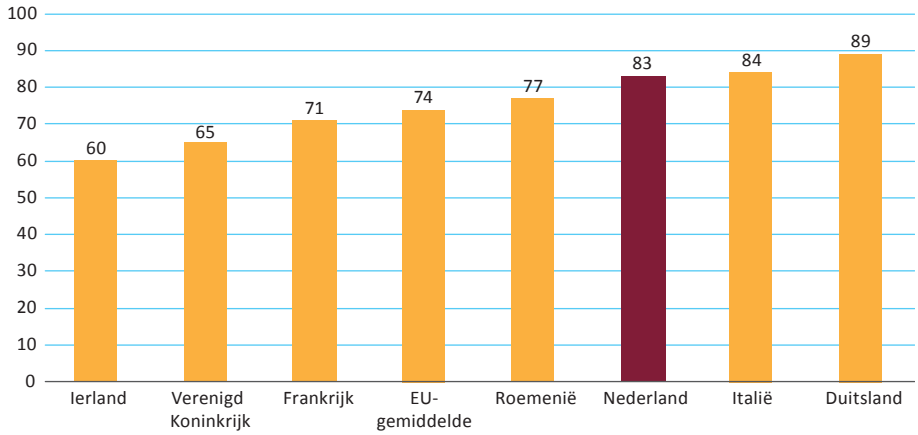
De vraag is wat te vinden van deze cijfers. Kort gezegd komt het erop neer dat Nederlanders een laag gevoel van controle over hun persoonsgegevens hebben, zich daar relatief weinig zorgen over maken en in hoge mate accepteren dat het verstrekken van persoonsgegevens 'er nou eenmaal bij hoort'. Dat is op zich nog wel consistent en te duiden als een 'luchtige houding' of groot vertrouwen ten opzichte van het verstrekken van persoonsgegevens. Echter, aangevuld met het feit dat Nederlanders het verstrekken van persoonsgegevens ook een belangrijk punt vinden en ongemakkelijk zijn met het personaliseren van informatie en advertenties maakt dat wellicht beter kan worden gesproken van een toenemende 'apathische houding'. Een andere mogelijke duiding is dat Nederlanders zich niet zozeer druk maken om het verstrekken van persoonsgegevens, maar vooral om wat er vervolgens met de persoonsgegevens gebeurt. Opvallend

4 Gebaseerd op Eurobarometer 431 (2015), p. 10, 13, 29, 32 en 40.

is in elk geval dat Nederland op alle percentages in tabel 10.2 op de uiteinden van het spectrum zit vergeleken met andere EU-landen.

Bewustzijn

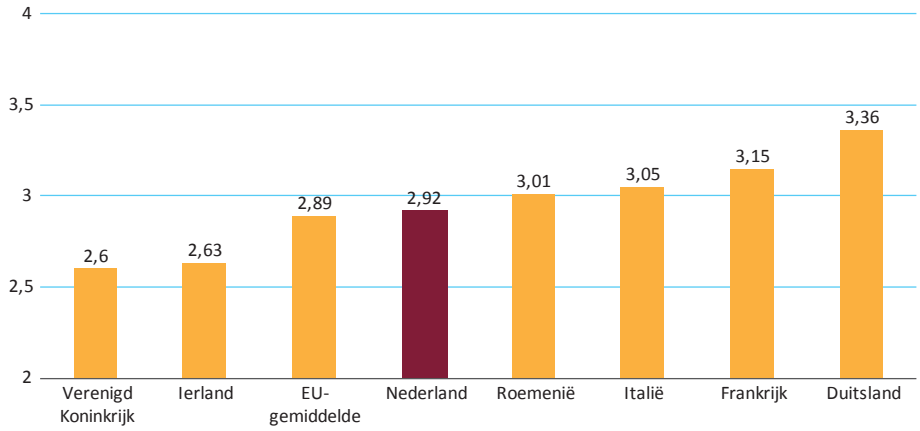
Met betrekking tot het bewustzijn over het gebruik van persoonsgegevens kunnen verschillende kengetallen met elkaar worden vergeleken. In de eerste plaats is de vraag of gebruikers zich ervan bewust zijn dat persoonsgegevens die ze achterlaten op een website gebruikt worden (voor uiteenlopende doeleinden, zoals om gebruikers via e-mail te benaderen, maar ook om de inhoud van websites en advertenties te personaliseren (zie figuur 10.1). Uit deze figuur kan worden geconcludeerd dat Nederlanders zich in het algemeen goed bewust zijn dat gegevens die ze op websites achterlaten worden gebruikt voor verschillende doeleinden.



Figuur 10.1 Percentage mensen dat zich ervan bewust is dat persoonsgegevens die ze op een website achterlaten worden gebruikt (voor verschillende doeleinden)[5]

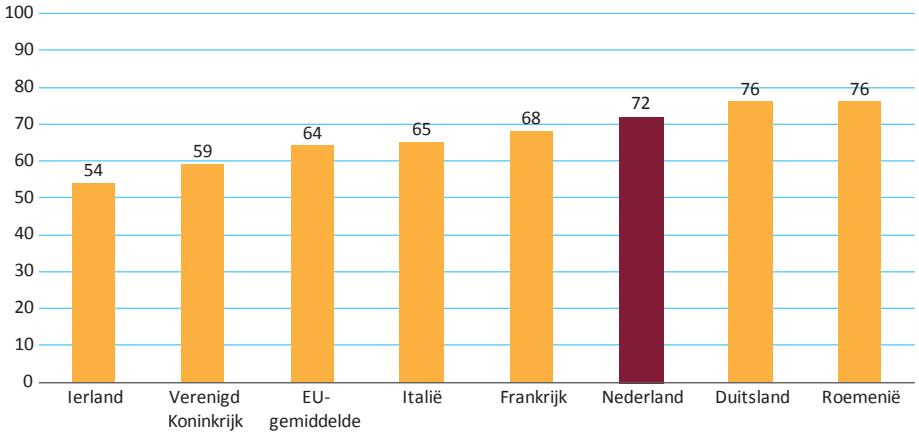
Daarnaast kan worden vergeleken in hoeverre burgers daadwerkelijk privacyinbreuken hebben meegemaakt. Dit is weergegeven in figuur 10.2, waarbij een score tussen 1 en 7 kon worden gegeven (1 = nooit, 7 = zeer frequent). Uit deze figuur kan worden geconcludeerd dat Nederland dicht tegen het EU-gemiddelde zit. Verder kan worden geconcludeerd dat in de gehele EU burgers niet zeer frequent privacyinbreuken ervaren. Merk op dat hiermee niet gezegd is dat er daadwerkelijk weinig inbreuken plaatsvinden; het kan ook zijn dat privacyinbreuken niet als zodanig worden opgemerkt, waargenomen of ervaren.

5 Gebaseerd op de CONSENT country reports. Geen data beschikbaar voor Zweden.



Figuur 10.2 Frequentie waarin burgers daadwerkelijk privacyinbreuken hebben meegemaakt (1 = nooit, 7 = zeer frequent)[6]

Als het gaat om het lezen van privacy policies of de algemene voorwaarden van websites, dan heeft in Nederland, net als elders in Europa, een groot aantal mensen deze documentatie zelden of nooit gelezen. Toch denken grote groepen mensen de teksten geheel of grotendeels te begrijpen. In figuur 10.3 zijn percentages weergegeven van mensen die de teksten geheel of grotendeels zeggen te begrijpen. Uit deze figuur kan worden geconcludeerd dat Nederlanders, aanzienlijk meer dan gemiddeld in de EU, denken privacy policies geheel of grotendeels te begrijpen. Uiteraard geeft dit geen uitsluitsel over de vraag of Nederlanders beter in staat zijn deze teksten te begrijpen.



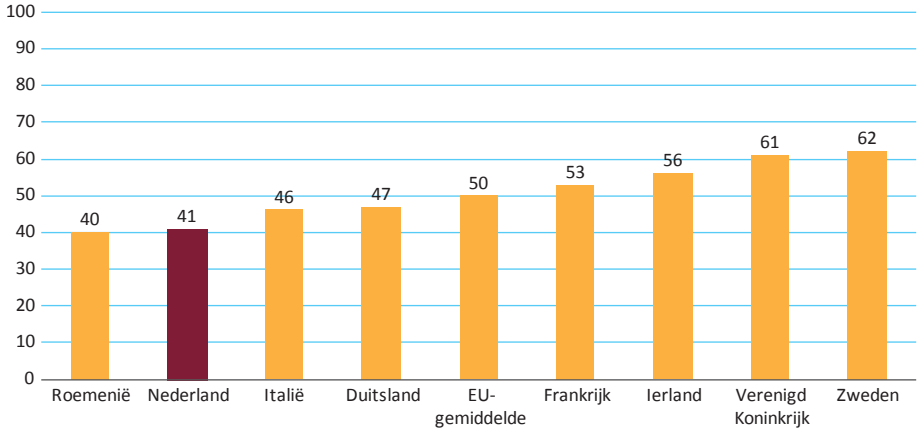
Figuur 10.3 Percentage mensen dat aangeeft privacy policies geheel of grotendeels te begrijpen[7]

6 Gebaseerd op de CONSENT country reports. Geen data beschikbaar voor Zweden.
7 Gebaseerd op de CONSENT country reports. Geen data beschikbaar voor Zweden.

Hoewel dit maar enkele kentallen zijn op het gebied van bewustzijn, komt duidelijk naar voren dat Nederlanders een heel behoorlijk beeld denken te hebben van wat er speelt op het vlak van privacy en bescherming van persoonsgegevens. Ook andere kentallen, zoals het bewustzijn van cookies (91% onder Nederlanders, EU-gemiddelde 65%) en het niet gebruiken van websites in verband met het privacybeleid (61% van de Nederlanders, EU-gemiddelde 47%), wijzen in die richting.

Vertrouwen

Hoewel Nederlanders zich duidelijk weinig zorgen maken over het gebrek aan controle over hun persoonsgegevens, maken ze zich wel zorgen over risico's op misbruik van persoonsgegevens (een score van 6,23 op 7-puntsschaal, waarbij 1 = oneens en 7 = eens). Er worden vooral risico's gezien in het gebruiken en delen van persoonsgegevens die ze verstrekken op sociale media zonder dat ze daarvan weet hebben of toestemming voor hebben gegeven. Veel minder worden risico's gezien om slachtoffer te worden van fraude. In figuur 10.4 is in percentages weergegeven in hoeverre mensen vrezen slachtoffer van fraude te worden. Op basis van deze figuur kan worden geconcludeerd dat de waargenomen risico's door Nederlanders achterblijven bij het EU-gemiddelde.[8]

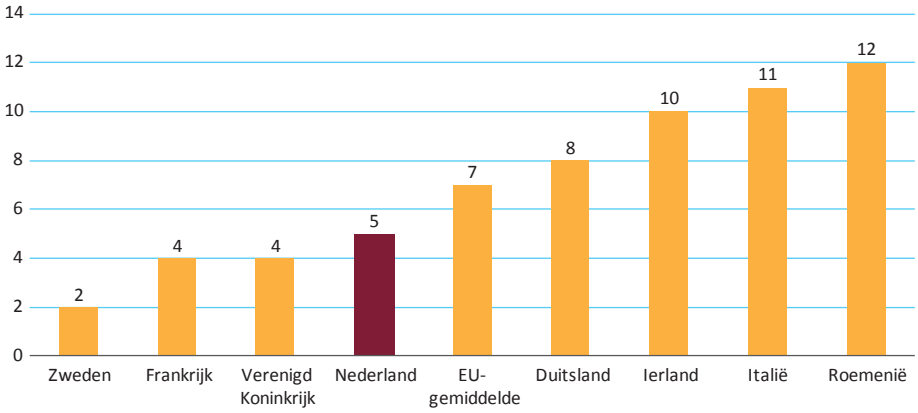


Figuur 10.4 Waargenomen risico slachtoffer van fraude te worden wanneer persoonsgegevens online worden achtergelaten[9]

Voor het risico op beschadiging van persoonlijke reputatie ligt het beeld dichter bij het EU-gemiddelde (zie figuur 10.5). In deze figuur is te zien dat het waargenomen risico op reputatieschade wanneer online persoonsgegevens worden achtergelaten in de gehele EU laag ligt.

8 Omdat sprake is van waargenomen risico's, kan niet worden uitgesloten dat burgers zich niettemin bewust zijn van zulke risico's, ondanks dat ze deze risico's wellicht niet (persoonlijk) hebben waargenomen.

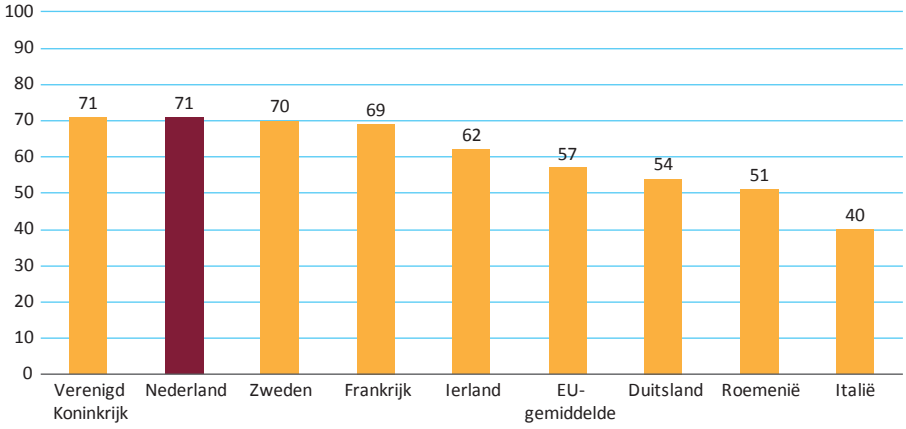
9 Gebaseerd op Eurobarometer 431 (2015), p. 102. Met het achterlaten van persoonsgegevens wordt hier bedoeld het bewust achterlaten van persoonsgegevens, niet op sporen die onbewust worden achtergelaten.



Figuur 10.5 Waargenomen risico op reputatieschade (percentages van de bevolking) wanneer persoonsgegevens online worden achtergelaten[10]

Beschermingsmaatregelen

Er zijn verschillende manieren waarop internetgebruikers zelf maatregelen kunnen nemen om hun persoonsgegevens beter te beschermen. Een typisch voorbeeld is het aanpassen van de privacyinstellingen. Het percentage Nederlanders dat hiervan gebruikmaakt is 71, hetgeen het hoogste cijfer is binnen de EU, samen met het Verenigd Koninkrijk (zie figuur 10.6).

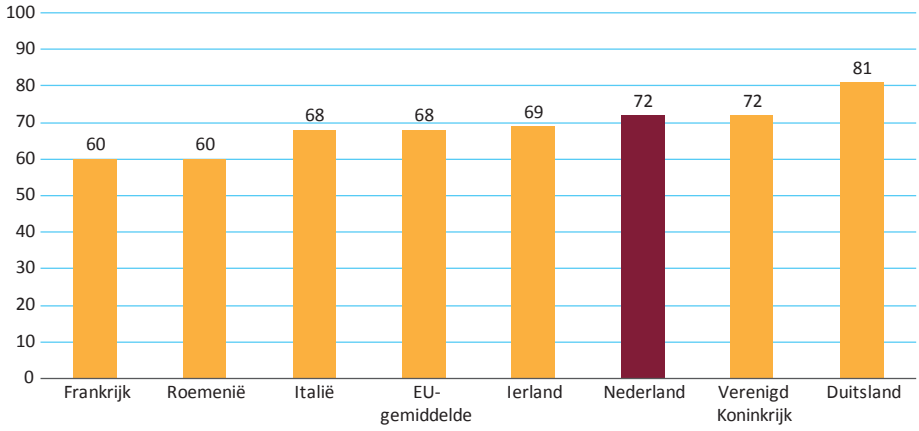


Figuur 10.6 Percentage dat ooit geprobeerd heeft privacyinstellingen van hun profiel op sociale media aan te passen[11]

Een andere mogelijkheid is het uitzetten van cookies. Het percentage Nederlanders dat deze maatregel treft ter verdere bescherming van hun persoonsgegevens is 72 en ligt

10 Gebaseerd op Eurobarometer 431 (2015), p. 102.
11 Gebaseerd op Eurobarometer 431 (2015), p. 92.

daarmee iets boven het EU-gemiddelde (zie figuur 10.7). Merk op dat dit niet betekent dat bijna drie kwart van de Nederlanders altijd cookies uitzet. Vaak betekent het uitzetten van cookies immers dat een website niet toegankelijk is of (sterk) verminderde functionaliteit biedt. Het percentage van 72 ziet op het aantal Nederlanders dat ooit wel eens cookies uitzet. Het onderzoek waarop deze cijfers zijn gebaseerd, peilt dus veel meer het bewustzijn dan het gedrag met betrekking tot cookies.



Figuur 10.7 Percentage mensen dat cookies uitzet (met als basis de groep mensen die zich bewust is van cookies)[12]

Ook op andere vlakken laten Nederlanders resultaten zien die duidelijk boven de EU-gemiddelden liggen. Daarbij kan bijvoorbeeld worden gedacht aan het blokkeren van pop-ups, het aanvinken van opt-in- en opt-outmogelijkheden, het blokkeren van bepaalde e-mailadressen, het controleren op spyware en het verwijderen van de zoekgeschiedenis. Alles bij elkaar kan worden geconcludeerd dat Nederlanders zowel in algemene zin als in vergelijking met andere EU-lidstaten behoorlijk zelfredzaam zijn als het aankomt op de bescherming van hun persoonsgegevens.

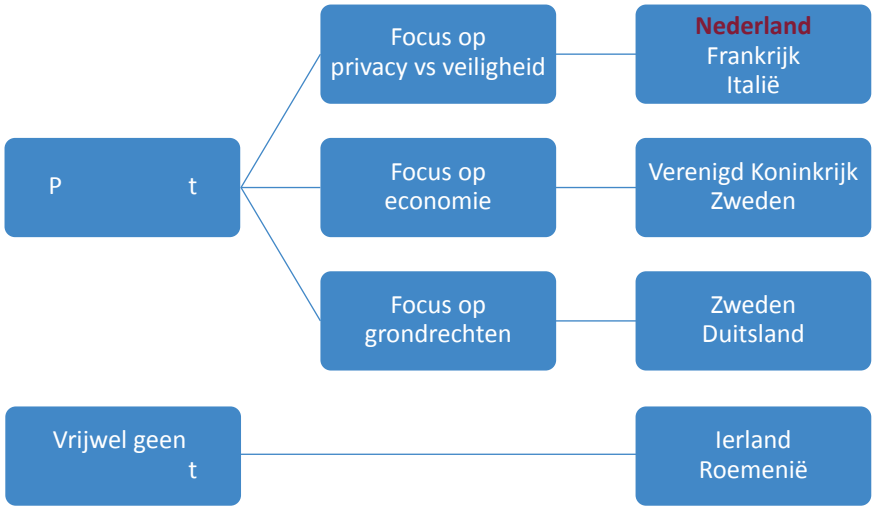
Nationale politiek

In de Nederlandse politiek, zowel in de Eerste als de Tweede Kamer, is sprake van een actief politiek debat over privacy en de bescherming van persoonsgegevens (zie paragraaf 2.1). Regelmatig komen de onderwerpen privacy en bescherming van persoonsgegevens aan bod in debatten op het terrein van criminaliteit, openbare orde, opsporing en nationale veiligheid.

In de landen die in dit onderzoek zijn vergeleken, is niet overal een actief politiek debat over privacy en de bescherming van persoonsgegevens. En als sprake is van een actief politiek debat, gaat het niet altijd over dezelfde onderwerpen. Ierland en Roemenië zijn landen waar vrijwel geen sprake is van een politiek debat over privacy en de bescherming van persoonsgegevens. In Frankrijk is wel sprake van een politiek debat op dit vlak,

12 Gebaseerd op de CONSENT country reports. Geen data beschikbaar voor Zweden.

maar het sterkst lijkt het politieke debat te zijn in Nederland, Duitsland, Zweden, het Verenigd Koninkrijk en Italië. In sommige landen, waaronder Nederland en Italië, wordt het debat versterkt doordat de toezichthouder een wettelijk recht heeft te adviseren over wetgeving waarbij het verwerken van persoonsgegevens een rol speelt.
Het politieke debat over privacy en de bescherming van persoonsgegevens in de verschillende landen heeft ook duidelijk een andere focus (zie figuur 10.8). In Nederland, Frankrijk en Italië staat regelmatig de verhouding tussen privacy enerzijds en veiligheid anderzijds centraal. Het politieke debat in het Verenigd Koninkrijk staat veel meer in het teken van de (digitale) economie. Dit is ook het geval in Zweden, maar daar wordt het debat over de digitale economie meer gecombineerd met vraagstukken over hoe een open, vrije samenleving eruit moet zien. Naast economische aspecten worden dus ook duidelijk grondrechtelijke en maatschappelijke aspecten in het debat meegenomen. In Duitsland, ten slotte, ligt de focus van het politieke debat veel meer op het vlak van grondrechten. In Duitsland is bovendien een toenemende consensus te bespeuren in de richting van meer bescherming van privacy en persoonsgegevens (zie paragraaf 3.1).



Figuur 10.8 Mate van actief politiek debat over privacy en de bescherming van persoonsgegevens in verschillende landen en de focus van het debat

Wanneer de positie van Nederland wordt vergeleken met andere landen, valt in positieve zin op dat in Nederland sprake is van een actief politiek debat. Niettemin kan het Nederlandse politieke debat over privacy en de bescherming van persoonsgegevens worden gekenschetst als soms wat eenzijdig, met veel nadruk op zaken als criminaliteit, openbare orde, opsporing en veiligheid. In Duitsland, Zweden en het Verenigd Koninkrijk richt het debat zich meer op zaken als de digitale economie, de digitale

samenleving en digitale grondrechten. Mogelijk liggen hier nog kansen voor Nederland het debat in breder perspectief te trekken. Pogingen hiertoe vinden reeds plaats.[13]

Media-aandacht

In veel van de onderzochte landen is er media-aandacht voor de onderwerpen privacy en de bescherming van persoonsgegevens (zie tabel 10.3). In Nederland, Duitsland, Frankrijk, het Verenigd Koninkrijk en Ierland is er uitgebreide media-aandacht, al variëren de onderwerpen die in de belangstelling staan. Zo was er in Ierland vooral aandacht voor de rechtszaak die privacyactivist Max Schrems tegen Facebook voerde en won (het Europese hoofdkwartier van Facebook is gevestigd in Ierland). In Frankrijk richt de media-aandacht zich mede op de privacy van bekende personen, waaronder politici. In Zweden en Italië is er wel enige media-aandacht voor privacy en de bescherming van persoonsgegevens, maar niet zo uitgebreid als in de eerdergenoemde landen. In Roemenië is er nauwelijks media-aandacht voor deze onderwerpen. In het Verenigd Koninkrijk is er al uitgebreide media-aandacht, maar deze lijkt bovendien verder toe te nemen.

	Media-aandacht	**Big Brother Awards**
Nederland	Hoog	Ja
Duitsland	Hoog	Ja
Zweden	Medium	Nee
Verenigd Koninkrijk	Hoog	Ja
Ierland	Hoog	Nee
Frankrijk	Hoog	Ja
Roemenië	Laag	Nee
Italië	Medium	Ja

Tabel 10.3 Media-aandacht voor de onderwerpen privacy en bescherming van persoonsgegevens

Een andere, zij het meer indirecte, indicator voor de hoeveelheid media-aandacht voor privacy en de bescherming van persoonsgegevens zijn de Big Brother Awards, jaarlijkse 'prijzen' die worden uitgereikt aan personen, bedrijven, overheidsorganisaties of plannen die de privacy schenden.[14] Big Brother Awards kunnen zowel de oorzaak als het gevolg zijn van media-aandacht voor privacy. Deze awards worden in 17 landen jaarlijks uit-

13 Ter illustratie: in 2014 diende SP-senator Gerkens in de Eerste Kamer een motie in die de regering verzocht het Rathenau Instituut te laten onderzoeken of een ethische commissie noodzakelijk is in de voortschrijdende digitaliserende samenleving. Zie *Kamerstukken I*, vergaderjaar 2014-2015, CVIII, E. Dit rapport is inmiddels beschikbaar, zie: Kool, L., Timmer, J., Royakkers, L. en Van Est, R. (2017), *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*. Den Haag: Rathenau Instituut. Zie https://www.rathenau.nl/nl/file/2797/Opwaarderen_Rathenau_Instituut.pdf.

14 https://en.wikipedia.org/wiki/Big_Brother_Awards.

gedeeld. Van de landen die betrokken zijn in dit onderzoek kennen Frankrijk, Duitsland, Italië, Nederland en het Verenigd Koninkrijk zulke Big Brother Awards. In Ierland, Roemenië en Zweden zijn er geen Big Brother Awards.
Wanneer de media-aandacht voor privacy en de bescherming van persoonsgegevens in Nederland wordt vergeleken met andere landen, valt op dat er in Nederland ruime media-aandacht is voor dit onderwerp.

Datalekken
De meeste EU-lidstaten hebben nog geen algemene wettelijk meldplicht datalekken, al zal dat wel vanaf mei 2018 het geval zijn wanneer de AVG van kracht wordt. Wel hebben alle EU-lidstaten inmiddels de e-Privacy richtlijn omgezet in nationale wetgeving, inclusief de daarin opgenomen meldplicht datalekken specifiek voor aanbieders van elektronische communicatiediensten. Er zijn slechts twee landen die, vooruitlopend op de AVG al een wettelijke meldplicht datalekken implementeerden. Dat zijn Duitsland, in 2009, en Nederland, in 2016.

	Wettelijke meldplicht datalekken?	**Opmerkingen**
Duitsland	Ja	Art. 42a BDSG, sinds 2009[15]
Nederland	Ja	Art. 34a Wbp, sinds 2016
Ierland	Nee	Wel een richtlijn van de toezichthouder
Zweden	Nee	
Verenigd Koninkrijk	Nee	
Frankrijk	Nee	
Roemenië	Nee	
Italië	Nee	

Tabel 10.4 Meldplicht datalekken[16]

Ondanks dat in veel landen er geen wettelijke verplichting is datalekken te melden, worden in de meeste landen niettemin door private organisaties openbare lijsten bijgehouden met incidenten van datalekken. In Nederland lijkt het bijhouden van zulke lijsten overgenomen te zijn door de toezichthouder, maar in Duitsland is ook een overzicht van datalekken beschikbaar buiten de toezichthouder om.[17] In verschillende landen (zoals in het Verenigd Koninkrijk en Italië) is het wel mogelijk datalekken te melden bij de toezichthouder (ondanks dat dit niet verplicht is) en in sommige landen

15 https://dejure.org/gesetze/BDSG/42a.html.
16 Gebaseerd op https://www.dlapiperdataprotection.com/index.html?c=SE&c2=&t=breach-notification.
17 https://www.projekt-datenschutz.de/news.

(zoals in Frankrijk) reageert de toezichthouder ook publiekelijk op datalekken die aan het licht zijn gekomen.
In alle onderzochte landen waren de afgelopen jaren aanzienlijke datalekken te zien. Echter, vanwege het ontbreken van een wettelijke meldplicht in de meeste landen is het lastig het aantal incidenten te vergelijken.[18] In Nederland waren er 5.693 datalekken in 2016.[19] Zodra vanaf 2018 alle landen een wettelijke meldplicht datalekken hebben, zal een vergelijking mogelijk zijn. Samengevat kan worden gesteld dat Nederland met de invoering van de meldplicht datalekken tot de koplopers van de EU behoort.

Burgerrechtenorganisaties
In alle onderzochte landen zijn burgerrechtenorganisaties aanwezig. Dit betreft zowel nationale als nationale afdelingen van internationale organisaties. Bij die laatste categorie kan worden gedacht aan onder meer Amnesty International en de International Commission of Jurists (ICJ). Deze organisaties zetten zich in voor mensenrechten in brede zin. In dit onderzoek ligt de nadruk op die burgerrechtenorganisaties die zich specifiek toeleggen op de bescherming van privacy en persoonsgegevens. In alle onderzochte landen zijn burgerrechtenorganisaties die zich hierop toeleggen aanwezig, maar hun budgetten en invloeden wisselen nogal.
Aan de ene kant van het spectrum zitten landen met organisaties met een beperkt budget en een beperkte invloed. In Zweden heeft de DFRI geen staf, ongeveer 80 vrijwilligers, een budget van circa 10.000 euro per jaar en naar eigen zeggen weinig invloed. In Roemenië is het beeld vergelijkbaar: er zijn weliswaar veel van deze burgerrechtenorganisaties, maar die hebben slechts beperkte publieke steun en beperkte invloed. Ook de Nederlandse organisaties Bits of Freedom, Privacy First, de Vereniging voor Privacyrecht en het NJCM zijn alle betrekkelijk kleine organisaties met kleine budgetten (ordegrootte 100.000 euro per jaar). Ondanks de geringe omvang en budgetten lukt het met name Bits of Freedom en Privacy First regelmatig media-aandacht te trekken. Het NJCM schrijft schaduwrapportages voor de VN waarmee internationale invloed wordt uitgeoefend.
Aan de andere kant van het spectrum zitten landen met organisaties met veel ruimere budgetten en veel meer invloed. In Duitsland zijn er veel burgerrechtenorganisaties actief (CAC, GPA, NDPE, ADPDS, Stiftung Datenschutz). Deze organisaties beschikken in sommige gevallen ook over veel ruimere budgetten. Bijvoorbeeld de Stiftung Datenschutz kreeg bij de oprichting in 2013 een startkapitaal van 10 miljoen euro mee van de rijksoverheid.[20] De Duitse burgerrechtenorganisaties gelden tevens als invloedrijk met betrekking tot wetgeving en regulering en het publieke debat. Ook in het Verenigd Koninkrijk zijn de burgerrechtenorganisaties professioneel, met name Big Brother Watch en Privacy International. Privacy International is wereldwijd bekend (onder meer vanwege de wereldwijde privacy rankings), heeft een jaarlijks budget van 1,4

18 In Duitsland worden opmerkelijke datalekken weliswaar gepubliceerd op de website https://www.projekt-datenschutz.de/news?page=3, maar een compleet overzicht is niet beschikbaar. In 2016 werden 86 incidenten gepubliceerd. In Italië ontving de toezichthouder 49 meldingen van datalekken in 2015, maar deze cijfers kunnen niet worden vergeleken omdat er in Italië geen meldplicht datalekken bestaat.
19 AP (2017), *Jaarverslag 2016*. Den Haag: AP, p. 7.
20 https://stiftungdatenschutz.org/ueber-uns/vermoegen/.

miljoen Britse ponden,[21] publiceert kwalitatief goede onderzoeksrapporten (onder meer voor de VN) en heeft serieuze invloed op het politieke en maatschappelijke debat. In Frankrijk is het speelveld van burgerrechtenorganisaties verdeeld over meerdere spelers, waarvan La Quadrature de grootste organisatie is. Vergeleken met de Duitse en Britse organisaties, heeft La Quadrature een beperkter budget (320.000 euro in 2017), maar ook deze burgerrechtenorganisatie kan als professioneel worden omschreven. De Franse burgerrechtenorganisaties hebben aanzienlijke invloed op het publieke debat.
In deze vergelijking valt op dat Nederland weliswaar een redelijk aantal burgerrechtenorganisaties kent op het vlak van bescherming van privacy en persoonsgegevens, maar dat de budgetten en de invloed in vergelijking met andere landen bescheiden zijn.[22] Dit zorgt voor een speelveld waarin de continuïteit niet is gegarandeerd: bijvoorbeeld in de periode 2006-2009 moest Bits of Freedom de activiteiten opschorten vanwege een gebrek aan financiën. Ook zijn de organisaties weinig bekend (18% van de Nederlanders heeft gehoord van Bits of Freedom, 13% van Privacy First).

10.1.2 *Beleid*

Nationaal beleid, Privacy Impact Assessments
Hoewel de AVG bij bepaalde vormen van verwerking van persoonsgegevens een Privacy Impact Assessment (PIA, of beter gezegd een Data Protection Impact Assessment, DPIA) voorschrijft indien sprake is van hoge risico's voor de rechten en vrijheden van personen, zijn zulke assessments in geen van de onderzochte landen wettelijk verplicht. Een uitzondering is Frankrijk, waar in artikel 34 van de wet inzake gegevensbescherming een wettelijke plicht kan worden gelezen voor gegevensbeheerders om risico's van het verwerken van persoonsgegevens in kaart te brengen. In Frankrijk zijn PIA's niet verplicht bij nieuwe wet- en regelgeving. Afgezien van wetgeving zijn er in verschillende landen wel andere reguleringsvormen waarbij PIA's in meer of minder mate verplicht zijn. In Nederland is de situatie min of meer omgekeerd: er is geen algemene wettelijke verplichting voor gegevensbeheerders om PIA's uit te voeren, maar wel een specifieke verplichting voor de rijksoverheid om PIA's uit te voeren bij nieuwe wetgeving en nieuwe informatiesystemen. Deze verplichting voor gegevensbeheerders binnen de rijksoverheid is sinds 1 september 2013 vastgelegd in het zogeheten Integraal Afwegingskader (IAK).[23] Daarvoor had de regering al verschillende moties in het parlement geaccepteerd waarin werd opgeroepen PIA's uit te voeren bij het ontwerpen van wetgeving waarbij de verwerking van persoonsgegevens een rol speelt. Hiermee had de regering zich eerder ook al verplicht tot het uitvoeren van PIA's. In andere landen, zoals het Verenigd Koninkrijk, Ierland en Italië hebben de toezichthouders via beleidsregels nadere verplichtingen omtrent het al dan niet uitvoeren van PIA's in het leven geroepen. In sommige landen zijn modellen en/of standaarden beschikbaar voor het uitvoeren van PIA's. Begeleiding vanuit de toezichthouders is in sommige landen

21 Dit budget komt van private donaties en overheden, maar niet van bedrijven.
22 In vergelijking met het Duitsland en het Verenigd Koninkrijk geldt dat deze budgetten in Nederland zowel absoluut als relatief (d.w.z. omgerekend naar inwonertal of BNP) gering zijn.
23 Zie https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving.

beschikbaar. Zie voor een overzicht tabel 10.5. Opvallend is ook dat in alle onderzochte landen veel (en steeds meer) private aanbieders beschikbaar zijn voor het uitvoeren van zulke assessments.

	Wettelijk verplicht	**Andere regulering/verplichting**	**Model/standaard beschikbaar**	**Begeleiding vanuit DPA?**
Nederland	Nee	Ja[24] (moties)	Ja[25]	Nee
Duitsland	Nee	Nee	Ja (voor RFID)	Nee[26]
Zweden	Nee	Nee	Nee	Nee
Verenigd Koninkrijk	Nee	Ja (DPA-beleidsregels voor bij overheden)	Ja	Ja
Ierland	Nee	Nee	Nee	Nee
Frankrijk	Ja[27]	Nee	Ja	Ja
Roemenië	Nee	Nee	Nee	Nee
Italië	Nee	Ja (DPA beleidsregels)	Nee	Nee

Tabel 10.5 Privacy Impact Assessments

Het overzicht in tabel 10.5 laat een wisselend beeld zien in de vergeleken landen. Frankrijk lijkt koploper te zijn op dit punt, maar heeft (in tegenstelling tot Nederland) geen PIA's voor nieuwe wetgeving. Voor verdere verbetering zou Nederland zich vooral kunnen richten op het verplicht stellen van PIA's voor gegevensbeheerders. Het standaardmodel voor PIA's voor de rijksoverheid is recent geëvalueerd en wordt momenteel herijkt.[28] Uit de evaluatie blijkt dat er ruimte voor verbetering is omtrent praktische toepasbaarheid, volledigheid, begrijpelijkheid en bruikbaarheid als gebruikersvriendelijkheid. Verder zou begeleiding vanuit de toezichthouder bij het uitvoeren van PIA's kunnen worden overwogen.

25 Veelheid aan modellen beschikbaar.
24 Voor nieuwe wetgeving, niet voor gegevensbeheerders.
26 De federale toezichthouder (BfDI) biedt geen begeleiding.
27 Voor gegevensbeheerders, niet voor nieuwe wetgeving. Zie artikel 34 wet inzake gegevensbescherming.
28 Versmissen, J.A.G. Terstegge, J.H.J., Siemers, K.M., en Tran, T.H. (2016), *Evaluatie Toetsmodel PIA Rijksdienst*. Utrecht: Privacy Management Partners.

Privacy en de bescherming van persoonsgegevens in nieuw beleid

In alle onderzochte landen spannen de toezichthouders zich in om privacy en de bescherming van persoonsgegevens een rol te laten spelen in nieuw beleid. De toezichthouders worden in alle landen geconsulteerd bij het ontwerpen van nieuwe wetgeving als die raakt aan de onderwerpen privacy en bescherming van persoonsgegevens (zie ook paragraaf 10.1.5). In het bijzonder worden toezichthouders geraadpleegd over de mate waarin wetsvoorstellen in overeenstemming zijn met wetgeving aangaande privacy en de bescherming van persoonsgegevens en de vraag of wetsvoorstellen handhaafbaar zijn voor de toezichthouder.

In alle onderzochte landen proberen overheden te anticiperen op nieuwe ontwikkelingen zoals big data, Internet of Things, quantified self, etc. Ook Privacy by Design wordt regelmatig genoemd als een belangrijk onderwerp en een mogelijke oplossing voor bepaalde problemen. In alle onderzochte landen zijn denktanks, platforms en onderzoeken ingesteld naar nieuwe ontwikkelingen en hoe daarop te anticiperen. Daarbij zijn geen grote verschillen waar te nemen tussen de landen onderling. Wel valt op dat hier veelal sprake is van veel papier en weinig praktijk. Bijvoorbeeld de term Privacy by Design wordt in alle landen regelmatig genoemd als een belangrijk concept, maar praktische voorbeelden zijn niet of nauwelijks beschikbaar. Kennelijk is er nog weinig zicht op hoe dit geconcretiseerd moet worden. Enigszins een uitzondering hierop is het Verenigd Koninkrijk, waar in elk geval een duidelijke visie heerst dat Privacy by Design gekoppeld zou moeten zijn aan PIA's: het uitvoeren van PIA's (breed beschouwde risico-/rechtmatigheidsanalyses) zou ontwerpvereisten moeten opleveren voor nieuwe systemen en regulering. In Nederland wordt, net als in de andere landen, in ruime mate verkennend onderzoek verricht naar en debat gevoerd over toekomstige ontwikkelingen.

Maatschappelijk debat

In verschillende van de onderzochte landen stelt de overheid zich actief op in het maatschappelijk debat. Dit is onder meer het geval in Nederland, Duitsland, Zweden, het Verenigd Koninkrijk en Frankrijk. In Ierland stelt de overheid zich beperkt actief op en in Roemenië en Italië is de overheid meer reactief dan proactief. In deze landen is enige/weinig dialoog tussen de overheid en burgerrechtenbewegingen en tussen overheid en burgers. Wat met betrekking tot nieuwe wetgeving vooral opvalt, is dat in sommige landen de overheid kiest voor een dialoog met/consultatie van belangengroepen (zoals in Duitsland, Zweden en Ierland), terwijl in andere landen de overheid kiest voor een dialoog met/consultatie van burgers via internetnetconsultaties (zoals in Nederland, het Verenigd Koninkrijk, Frankrijk en Italië). Een overzicht is weergegeven in tabel 10.6.

	Actieve opstelling van de overheid	Consultatie van (vooral) burgers of (vooral) belangengroepen?
Nederland	Ja	Burgers
Duitsland	Ja	Belangengroepen
Zweden	Ja	Belangengroepen
Verenigd Koninkrijk	Ja	Burgers
Ierland	Beperkt	Belangengroepen
Frankrijk	Ja	Burgers
Roemenië	Nee	Geen van beide
Italië	Nee	Burgers

Tabel 10.6 Opstelling van de overheid in het maatschappelijk debat en consultatievormen

De positie van Nederland verschilt niet veel met die van de meeste andere landen. Wat opvalt is dat in Nederland de dialoog tussen de overheid en de belangengroepen tot dusver niet erg uitgebreid is. Er werd meer ingezet op internetconsulaties, maar ook daarop is kritiek te leveren, onder meer omdat er geen uniform beleid hiervoor is en omdat vaak dezelfde (niet noodzakelijkerwijs representatieve) groep mensen reageert. Mogelijk gaat dit veranderen. In 2015 heeft zich een zogeheten privacycoalitie gevormd tussen verschillende personen en organisaties vanuit burgerrechten, journalistiek, strafrecht en wetenschap.[29] De overheid is een dialoog gestart met deze coalitie over onder meer onderwerpen als de opslag van gegevens[30] en big data[31] en lijkt voornemens te zijn deze dialoog voort te zetten en verder te versterken.

Informatiecampagnes

Toezichthouders in het domein van privacy en de bescherming van persoonsgegevens rekenen het tot hun taak informatie te verschaffen aan burgers, bedrijven en overheden over hun toezichtsdomein (zie ook paragraaf 10.1.5). Daarbij stellen ze via hun websites verschillende materialen beschikbaar, waaronder brochures, factsheets, rapporten en voorlichtingsmateriaal. In sommige landen, zoals het Verenigd Koninkrijk en Ierland, wordt ook lesmateriaal voor scholen beschikbaar gesteld.

Daarnaast worden in verschillende landen vanuit de overheid ook informatiecampagnes gevoerd. In Nederland en het Verenigd Koninkrijk zijn er relatief veel informatiecampagnes gevoerd, zowel online als via tv, maar ook in Ierland en Frankrijk zijn er informatiecampagnes. Nederland loopt voorop met het inzetten van apps. Duitsland, Zweden, Roemenië en Italië zijn minder actief als het gaat om informatiecampagnes en richten

29 https://visieopprivacy.nl/.

30 http://nos.nl/artikel/2028170-privacycoalitie-stop-op-wetgeving-dataopslag.html.

31 *Kamerstukken II* 2014-2015, 32 761, nr. 83, blz. 4; *Kamerstukken II* 2016-2017, 26 643, nr. 426, blz. 10.

zich meer op het verstrekken van voorlichtingsmateriaal. Verder is opvallend dat in verschillende landen de nadruk ligt op informatiecampagnes voor/over minderjarigen. Naast het genoemde lesmateriaal voor scholen in het Verenigd Koninkrijk en Ierland is er ook in Italië veel aandacht voor minderjarigen, onder meer op het onderwerp cyberpesten. De Nederlandse toezichthouder schenkt relatief weinig aandacht aan deze doelgroep.[32] Over de effectiviteit van de verschillende informatiecampagnes en het beschikbare voorlichtingsmateriaal is niets bekend. In vergelijking met de andere onderzochte landen loopt Nederland hier voorop, onder meer door informatiecampagnes die multimediaal (zowel online als via tv) en interactief (onder meer via apps) worden ingezet.

10.1.3 *Wet- en regelgeving*

Implementatie van de EU-richtlijn

Alle lidstaten zijn verplicht EU-richtlijn 95/46/EC voor de bescherming van persoonsgegevens om te zetten in nationale wetgeving. Bij de invoering was een deadline van drie jaar gesteld, dus in 1998. Vijf landen haalden deze deadline niet (Frankrijk, Luxemburg, Nederland, Duitsland en Ierland). Uiteindelijk is de richtlijn ook in deze landen met enige vertraging geïmplementeerd (zie tabel 10.7). Uiteindelijk was Frankrijk in 2004 het laatste met omzetting. Inmiddels is de nationale wetgeving in verschillende landen alweer herzien. In Nederland waren er belangrijke wijzigingen van de Wbp in 2012 en 2016, toen administratieve lasten werden verlaagd, boetes werden verhoogd en een meldplicht datalekken werd ingevoerd. In Duitsland waren belangrijke wetswijzigingen in 2003 en 2009, waarbij registraties werden vereenvoudigd en de positie van privacyfunctionarissen werd gewijzigd. In Roemenië werd de wet gewijzigd in 2005 omdat eerder was vastgesteld dat de vorige implementatie niet aan de eisen voldeed.

32 Enerzijds vormen minderjarigen een kwetsbare doelgroep en is aandacht hiervoor eenvoudig te rechtvaardigen. Anderzijds is wel de vraag of dit een taak moet zijn voor de toezichthouder of voor andere organisaties. De aankomende Algemene Verordening Gegevensbescherming zal de aandacht voor de bescherming van persoonsgegevens van minderjarigen verder versterken, waardoor het voor de hand ligt dat ook toezichthouders hiervoor meer aandacht zullen hebben.

	Implementatie	Belangrijke updates	Minimumimplementatie
Nederland	2001	2012, 2016	Minimum + meldplicht datalekken
Duitsland	2001	2003, 2009	Minimum + aantal extra zaken[33]
Zweden	1998	2007	Minimum + verdere invulling
Verenigd Koninkrijk	1998	2000	Minimum + good practices als PIA's en 'Privacy by Design'-methoden
Ierland	2003	N/A	Minimum op paar punten niet gehaald (zie par. 6.3)
Frankrijk	2004	2011	Minimum + aanvullingen gezondheidsgegevens en kinderen
Roemenië	2001	2005	Minimum + gedragscodes verplicht voorleggen aan toezichthouder
Italië	1996	2003[34]	Minimum + extra regels voor gegevensbeheerders

Tabel 10.7 Implementatie van de EU-richtlijn[35]

Implementatie van EU-richtlijnen houdt in dat deze minimaal moeten worden geïmplementeerd. Het staat landen echter vrij om hogere beschermingsnormen te implementeren en in nationale wetgeving verdere invulling te geven aan de richtlijnen. In alle onderzochte landen is het minimum van de richtlijn geïmplementeerd, al waren daar in Roemenië twee rondes voor nodig en staat de wetgeving in Ierland nog steeds op gespannen voet met de richtlijn (zie paragraaf 6.3). In de meeste landen zijn enkele (ten opzichte van de richtlijn) aanvullende bepalingen opgenomen in de nationale wetgeving. Een overzicht is weergegeven in tabel 10.7.
Tabel 10.7 laat zien dat Nederland de EU-richtlijn net als andere landen heeft ingevuld volgens de minimale eisen, met uitzondering van de meldplicht datalekken. Nederland heeft, net als Duitsland en Frankrijk, de wetgeving recent nog geactualiseerd, terwijl dat voor andere landen langer geleden is.

Sectorale wetgeving
Naast de algemene implementatie van EU-richtlijn 95/46/EC hebben alle onderzochte landen ook sectorale wetgeving ingevoerd die meer specifiek is toegesneden op het verwerken van persoonsgegevens in bepaalde sectoren. Gelet op de grote hoeveelheid verschillende sectoren waarvoor wetgeving aanwezig is, is het onmogelijk om hier een

33 Onder meer pseudonimisering, data thrift & data avoidance, video surveillance en data protection audits.
34 Deze update werd van kracht in 2004.
35 Grotendeels gebaseerd op http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm.

uitputtend overzicht van sectorale wetgeving weer te geven. Bijvoorbeeld in Zweden zijn er al meer dan 300 sectorale wetten en regelingen die de bescherming van persoonsgegevens verder invullen.
In alle onderzochte landen is sectorale wetgeving aanwezig voor onder meer de medische sector, de telecomsector, de financiële sector, belastingdiensten, inlichtingendiensten, toegang tot overheidsgegevens, cameratoezicht en de strafrechtsector. In tabel 10.8 is een overzicht weergegeven van enkele belangrijke sectoren (gezondheidszorg, telecommunicatie, financiën, strafrecht en overheidsgegevens) per land. In dit overzicht is te zien dat alle landen sectorale wetgeving hebben op het terrein van gezondheidszorg (behalve in het Verenigd Koninkrijk, waar een gedragscode bestaat), telecommunicatie, de financiële sector (behalve in Nederland, waar een gedragscode bestaat), strafrecht (behalve Ierland, waar een gedragscode bestaat, en Italië) en overheidsgegevens (waarbij toegangsrechten in Italië beperkt zijn). Ter illustratie, in Nederland gaat het om respectievelijk de WGBO, de Telecommunicatiewet, de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen, de Wpg en Wjsg en de Wob.[36]

	Gezondheids-zorg	**Telecom**	**Financiën**	**Strafrecht**	**Overheids-gegevens**[37]
Nederland	Ja	Ja	Nee[38]	Ja	Ja
Duitsland	Ja	Ja	Ja	Ja	Ja
Zweden	Ja	Ja	Ja	Ja	Ja
Verenigd Koninkrijk	Nee[39]	Ja	Ja	Ja	Ja
Ierland	Ja	Ja	Ja	Nee[40]	Ja
Frankrijk	Ja	Ja	Ja	Ja	Ja
Roemenië	Ja	Ja	Ja	Ja	Ja
Italië	Ja	Ja	Ja	Nee[41]	Gedeeltelijk[42]

Tabel 10.8 Sectorale wetgeving voor de bescherming van persoonsgegevens

36 De Wob (Wet openbaarheid van overheidsinformatie) richt zich niet specifiek op persoonsgegevens en valt daarmee grotendeels buiten de reikwijdte van dit onderzoek.
37 Zie ook het overzicht op: https://en.wikipedia.org/wiki/Freedom_of_information_laws_by_country.
38 Er is in Nederland wel een Gedragscode Verwerking Persoonsgegevens Financiële Instellingen: http://wetten.overheid.nl/BWBR0033201/2010-04-26.
39 Er is in het Verenigd Koninkrijk wel een gedragscode: Subject access code of practice. Zie: https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf.
40 Er is in Ierland wel een gedragscode voor de politie. Zie http://www.garda.ie/Controller.aspx?Page=136&Lang=1.
42 Hoofdstuk V van wet no. 241 d.d. 7 augustus 1990 verschaft toegang tot overheidsdocumenten, maar de aanvrager dient belanghebbende te zijn. Voor overheidsinstellingen is verder titel III van hoofdstuk II van de DPACode van toepassing, maar deze heeft geen directe betrekking op overheidsgegevens.
41 Verwacht in Annex C van de DPCode maar nooit gerealiseerd.

Dieper ingaand op het strafrecht komt het volgende beeld naar voren. In Nederland is er specifieke wetgeving voor de bescherming van persoonsgegevens in het strafrecht voor enerzijds de politie (de wet politiegegevens, Wpg) en anderzijds voor het Openbaar Ministerie (Wjsg). Daarnaast is deze wetgeving verder uitgewerkt in respectievelijk het Besluit politiegegevens en het Besluit justitiële en strafvorderlijke gegevens. In Duitsland is de bescherming van persoonsgegevens in het strafrecht uitgewerkt in het Bundesgrenzschutzgesetz 1994 (de Duitse politiewet) waarin de verwerking van persoonsgegevens door de politie is geregeld.[43] In Zweden regelt de Police Data Protection Act (1998:622) hoe de politie mag omgaan met persoonsgegevens. Deze wet regelt ook dat de politie bevoegd is strafrechtelijke dossiers en DNA-informatie bij te houden. Een nieuwe wet, de Police Data Protection Act (2010:361), is op 1 maart 2012 van kracht geworden.[44] In Frankrijk is in 2014 een wet in werking getreden die de Franse politie en inlichtingendiensten meer bevoegdheden heeft gegeven, waaronder het verzamelen van gegevens zonder rechterlijke machtiging.[45] In het Verenigd Koninkrijk is de verwerking van strafrechtelijke persoonsgegevens geregeld in het Criminal Justice and Data Protection Protocol.[46] In Ierland is de verwerking van strafrechtelijke persoonsgegevens geregeld in een gedragscode (An Garda Síochána).[47] In Roemenië is er specifieke wetgeving (Law 238/2009) voor de verwerking van strafrechtelijke persoonsgegevens. Daarnaast bevat de politiewetgeving (Law 218/2002) aanvullende bepalingen.[48] Alleen in Italië is er geen specifieke wet- of regelgeving voor de bescherming van persoonsgegevens in het strafrecht (afgezien uiteraard van de generieke wetgeving op het terrein van strafrechtelijke opsporing en ter bescherming van persoonsgegevens).[49] Merk op dat EU-richtlijn 2016/680 hierin verandering zal brengen.

Alle wetgeving die in de landen is geïmplementeerd om persoonsgegevens te beschermen kent specifieke bepalingen voor de omgang met bijzondere categorieën persoonsgegevens (de zogeheten gevoelige persoonsgegevens). Dit is het gevolg van de harmoniserende werking van richtlijn 95/46/EC. Wanneer de positie van Nederland wordt vergeleken met andere landen, valt op dat Nederland via sectorale wetgeving ruim nadere invulling heeft gegeven aan de bescherming van persoonsgegevens. In het bijzonder met de strafrechtelijke wetgeving en aanvullende besluiten valt op dat Nederland voorligt op andere landen, waar dit vaak geregeld is als onderdeel van de politiewet (zoals in Duitsland, Zweden en Roemenië), op een lager niveau (zoals een gedragscode in Ierland) of helemaal niet (zoals in Italië).

43 http://policehumanrightsresources.org/wp-content/uploads/2016/08/Federal-Police-Act-Germany-1994.pdf. Subsectie 2, deel 1 gaat over het verzamelen van gegevens, deel 2 gaat over het verwerken en gebruik van gegevens.

44 https://polisen.se/Global/.../Polisen_en_presentation_110506.pdf, p. 17.

45 http://www.hldataprotection.com/tags/france/.

46 Criminal Justice and Data Protection (Protocol No.36) Regulations 2014, SI 2014/3141.

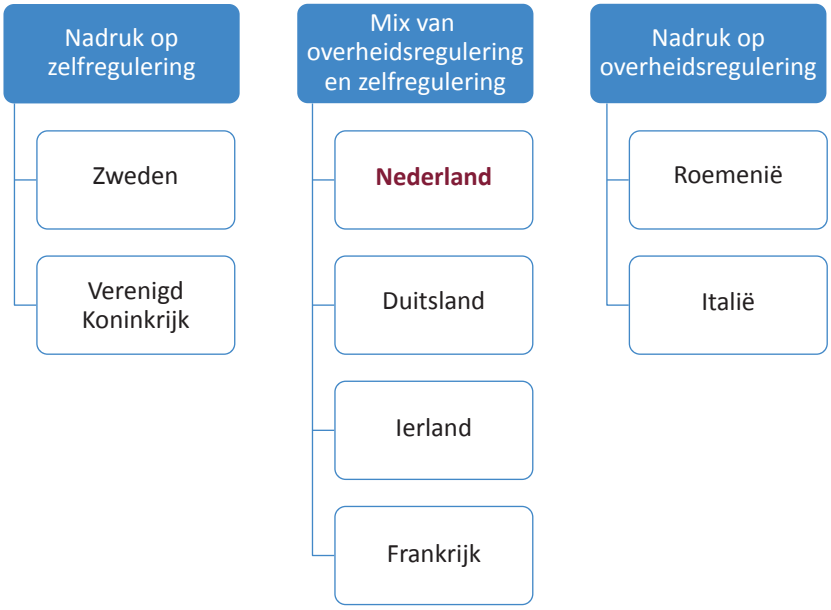
47 http://www.garda.ie/Controller.aspx?Page=136&Lang=1.

48 Law No. 218/2002 on the organizing and functioning of the Romanian Police.

49 Koops, B.J. (2016), *Criminal Investigation and Privacy in Italian Law* (December 21, 2016). TILT Law & Technology Working Paper Series, version 1.0, December 2016, p. 34. Available at SSRN: https://ssrn.com/abstract=2888422 or http://dx.doi.org/10.2139/ssrn.2888422.

Zelfregulering en gedragscodes

Artikel 27 van EU-richtlijn 95/46/EC schrijft voor dat lidstaten het gebruik van gedragscodes moeten aanmoedigen. De vraag is of dat ook daadwerkelijk in alle landen gebeurt. Uit de vergelijking van de landen in dit onderzoek blijkt dat landen als Zweden en het Verenigd Koninkrijk een lange traditie van zelfregulering hebben en daarop veel meer de nadruk leggen dan op wetgeving en regulering, inclusief regulering vanuit de toezichthouder. Landen als Nederland, Duitsland, Ierland en Frankrijk maken gebruik van een mix van zelfregulering en overheidsregulering. In Roemenië en Italië ligt de nadruk vooral op overheidsregulering, grotendeels via richtlijnen, en regulering vanuit de toezichthouders. Zie voor een overzicht figuur 10.9.



Figuur 10.9 Zelfregulering versus overheidsregulering

Nederland neemt een positie in het midden in, waarbij sprake is van een mix van overheidsregulering en zelfregulering. Het aantal gedragscodes dat jaarlijks wordt voorgelegd aan de Autoriteit Persoonsgegevens is niettemin erg gering (2 in 2016, 3 in 2015, 2 in 2014, 4 in 2013 en 4 in 2012).[50] Ook in Duitsland komt dit moeizaam van de grond.[51] Zowel in Nederland als in Duitsland wordt het opstellen van gedragscodes gezien als een langdurig, tijdrovend en kostbaar proces met weinig concrete voordelen. Het gebruik van modelconvenanten, aangeboden door de toezichthouder, is iets dat we in andere landen niet zijn tegengekomen. De Autoriteit Persoonsgegevens heeft meerdere beleidsregels, voorheen richtsnoeren genoemd, gepubliceerd op de website. Dit is vergelijkbaar met toezichthouders in andere landen.

50 AP (2017), Bijlage *Jaaverslag 2016*. Den Haag: AP, p. 5.
51 Zie paragraaf 3.4.

10.1.4 *Implementatie*

Privacyfunctionarissen

In veel landen is het (nog) niet verplicht om privacyfunctionarissen aan te stellen. Wanneer de AVG in mei 2018 van kracht zal worden, zullen veel organisaties wel verplicht zijn om een privacyfunctionaris aan te stellen. Naar schatting zijn er vanaf 2018 wereldwijd zo'n 75.000 privacyfunctionarissen nodig.[52] Deze privacyfunctionarissen zijn niet alleen binnen de EU nodig, maar ook daarbuiten, wanneer bedrijven samenwerken of handel drijven met organisaties in de EU.

In de onderzochte landen zijn privacyfunctionarissen niet verplicht, met uitzondering van Duitsland, waar een verplichting geldt voor organisaties met 10 werknemers of meer. Duitsland was overigens ook het eerste land waar (in 1970) iemand de rol van privacyfunctionaris vervulde. Omdat privacyfunctionarissen niet verplicht zijn, worden er ook geen statistieken bijgehouden van de aantallen privacyfunctionarissen in een land. In sommige landen worden door de toezichthouder wel registratiemogelijkheden aangeboden. In tabel 10.9 is een overzicht te zien van de beschikbare gegevens.

	Privacyfunctionaris verplicht?	**Aantal geregistreerde privacyfunctionarissen**	**Aantal privacyfunctionarissen per miljoen inwoners**
Duitsland	Ja	> 700.000[53]	8.593
Zweden	Nee	7.513[54]	762
Frankrijk	Nee	16.400[55]	247
Nederland	Nee	722[56]	42
Verenigd Koninkrijk	Nee	Geen gegevens	N/A
Ierland	Nee	Geen gegevens	N/A
Italië	Nee	Geen gegevens	N/A
Roemenië	Nee	Vrijwel geen	Vrijwel geen

Tabel 10.9 Privacyfunctionarissen

52 http://www.v3.co.uk/v3-uk/news/2477538/gdpr-will-require-at-least-75-000-data-protection-officers.

53 Schatting: in Duitsland zijn 3.647.326 bedrijven waarvan 80% mkb is. https://www.destatis.de/EN/FactsFigures/NationalEconomyEnvironment/EnterprisesCrafts/EnterprisesCrafts.html. Een minimumschatting is derhalve dat er ruim 700.000 bedrijven zijn waar een privacyfunctionaris is aangesteld. Waarschijnlijk is het aantal nog groter, aangezien onder het mkb ook bedrijven met meer dan 10 werknemers vallen.

54 In Zweden stonden in 2015 7.513 bedrijven met een privacyfunctionaris geregistreerd, maar deze rollen werden ingevuld door 4.756 personen. In Zweden kunnen werknemers de rol van privacyfunctionaris voor meerdere bedrijven tegelijkertijd invullen.

55 In 2015.

56 In 2016.

Omdat in grote landen meer bedrijven en mogelijk dus ook meer privacyfunctionarissen zijn te vinden, is in tabel 10.9 ook het aantal privacyfunctionarissen per miljoen inwoners van een land berekend, zodat een betere vergelijking kan worden gemaakt. Uit het overzicht valt op dat Nederland meer privacyfunctionarissen heeft dan Roemenië, maar aanzienlijk achterblijft bij landen als Zweden, Frankrijk en Duitsland. Door een gebrek aan gegevens kunnen de overige landen niet in de vergelijking worden betrokken. Het is in elk geval duidelijk dat het aantal privacyfunctionarissen in Nederland vanaf 2018 flink zal moeten groeien. Hiervoor zullen onder meer opleidingen nodig zijn.

Beveiligingsmaatregelen
In meerdere landen zijn door de toezichthouders richtlijnen ontwikkeld voor de beveiliging van persoonsgegevens. Daarnaast wordt gebruikgemaakt van standaard ISO-beveiligingsnormen. In tabel 10.10 is een overzicht weergegeven met daarin welke landen richtlijnen hebben voor beveiliging en in welke landen de toezichthouder certificaten, zegels en keurmerken uitreikt voor adequate beveiliging.

	Richtlijnen voor beveiliging	**Certificering/zegel/keurmerk vanuit de toezichthouder**
Nederland	Ja	Nee[57]
Duitsland	Ja	Ja
Zweden	Nee	Nee[58]
Verenigd Koninkrijk	Nee	Ja (in voorbereiding)
Ierland	Ja	Nee
Frankrijk	Ja	Ja
Roemenië	Ja	Nee
Italië	Ja	Nee

Tabel 10.10 Beveiligingsmaatregelen

In Nederland heeft de Autoriteit Persoonsgegevens richtlijnen uitgevaardigd voor de beveiliging van persoonsgegevens. Daarnaast is er een code voor informatiebeveiliging waarvan gebruik kan worden gemaakt. In landen als Roemenië en Italië zijn er minimumvereisten voor beveiliging. In andere landen, waaronder Nederland, Ierland en Frankrijk, zijn de beveiligingsrichtlijnen meer indicatief. In Zweden en het Verenigd Koninkrijk ontbreken beveiligingsrichtlijnen (al kunnen uiteraard de ISO-standaarden worden gebruikt). In Duitsland is er een speciale overheidsorganisatie die zich richt op informatiebeveiliging, het Bundesamt für Sicherheit in der Informationstechnik (BSI),[59]

57 NEN/ISO-normen kunnen wel worden gecertificeerd, maar door particuliere organisaties.
58 NEN/ISO-normen kunnen wel worden gecertificeerd, maar door particuliere organisaties.
59 In het Engels: Federal Office for Information Security (FOIS).

die zelf standaarden ontwikkeld. De andere onderzochte landen kennen geen vergelijkbaar overheidsinstituut.
Opvallend is dat in bepaalde landen de toezichthouder zelf certificaten, zegels of keurmerken uitreikt wanneer sprake is van een adequate beveiliging. Dit is het geval in Duitsland en Frankrijk. In het Verenigd Koninkrijk is dit in voorbereiding. Nederland (evenals Zweden, Ierland, Roemenië en Italië) kent een dergelijke praktijk niet.

Transparantie
In zijn algemeenheid valt te stellen dat het slecht gesteld is met de transparantie voor wat betreft de verwerking van persoonsgegevens.[60] Doorgaans wordt aangenomen dat gegevensbeheerders door middel van het gebruik van privacyvoorwaarden en/of algemene voorwaarden transparantie bieden over welke persoonsgegevens ze verzamelen en voor welke doeleinden deze persoonsgegevens worden verwerkt.[61] Het probleem is echter dat mensen deze privacyvoorwaarden niet lezen (in de EU leest gemiddeld 11% de hele tekst).[62] Het lezen van deze documenten kost erg veel tijd. Onderzoek wijst uit dat het op jaarbasis 244 uur per persoon zou kosten om alles te lezen.[63] Dat terwijl uit ander onderzoek blijkt dat mensen slechts bereid zijn hieraan 1-5 minuten te besteden.[64] Zelfs mensen die moeite doen om deze teksten te lezen, hebben problemen de juridische en technische teksten te doorgronden. Soms zijn er heldere korte privacyvoorwaarden beschikbaar, maar dan is het de vraag hoeveel informatie deze echt bieden.[65]
Opvallend is dat de Nederlandse overheid via de website www.mijnoverheid.nl tracht de transparantie te verbeteren ten aanzien van persoonsgegevens die worden verwerkt over burgers. Deze dienst lijkt breed gebruikt te worden door burgers: sinds begin 2017 zijn er meer dan zes miljoen geregistreerde gebruikers.[66] Onduidelijk is echter hoe vaak deze gebruikers deze dienst gebruiken. Een dergelijk initiatief zijn we in geen van de andere onderzochte landen tegengekomen.
Er zijn geen grote verschillen te duiden in transparantie in de onderzochte landen. Dat maakt het lastig om van andere landen te leren, terwijl het gebrek aan transparantie een wezenlijk probleem is, onder meer omdat een gebrek aan transparantie het lastig maakt voor burgers om hun rechten met betrekking tot hun persoonsgegevens uit te oefenen. Hier is sprake van een breder probleem, dat ligt in de complexiteit van de

60 Custers B.H.M., Hof S. van der & Schermer B. (2014), 'Privacy Expectations of Social Media Users. The Role of Informed Consent in Privacy Policies', *Policy and Internet* 6(3): 268-295.
61 Custers B.H.M., Hof S. van der, Schermer B.W., Appleby-Arnold S., Brockdorff & N. (2013), 'Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law', *Script-ed: a journal of law and technology* 10(4): 435-457.
62 Consent Country Report The Netherlands (2012), p. 4.
63 McDonald, A. M. & Cranor, L. F. (2008), 'The cost of reading privacy policies', *I/S Journal for Law and Policy for the Information Society.*http://www.aleecia.com/authors-drafts/readingPolicyCost-AV.pdf.
64 Van den Berg, B. en Van der Hof, S. (2012), What happens to my data? A novel approach to informing users of data processing practices, 17 *First Monday*.
65 Toubiana, V., and Nissenbaum, H. (2011), 'An Analysis of Google Logs Retention Policies', *Journal of Privacy and Confidentiality* 3 (1): Article 2.
66 https://www.logius.nl/diensten/mijnoverheid/actueel/mijnoverheid-in-cijfers/.

technologie.[67] Kort gezegd komt dit erop neer dat het lastig is de complexiteit van gegevensverwerkingen eenvoudig en begrijpelijk uit te leggen; wanneer daarentegen wordt gekozen voor een eenvoudig uitleg, is het gevolg veelal dat de complexiteit zodanig wordt gereduceerd dat niet langer een adequaat beeld wordt gegeven van de realiteit.

10.1.5 *Toezicht en handhaving*

Toezichthouders
In alle onderzochte landen is er een speciale toezichthouder voor het toezicht op privacy en de bescherming van persoonsgegevens. Alleen in Roemenië was in eerste instantie deze toezichthoudende taak belegd bij de nationale ombudsman, maar na een audit vanuit de EU werd ook hier een aparte toezichthouder opgericht.

	Budget (miljoen euro)	**Aantal medewerkers**
Duitsland (2016)	13,7 (federaal)[68]	110 (federaal)
Verenigd Koninkrijk (2016)	26,5[69]	442[70]
Italië (2015)	19,2	121
Frankrijk (2016)	19	192
Nederland (2015)	8,1[71]	73
Ierland (2017)	7,5[72]	60
Zweden (2014)	4,6	40
Roemenië (2015)	0,7	41

Tabel 10.11 Toezichthouders: budgetten en aantallen medewerkers[73]

67 Zie ook: Custers B.H.M., Hof S. van der & Schermer B. (2014), 'Privacy Expectations of Social Media Users. The Role of Informed Consent in Privacy Policies', Policy and Internet 6(3): 268-295; Custers B.H.M. (2016), 'Click here to consent forever; Expiry dates for informed consent', *Big Data & Society*: 1-6.

68 De 16 toezichthouders in de respectievelijke bondsstaten zijn niet meegenomen in dit overzicht.

70 Waarvan 409 medewerkers fulltime in dienst waren.

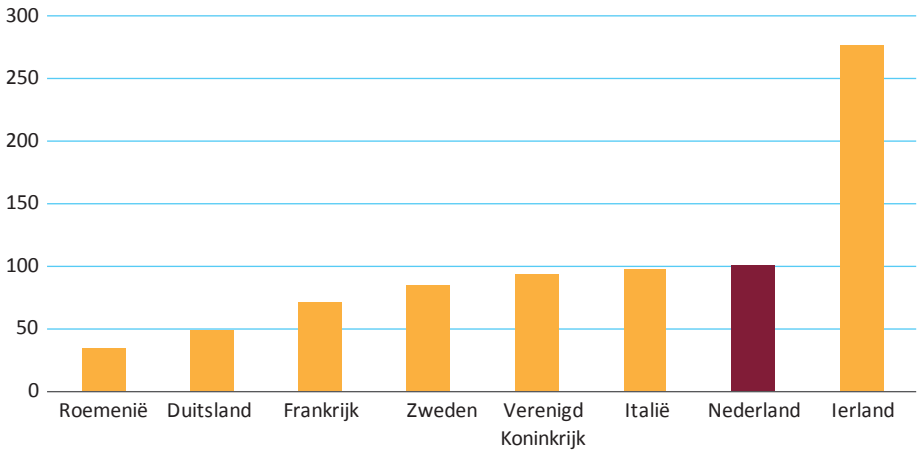
69 Jaarbudget in 2016 was 23 miljoen Britse ponden.

71 Het ministerie van Veiligheid en Justitie en de Autoriteit Persoonsgegevens zijn in 2016 een traject gestart waarin een onafhankelijk adviesbureau de consequenties in kaart brengt van de versteviging van bevoegdheden van de Autoriteit Persoonsgegevens door de AVG voor de capaciteit en het budget van dit college (*Kamerstukken II* 2016-2017, 26643, nr. 426, blz. 9). Dit heeft geleid tot het volgende rapport: Andersson Elffers Felix (2017), *Organisatorische vertaling Verordening & Richtlijn gegevensbescherming.* Utrecht: Andersson Elffers Felix. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/eindrapportage_aef.pdf.

72 In 2017. Het budget voor de Ierse toezichthouder is de laatste jaren sterk gestegen: in 2015 was het budget 3,65 miljoen euro, in 2016 was het budget 4,7 miljoen euro en in 2017 7,5 miljoen euro.

73 De meest recente beschikbare cijfers zijn gebruikt.

In tabel 10.11 is een overzicht te zien van het jaarlijks budget van de toezichthouders in de verschillende landen en het aantal medewerkers dat ze in dienst hebben. Voor Duitsland is de vergelijking lastig te maken, omdat er naast een federale toezichthouder ook 16 toezichthouders in de bondsstaten zijn. Als deze worden meegenomen in de cijfers, staat Duitsland hoog bovenaan de lijst met beschikbare budgetten en aantallen medewerkers. De grote landen (Duitsland, het Verenigd Koninkrijk, Italië en Frankrijk) hebben duidelijk de grootste budgetten beschikbaar gesteld aan de toezichthouders. Een eerlijkere vergelijking is echter om de budgetten te vergelijken wanneer rekening wordt gehouden met het bruto nationaal product van elk land. Dit is weergegeven in figuur 10.10. In de figuur is zichtbaar dat Roemenië in verhouding het minste uitgeeft, en Ierland[74] het meeste.

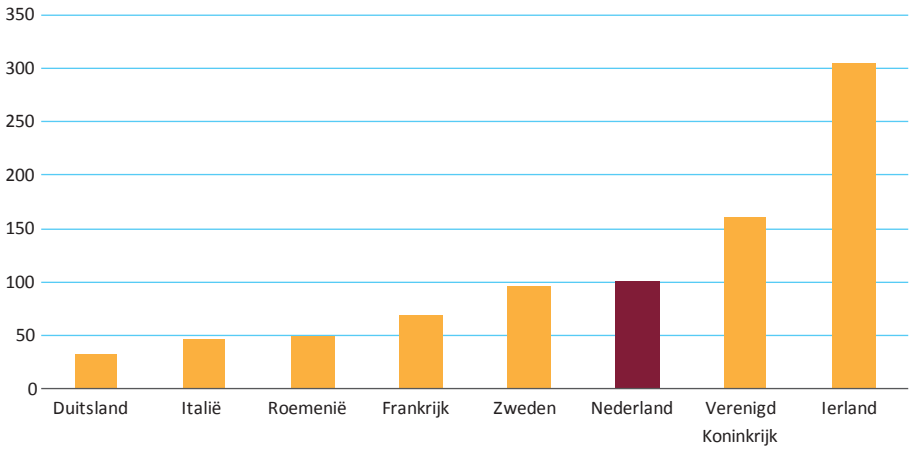


Figuur 10.10 Uitgaven aan de toezichthouder in verhouding tot het bruto nationaal product, waarbij Nederland op 100 is gesteld

Wat opvalt in de vergelijking met andere landen is dat de kosten van de toezichthouder in Nederland redelijk gelijke tred houden met andere landen (in elk geval met Zweden, het Verenigd Koninkrijk en Italië). Duitsland kan niet goed in deze vergelijking worden betrokken omdat alleen de cijfers van de federale toezichthouder zijn meegenomen in deze vergelijking – wanneer de cijfers voor de 16 toezichthouders in de bondsstaten zouden worden meegenomen in de vergelijking zou Duitsland met kop en schouders bovenaan staan wat betreft budgetten en aantallen medewerkers. De opvallende uitschieter in figuur 10.10 is Ierland. Het budget voor de Ierse toezichthouder is de laatste jaren sterk gestegen. Het budget voor 2017 is meer dan een verdubbeling ten opzichte van het budget van 2015.
Uit tabel 10.11 valt op te maken dat het aantal medewerkers in dienst bij de verschillende toezichthouders redelijk gelijke pas houdt met het beschikbare budget, al slagen landen als Roemenië en het Verenigd Koninkrijk er in om voor de beschikbare budgetten

74 Eigenlijk geeft Duitsland het meeste uit aan de toezichthouders, wanneer de 16 toezichthouders van de bondsstaten worden meegenomen in de vergelijking.

aanzienlijk meer medewerkers in dienst te hebben dan gemiddeld en blijft het aantal medewerkers in Italië enigszins achter bij het beschikbare budget.
Ook hier is het niet eerlijk om absolute aantallen te vergelijken, want dan komen grote landen altijd beter uit de bus dan kleine landen. Vandaar dat in figuur 10.11 de aantallen medewerkers van de toezichthouder zijn weergegeven in verhouding tot het aantal inwoners van het betreffende land, waarbij Nederland op 100 is gesteld. Wat betreft het aantal medewerkers bij de toezichthouder neemt Nederland een gemiddelde positie in. Italië[75] heeft de minste medewerkers per inwoner, Ierland heeft de meeste medewerkers per inwoner.



Figuur 10.11 Aantallen medewerkers bij de toezichthouder in verhouding tot het aantal inwoners van een land, waarbij Nederland op 100 is gesteld

Taken en bevoegdheden
De toezichthouders in alle onderzochte landen houden zich bezig met een vergelijkbaar palet aan activiteiten. De activiteiten zijn geclusterd rondom onderwerpen als toezicht houden, adviseren en informatie verstrekken. De meeste toezichthouders houden een uitgebreide website met informatiemateriaal bij. Opvallend is dat de Nederlandse toezichthouder geen uitgebreide dialoog onderhoudt met burgerrechtenorganisaties (in tegenstelling tot bijvoorbeeld Duitsland, Frankrijk en het Verenigd Koninkrijk; zie hiervoor).
De toezichthouders beschikken over een redelijk uitgebreid arsenaal aan bevoegdheden en sanctiemogelijkheden. Een overzicht hiervan is weergegeven in tabel 10.12. Gelet op de maximale boetes die door de toezichthouder kunnen worden opgelegd, valt op de Nederland sinds 2016 (toen de boetebevoegdheden aanzienlijk zijn verhoogd) weer redelijk in de pas loopt met andere landen. Zeker met de invoering van boetes die afhankelijk zijn van de omzet van bedrijven is Nederland koploper (samen met Roeme-

75 Duitsland heeft aanzienlijk meer medewerkers per inwoner wanneer de medewerkers van de 16 toezichthouders in de deelstaten worden meegenomen in de vergelijking.

nië). Deze vorm van boetes loopt vooruit op de boetes die mogelijk worden vanaf 2018 wanneer de AVG van kracht wordt. Een strafrechtelijke aanpak is in de meeste landen mogelijk, waarbij maximale gevangenisstraffen van 2 tot 5 jaar kunnen worden opgelegd.

	Maximale boete door toezichthouder (euro)[76]	**Strafrecht**[77] **(maximale gevangenisstraf)**	**Aantal vragen/ meldingen**	**Aantal onderzoeken**	**Aantal klachten van burgers**
Nederland	820.000 of 10% van de omzet	Ja (max. 6 maanden)	8.799	197	303[78]
Duitsland	300.000	Ja (max. 2 jaar)	6.687	Geen data	3.699
Zweden	105.000[79]	Ja (max. 2 jaar)	12.000	Geen data	214 + 223[80]
Verenigd Koninkrijk	580.000[81]	Ja (geen max. onbekend)	16.300 (meldingen) + 204.700 (vragen)	Geen data	5.100
Ierland	100.000	Ja (max 12 maanden)	30.000	52	932
Frankrijk	3.000.000	Ja (max. 5 jaar)	Geen data	421	7.908
Roemenië	22.000 of 2% van de omzet	Ja (max. 3 jaar)	7.500 (meldingen) + 1242 (vragen)	229	1.074
Italië	300.000	Ja (max. 3 jaar)	25.600	303	Geen data

Tabel 10.12 Bevoegdheden en activiteiten van toezichthouders

77 https://iapp.org/media/pdf/resource_center/BM-2016-Global-Enforcement-Report.pdf.
76 https://iapp.org/media/pdf/resource_center/BM-2016-Global-Enforcement-Report.pdf.
78 Dit betreft het aantal bemiddelingen. De Autoriteit Persoonsgegevens registreert en behandelt geen klachten. Burgers kunnen wel zaken melden, dit is in kolom vier van tabel 10.12 weergegeven.
80 214 klachten en 223 kwalificerende vragen.
79 1 miljoen Zweedse kronen.
81 500.000 Britse ponden.

Gebruik van bevoegdheden

Wat betreft het aantal vragen, meldingen, onderzoeken en klachten van burgers zijn beperkte data beschikbaar. Hetzelfde geldt voor het totaal aan geïnde boetes.[82] Daar komt bij dat in de beschikbare gegevens lastig is te onderscheiden wat de verschillen zijn tussen meldingen, vragen en klachten. Onderzoeken zijn in de cijfers wel duidelijk te onderscheiden, maar deze cijfers zijn weer lastig te vergelijken omdat sommige onderzoeken klein en kortdurend zijn, terwijl andere onderzoeken een groot team maanden of zelfs jaren bezighouden. Deze cijfers kunnen dus niet goed worden vergeleken.

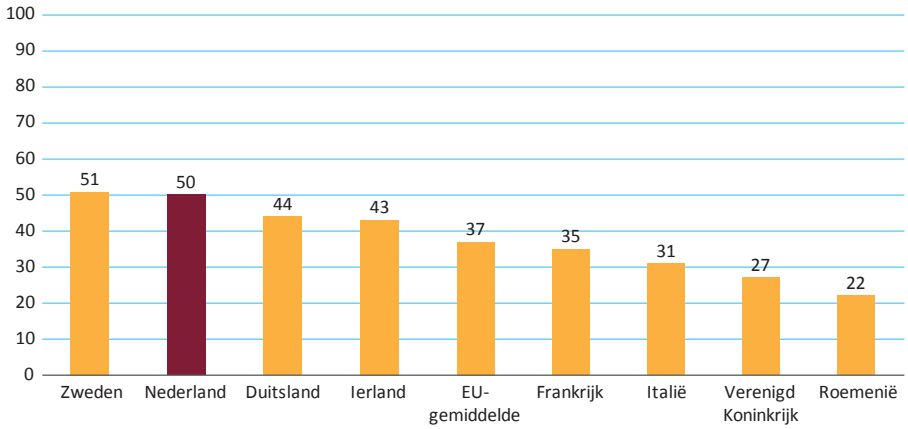
Wel zijn er enkele algemene tendensen op te merken. Zo neigt de toezichthouder in Duitsland naar een steeds striktere handhaving. In het verleden werden weinig boetes uitgedeeld. In Nederland is dezelfde tendens waarneembaar. De Autoriteit Persoonsgegevens heeft de afgelopen jaren ook meer medewerkers in dienst genomen die ervaring hebben met procederen en heeft de afgelopen jaren ook meer rechtszaken gevoerd.

Verder valt op dat de Nederlandse toezichthouder weinig tot geen dialoog voert met de organisaties waarop toezicht wordt gehouden. Wel voert de AP dialogen met brancheorganisaties in de publieke en private sector. De toezichthouder organiseert zelf geen workshops, symposia of opleidingen, maar spreekt wel in toenemende mate op congressen en symposia. Verder lijkt de Autoriteit Persoonsgegevens terughoudend te zijn in het afhandelen van vragen van burgers en organisaties over hoe wet- en regelgeving moet worden nageleefd of hoe 'privacy-proof' te zijn. Zodoende kan gesteld worden dat het ondersteunen van burgers beperkt is. Met andere woorden: er is weinig tot geen begeleiding van en overleg met degenen op wie toezicht wordt gehouden.

Reputatie

De bekendheid en reputatie van toezichthouders kan bepalend zijn voor een effectieve handhaving. In figuur 10.12 is weergegeven in hoeverre burgers hun toezichthouder op het terrein van privacy en de bescherming van persoonsgegevens kennen. Uit het overzicht blijkt dat in de EU gemiddeld slechts ongeveer een op de drie mensen de toezichthouder kent. Hier is dus nog wel wat ruimte voor verbetering. In vergelijking met andere landen scoort Nederland niet slecht in dit overzicht: in Nederland kent ongeveer de helft van de mensen de toezichthouder. Binnen Europa zijn in Zweden en in Nederland de toezichthouders het meest bekend.

82 De Roemeense toezichthouder inde in 2015 in totaal 250.000 euro aan boetes en de Italiaanse toezichthouder inde in totaal 3,5 miljoen euro aan boetes.



Figuur 10.12 Percentage mensen dat de toezichthouder kent[83]

In dit onderzoek bleek het niet mogelijk de reputatie van de toezichthouders in de afzonderlijke landen vast te stellen. Zo is onduidelijk of in bepaalde landen de toezichthouder wordt gevreesd of dat de samenwerking juist als prettig wordt ervaren. In Nederland lijkt de Autoriteit Persoonsgegevens niet te worden gevreesd (al kan dat veranderen nu de boetes hoger worden en de handhaving strikter), maar er is ook weinig tot geen samenwerking tussen toezichthouder en de organisaties waarop toezicht wordt gehouden.

10.2 Antwoord op de hoofdvraag

In de vorige paragraaf zijn de acht landen met elkaar vergeleken op de verschillende aspecten. Met deze resultaten is het mogelijk antwoord te geven op de hoofdvraag van dit onderzoek:

'Wat is de positie van Nederland met betrekking tot de bescherming van de persoonsgegevens van de burgers in vergelijking met enkele andere landen binnen de Europese Unie?'

Algemene situatie

In het algemeen kan worden gesteld dat Nederlanders, zowel in absolute zin als in vergelijking met inwoners van andere EU-lidstaten, een hoge mate van bewustzijn en zelfredzaamheid vertonen als het aankomt op de bescherming van hun privacy en persoonsgegevens. Nederlanders zijn veel online, zijn zich bewust van gevolgen van het achterlaten van persoonsgegevens en nemen de nodige maatregelen, waaronder het instellen van beveiligingsmaatregelen, het uitzetten van cookies en het aanpassen van profielinstellingen. Daar staat wel tegenover dat Nederlanders, in vergelijking met inwoners van andere EU-lidstaten, weinig bezorgd lijken te zijn over hun privacy en

83 Gebaseerd op Eurobarometer 431 (2015), p. 52.

de bescherming van persoonsgegevens en een hoge mate van acceptatie en berusting vertonen. Bepaalde risico's worden niet gezien, zoals het risico om slachtoffer te worden van fraude.

Conclusie 1. Nederlanders vertonen (m.b.t. de bescherming van hun persoonsgegevens) een hoge mate van bewustzijn en zelfredzaamheid. Tegelijkertijd is er een lage bezorgdheid/hoge mate van acceptatie en berusting.

Wat betreft de politiek en de media kan gesteld worden dat in Nederland ruime aandacht is voor privacy en de bescherming van persoonsgegevens. In de politiek spelen deze onderwerpen regelmatig een rol in het debat. Wel richt het debat zich vaak op privacy versus veiligheid. Van landen als Duitsland, Zweden en het Verenigd Koninkrijk kan worden geleerd dat het debat ook (meer) zou kunnen focussen op onderwerpen als economie/innovatie en grondrechten. De media-aandacht is hoog.

Conclusie 2. In Nederland is ruime aandacht voor de bescherming van persoonsgegevens in het politieke debat en in de media.

Nederland loopt voorop met de meldplicht datalekken die sinds 2016 van kracht is. In Duitsland bestond zo'n wettelijke plicht al sinds 2009, maar verder bestaat deze verplichting in geen van de andere onderzochte landen. In de gehele EU zal vanaf 2018 echter wel een dergelijke plicht gaan gelden wanneer de AVG van kracht wordt.

Conclusie 3. Nederland loopt (met Duitsland) voorop met de meldplicht datalekken.

In alle onderzochte landen zijn burgerrechtenorganisaties aanwezig die zich specifiek toeleggen op de bescherming van privacy en persoonsgegevens. In Zweden, Roemenië en Nederland hebben deze organisaties echter beperkte budgetten en invloed. In Frankrijk, Duitsland en het Verenigd Koninkrijk beschikken deze spelers over veel meer budget en mankracht en hebben ze tevens een veel grotere invloed, onder meer op het politieke en maatschappelijke debat.
Door de beperkte budgetten en mankracht kan de continuïteit niet altijd worden gegarandeerd. Er is nauwelijks of geen dialoog tussen de Nederlandse burgerrechtenorganisaties en de toezichthouder. Evenmin is er weinig tot geen dialoog met de overheid. Dit ligt deels aan de activistische opstelling van sommige burgerrechtenorganisaties. Wel is de overheid kort geleden een dialoog met dergelijke organisaties gestart en lijkt zij voornemens te zijn deze dialoog voort te zetten en te versterken. De Nederlandse burgerrechtenorganisaties zijn slechts beperkt bekend bij burgers.

Conclusie 4. De budgetten, invloed en bekendheid van burgerrechtenorganisaties in Nederland zijn beperkt.

Beleid

Het gebruik van Privacy Impact Assessments (PIA's) is in Nederland weliswaar niet wettelijk verplicht zoals in Duitsland, maar als gevolg van een aantal moties in de Tweede Kamer heeft de regering dit toch serieus opgepakt en behoort Nederland tot de koplopers. Wel dient opgemerkt te worden dat dit PIA's zijn voor nieuwe wetgeving en nieuwe informatiesystemen, niet voor gegevensbeheerders. Verder is het een probleem dat er een veelheid aan modellen beschikbaar is, waardoor uniformiteit ontbreekt. Andere landen, zoals het Verenigd Koninkrijk en Frankrijk, hebben wel uniforme modellen. Ook is er in Nederland geen begeleiding vanuit de toezichthouder bij het uitvoeren van PIA's, in tegenstelling tot enkele andere landen.

Privacy by Design is een concept dat in toenemende mate wordt genoemd in beleid, maar komt nog niet echt van de grond. Dit is echter in andere landen niet wezenlijk anders. Kennelijk worstelen beleidsmakers nog met de vraag hoe Privacy by Design verwezenlijkt moet worden.

In Nederland is er, net als in veel andere landen, een maatschappelijk debat over privacy en de bescherming van persoonsgegevens.[84] De Nederlandse overheid stelt zich hierin actief op. Bij consultatie ligt in Nederland de nadruk op het consulteren van burgers (via internetconsultaties) en minder op het consulteren van belangengroepen. In sommige landen, zoals Duitsland, Zweden en Ierland, is dit omgekeerd.

De Nederlandse overheid behoort tot de koplopers als het gaat om informatiecampagnes. In Nederland zijn de afgelopen jaren verschillende informatiecampagnes gevoerd, terwijl in andere landen de informatieverstrekking vanuit overheden vaak beperkt blijft tot websites en foldermateriaal. Wel opvallend is dat in Ierland en het Verenigd Koninkrijk ook lesmaterialen voor scholen beschikbaar wordt gesteld, iets dat in Nederland niet of nauwelijks gebeurt.

Conclusie 5. Nederland behoort tot de koplopers wat betreft Privacy Impact Assessments, maatschappelijk debat en informatiecampagnes.

Wet- en regelgeving

Alle lidstaten hebben EU-richtlijn 9/46/EC voor de bescherming van persoonsgegevens geïmplementeerd in nationale wetgeving. Verschillende landen hebben hun wetgeving daarna echter niet meer geactualiseerd In Nederland zijn echter sinds de implementatie in 2001 nog regelmatig wijzigingen doorgevoerd, de belangrijkste in 2012 en 2016. Nederland heeft niet veel meer opgenomen in de nationale wetgeving dan het verplichte minimum in de richtlijn, maar dat geldt voor de meeste lidstaten. In Nederland, net als in andere landen, is sprake van uitgebreide sectorale wetgeving. Verschillen tussen landen zijn wel te bespeuren in de mate van zelfregulering. In Nederland is sprake van een mix van zelfregulering en overheidsregulering, maar het aantal gedragscodes dat jaarlijks aan de toezichthouder wordt voorgelegd, is zeer beperkt (net als bijvoorbeeld in Duitsland). De Nederlandse toezichthouder loopt voorop met het (op de website)

84 Merk op dat het hier gaat om het maatschappelijk debat, onder meer in de media en de politiek, niet om de dialoog tussen de Nederlandse toezichthouder enerzijds en burgerrechtenorganisaties, politiek of degenen op wie toezicht wordt gehouden anderzijds (zie conclusie 12 hieronder).

aanbieden van modelconvenanten,[85] iets dat in andere landen niet lijkt te gebeuren. Alle landen kennen in ruime mate sectorale wetgeving. In het bijzonder met de strafrechtelijke wetgeving en aanvullende besluiten valt op dat Nederland voorop ligt ten opzichte van andere landen, waar dit vaak geregeld is als onderdeel van de politiewet (zoals in Duitsland, Zweden en Roemenië), op een lager niveau (zoals een gedragscode in Ierland) of helemaal niet (zoals in Italië).[86]
Alles bij elkaar zijn de verschillen op het gebied van wet- en regelgeving, als gevolg van de harmoniserende werking van de EU-richtlijn, niet groot tussen de onderzochte landen.

Conclusie 6. Op het gebied van wet en regelgeving zijn de verschillen tussen de onderzochte landen niet groot.

Implementatie
In geen van de onderzochte landen, behalve Duitsland, bestaat er een wettelijke plicht om privacyfunctionarissen aan te stellen.[87] Duitsland loopt daarmee voorop. Wanneer de AVG in mei 2018 van kracht wordt, zullen veel organisaties wel verplicht zijn een privacyfunctionaris aan te stellen, ook in Nederland. Aangezien er in de meeste landen geen verplichting bestaat privacyfunctionarissen aan te stellen en te registreren, zijn er slechts beperkt gegevens beschikbaar over de aantallen privacyfunctionarissen in elk land. In Nederland en enkele andere landen zijn er wel mogelijkheden tot het registreren van privacyfunctionarissen bij de toezichthouder, maar omdat dit op vrijwillige basis is, geven de cijfers mogelijk een vertekend beeld. Op basis van de aanwezige cijfers kan een voorzichtige conclusie worden getrokken dat Nederland, zowel in absolute cijfers als wanneer wordt gecorrigeerd voor het aantal inwoners, weinig privacyfunctionarissen telt. Ter illustratie: Zweden, een land met aanzienlijk minder inwoners dan Nederland, telt ruim tien keer zoveel privacyfunctionarissen dan Nederland.

Conclusie 7. Het aantal privacyfunctionarissen lijkt in Nederland achter te blijven bij andere landen.

In de meeste onderzochte landen bieden de toezichthouders richtlijnen voor de beveiliging van persoonsgegevens aan, ook in Nederland. In Duitsland bestaat er zelfs een aparte overheidsorganisatie voor het beveiligen van informatie. Opvallend is dat in

85 Zie bijvoorbeeld: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/med/med_20040722_modelconvenant_crim_preventie.pdf. Merk op dat deze modelconvenanten niet door de toezichthouder zelf zijn opgesteld, maar door het ministerie van Justitie.

86 Italië kent wel generieke wetgeving voor strafrechtelijke opsporing en voor de bescherming van persoonsgegevens, maar geen specifieke wetgeving voor de verwerking van strafrechtelijke persoonsgegevens. Zie ook Koops, B.J. (2016), *Criminal Investigation and Privacy in Italian Law*. TILT Law & Technology Working Paper Series, version 1.0, December 2016. Available at SSRN: https://ssrn.com/abstract=2888422 or http://dx.doi.org/10.2139/ssrn.2888422.

87 In Nederland bestaat er wel voor politieorganisaties een verplichting een privacyfunctionaris aan te stellen.

bepaalde landen de toezichthouder zelf certificaten, zegels of keurmerken uitreikt wanneer sprake is van een adequate beveiliging. Dit is het geval in Duitsland en Frankrijk. In het Verenigd Koninkrijk is dit in voorbereiding. Nederland (evenals Zweden, Ierland, Roemenië en Italië) kent een dergelijke praktijk niet. Voor Nederlandse organisaties is het daardoor lastiger om vast te stellen of hun beveiliging adequaat is of niet.

Conclusie 8. Voor de beveiliging van persoonsgegevens zijn er wel richtlijnen in Nederland, maar de toezichthouder biedt geen certificering of keurmerk zoals in andere landen.

Transparantie met betrekking tot welke persoonsgegevens worden verzameld en voor welke doeleinden deze persoonsgegevens worden verwerkt is laag. Zulke informatie is doorgaans terug te vinden in de privacyvoorwaarden en/of algemene voorwaarden, maar veruit de meeste mensen lezen deze teksten niet. Als ze al worden gelezen, zijn deze teksten vaak lastig te doorgronden vanwege het (soms cryptische) juridische en technische taalgebruik. Bovendien kost het (heel) veel tijd. Er zijn geen grote verschillen te duiden in transparantie in de onderzochte landen. De Nederlandse overheid geeft wel een goed voorbeeld middels de website www.mijnoverheid.nl die tracht de transparantie te verbeteren ten aanzien van persoonsgegevens van burgers die worden verwerkt. Een dergelijk initiatief zijn we in geen van de andere onderzochte landen tegengekomen.

Conclusie 9. Transparantie is in alle onderzochte landen laag.

Toezicht en handhaving

In alle onderzochte landen hebben de respectievelijke toezichthouders vergelijkbare taken, geclusterd rondom onderwerpen als toezicht houden, adviseren en informatie verstrekken. Wanneer de budgetten en de aantallen medewerkers van de toezichthouders worden vergeleken, dan blijkt Nederland een gemiddelde plaats in te nemen. Toezichthouders in landen als Frankrijk, Italië en het Verenigd Koninkrijk zijn aanzienlijk groter, maar die moeten ook toezicht houden in landen met een groter bruto nationaal product en een groter aantal inwoners. Wanneer wordt gecompenseerd hiervoor, blijkt Nederland nog steeds een gemiddelde plek in te nemen. Geen enkel land komt in de buurt van de omvang van het Duitse toezicht, waar naast een federale toezichthouder ook in elke bondsstaat een toezichthouder is opgericht. Merk op dat de toezichthouders met het van kracht worden van de AVG waarschijnlijk meer budget en mankracht nodig zullen hebben.[88]

Conclusie 10. Het budget en het aantal medewerkers van de Nederlandse toezichthouder loopt in de pas met andere landen.

88 Andersson Elffers Felix (2017), *Organisatorische vertaling Verordening & Richtlijn gegevensbescherming*. Utrecht: Andersson Elffers Felix. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/eindrapportage_aef.pdf.

Met de verhoging van de maximale boetes voor schendingen van de wet- en regelgeving voor de bescherming van persoonsgegevens in 2016 loopt Nederland weer in de pas met andere Europese landen. Nederland is met de invoering van boetes die afhankelijk zijn van de omzet van bedrijven koploper (samen met Roemenië). Deze vorm van boetes loopt vooruit op de boetes die mogelijk worden vanaf 2018 wanneer de AVG van kracht wordt. Een strafrechtelijke aanpak is in de meeste landen mogelijk, waarbij maximale gevangenisstraffen van 2 tot 5 jaar kunnen worden opgelegd. Nederland zet niettemin vooral in op een bestuursrechtelijke aanpak. Bij de strafrechtelijke aanpak in andere landen moet wel worden aangetekend dat deze alleen mogelijk is in gevallen van de zwaarste schendingen van de wetgeving voor de bescherming van persoonsgegevens en zelden tot nooit wordt ingezet.

Conclusie 11. Boetebevoegdheden van de Nederlandse toezichthouder lopen Europees gezien in de pas.

De toezichthouders in alle onderzochte landen houden zich bezig met een vergelijkbaar palet aan activiteiten. De activiteiten zijn geclusterd rondom onderwerpen als toezicht houden, adviseren en informatie verstrekken. Vanwege de beperkte beschikbaarheid van gegevens kunnen de activiteiten van de toezichthouders in de verschillende landen niet goed met elkaar worden vergeleken als het gaat om het aantal vragen, meldingen en klachten die ze ontvangen c.q. behandelen. Ook over de in totaal geïnde boetegelden zijn te weinig data beschikbaar om een vergelijking te kunnen maken. De aantallen onderzoeken die de toezichthouders uitvoeren, zijn ook lastig vergelijkbaar omdat deze onderzoeken erg variëren in omvang. Wel kan gesteld worden dat de Nederlandse toezichthouder (net als onder meer in Duitsland) de afgelopen jaren neigt naar striktere handhaving en het voeren van meer rechtszaken.
Verder valt op dat de Nederlandse toezichthouder weinig tot geen dialoog voert met de organisaties waarop toezicht wordt gehouden. Wel voert de Autoriteit Persoonsgegevens dialogen met brancheorganisaties in de publieke en private sector. De toezichthouder organiseert zelf geen workshops, symposia of opleidingen maar spreekt wel in toenemende mate op congressen en symposia. Verder lijkt de Autoriteit Persoonsgegevens terughoudend te zijn in het afhandelen van vragen van burgers en organisaties over hoe wet- en regelgeving moet worden nageleefd of hoe 'privacy-proof' te zijn. Dit lijkt een bewust gekozen strategie van de toezichthouder om te voorkomen dat toezicht moet worden gehouden op beleid en maatregelen waarover eerder is geadviseerd. Op basis van resultaten uit dit onderzoek kan worden vastgesteld dat Nederland hierin verschilt van andere landen, maar niet kan worden vastgesteld wat het meest effectief is. Mogelijk liggen hier kansen voor een uitbreiding of andere invulling van de rol van de Nederlandse toezichthouder.
Bovendien lijkt de AP het indienen van klachten niet echt aan te moedigen: in geval van een klacht over het gebruik van persoonsgegevens is het officiële advies om, afgezien van het indienen van een tip via het tipformulier, eerst contact op te nemen met de gegevensbeheerder en, als dat niet het gewenste resultaat oplevert, naar de rechter te

stappen.[89] Alles bij elkaar is er weinig tot geen begeleiding van en overleg met degenen op wie toezicht wordt gehouden (op individueel niveau, er is wel overleg met brancheorganisaties) en kan gesteld worden dat het ondersteunen van burgers beperkt is. Dit staat los van het maatschappelijk debat over de bescherming van privacy en persoonsgegevens, onder meer in de media en de politiek (zie conclusie 5).

Conclusie 12. De Autoriteit Persoonsgegevens onderhoudt op individueel niveau nauwelijks een dialoog met degenen op wie toezicht wordt gehouden en doet nauwelijks aan klachtbehandeling.

De reputatie van de Nederlandse toezichthouder is lastig vast te stellen, net als in andere landen overigens. De Autoriteit Persoonsgegevens lijkt niet te worden gevreesd, al kan dat in de toekomst veranderen wanneer de boetes hoger worden en de handhaving strikter. De Nederlandse toezichthouder is goed bekend onder burgers: ongeveer de helft van de mensen heeft ooit gehoord van de toezichthouder. Daarmee behoort Nederland (samen met Zweden) op dit punt tot de best scorende landen.

Conclusie 13. De Nederlandse toezichthouder is goed bekend bij burgers.

Wel voert de Autoriteit Persoonsgegevens dialogen met brancheorganisaties in de publieke en private sector. De toezichthouder organiseert zelf geen workshops, symposia of opleidingen maar spreekt wel in toenemende mate op congressen en symposia.

Wanneer deze conclusies bij elkaar worden opgeteld, kan gesteld worden dat Nederland het goed doet als het gaat om de bescherming van persoonsgegevens. Binnen de groep met landen die in dit onderzoek zijn vergeleken, kan gesteld worden dat Duitsland in de meeste opzichten koploper[90] is en dat met name Italië en Roemenië zich aan het andere uiteinde van het spectrum bevinden. Nederland doet het in de meeste opzichten bovengemiddeld goed. Zo is het goed gesteld met het bewustzijn en de zelfredzaamheid van Nederlanders, is er ruime aandacht voor de bescherming van persoonsgegevens in het politieke debat en de media, loopt Nederland voorop met de meldplicht datalekken, Privacy Impact Assessments, maatschappelijk debat en informatiecampagnes, lopen budgetten, aantallen medewerkers en boetebevoegdheden van toezichthouders goed in de pas en is de Nederlandse toezichthouder goed bekend bij burgers.
Ruimte voor verbetering in Nederland is mogelijk als het gaat om de budgetten, invloed en bekendheid van burgerrechtenorganisaties, het aantal privacyfunctionarissen in organisaties, certificering/keurmerken voor de beveiliging van persoonsgegevens,

89 https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/klacht-over-gebruik-persoonsgegevens?qa=klacht.

90 Merk op dat in dit onderzoek de nadruk ligt of de federale overheid in Duitsland, maar dat de Bundesländer bovendien allemaal hun eigen wetgeving en toezichthouders hebben. Zonder dat de deelstaten in de vergelijking worden meegenomen komt Duitsland al op veel aspecten goed uit de bus. Als de deelstaten zouden worden meegenomen in de vergelijking (hetgeen door beperkt beschikbare gegevens niet mogelijk was), zou Duitsland nog veel beter afsteken bij de andere landen in de vergelijking.

transparantie, klachtenafhandeling, dialoog tussen enerzijds toezichthouder en anderzijds degenen onder toezicht en burgerrechtenorganisaties. Daarbij dient echter te worden aangetekend dat transparantie in alle onderzochte landen laag is, dat de aankomende Algemene Verordening Gegevensbescherming een aantal zaken zal verstevigen en dat door de Nederlandse overheden op allerlei andere onderwerpen reeds (verdere) verbeteringen in gang zijn gezet. Dit laatste bevestigt het proactieve optreden van Nederlandse overheden op het terrein van privacy en de bescherming van persoonsgegevens. Door deze opstelling is Nederland goed voorbereid op de Algemene Verordening Gegevensbescherming en is het aannemelijk dat Nederland ook in de toekomst (met name technologische) ontwikkelingen die gevolgen kunnen hebben voor de bescherming van persoonsgegevens goed zal weten te adresseren.

Summary

The Protection of Personal Data
Comparison of Eight European Countries

Background and research questions

The protection of personal data in the European Union largely depends on existing legislation. The EU Data Protection Directive (Directive 95/46/EC), valid until May 25th 2018 and the General Data Protection Regulation (GDPR, Regulation 2016/679), in force after May 25th 2018, determine the legal framework for rights and obligations of persons whose data are collected and processed and for companies and governments that collect and process these personal data. The actual protection, however, does not only depend on the legal framework, but also on the further elaboration on and interpretation of the legislation and the ways in which it is enforced. The legislation on privacy and the protection of personal data contains many open norms. As a result of differences in legal systems and cultural differences, the legal implementation of the Data Protection Directive is different in EU member states. As a result of the open norms, in combination with cultural differences, the practical implementation of the protection of personal data is also different in EU member states. Although the GDPR will further harmonize this, it may be expected that differences in practices will continue to exist.

The differences in the extent to which personal data are protected raise the question of which country best protects personal data (which is an important aspect of privacy). This research focuses on the position of the Netherlands in relation to other European countries and the question whether the Netherlands is a frontrunner or lagging behind. An answer to this question enables further measures for the protection of privacy and personal data in the event that the protection in the Netherlands provides less protection in comparison to other EU member states. This leads to the central research question of this study:

What is the position of the Netherlands with regard to the protection of personal data of citizens in comparison with several other countries in the European Union?

In order to answer this question, six subquestions were formulated:

1. What is the general situation regarding personal data protection?
2. What are the national government's policies regarding personal data protection?
3. What are the national laws and regulations regarding personal data protection?
4. How are legislation and policies implemented in practice?
5. How are supervisory authorities organized and how is enforcement carried out?

6. When comparing the eight countries investigated on the abovementioned aspects, what is the position of the Netherlands?

The focus of this research is on the protection of personal data (informational privacy) and not on the protection of privacy in a broad sense. Although a considerable number of the research questions has a legal nature, this is not typical legal or legally positivistic research. Rather, the focus is on the question of how the protection of personal data for residents is implemented in practice and experienced by residents. Previous research has shown that the way people experience privacy does not always match the goals of legislation. This research does not provide a normative judgement on where the Netherlands should be positioned in comparison with other European countries, but does provide suggestions for how the Netherlands could move in a specific direction regarding particular aspects of its data protection framework.

Methodology

An international comparison requires decisions to be made on which aspects (of the protection of personal data) to compare and on which countries to compare.

Aspects to compare

Based on previous research, five aspects were chosen as points of comparison in this research. These aspects, reflected in the first five subquestions mentioned above are: (1) general situation, (2) national government policies, (3) laws and regulations, (4) implementation, and (5) regulatory authorities and enforcement. For each country investigated in this research, information was collected on these aspects by means of desk research, an extensive questionnaire and expert consultations. During the desk research stage, available literature and online data (for instance, websites and annual reports of data protection authorities, governments and civil rights organizations) were collected. In this research no survey was conducted among EU citizens, but secondary analyses and/or reuse of existing surveys (including the CONSENT Survey, the Eurobarometer and the Oxford Internet Survey) were used to collect further information, which was combined this with the expert consultations. Information that was not available via desk research was requested through an extensive questionnaire sent to experts in the respective countries. Furthermore, employees at the data protection authorities in the different countries were contacted for further information. These experts and data protection authorities did not receive the entire questionnaire, but only those questions that yielded limited results during the desk research. For aspects on which limited or no information was available after desk research and expert consultations, the results were supplemented with additional desk research, media analyses and interviews. For additional interviews, experts on personal data protection, policy makers, companies processing personal data, data protection authorities and civil rights organizations were contacted.

Finally, the collected material was clustered in 23 categories (labels). For the general situation, these are internet use, control, awareness, trust, protection actions, national politics, media attention, data breaches, and civil rights organizations. For national government policies, these are national policies and Privacy Impact Assessments, privacy

and data protection in new policies, societal debate, and information campaigns. For laws and regulations, these are implementation of the EU directive, sectoral legislation, self-regulation and codes of conduct. For implementation, these are privacy officers, security measures and transparency. For regulatory authorities and enforcement, these are supervisory authorities, main activities, the use of competences and reputation.

Countries to compare

This research focuses on the position of the Netherlands. Furthermore, the following countries were analyzed in this comparison: Germany, Sweden, the United Kingdom, Ireland, France, Romania and Italy. The countries were selected to ensure a distribution on several selection criteria. These are strict/lenient approaches towards privacy protection, approaches to personal data protection similar/dissimilar to the Netherlands (due to cultural dimensions, the legal system, and the monistic/dualistic approach to international law), maturity of privacy protection (history, particularly accession to the EU), and geographical distribution (North-South and East-West). In total, the five aspects of personal data protection were mapped for eight European countries. After that, the countries were compared on each aspect and the position of the Netherlands was determined in comparison to the other countries.

Results and conclusions

When comparing the position of the Netherlands with the other countries analyzed, this yields the following conclusions:

- The Dutch people show high levels of awareness and self-reliance with regard to the protection of their personal data. At the same time, there are low levels of concern and high levels of acceptance and resignation.
- In the Netherlands, there is extensive attention for the protection of personal data in the political debate and in the media.
- The Netherlands (together with Germany) is frontrunner with regard to data beach notification laws.
- The budgets, influence and notoriety of civil rights organizations in the Netherlands are limited.
- The Netherlands is among the frontrunners with regard to privacy impact assessments, societal debate, and information campaigns.
- Differences in national legislation are very small in the countries investigated.
- The number of privacy officers in the Netherlands lags behind the other countries compared.
- Guidelines for security measures exist in the Netherlands, but authorities do not offer certification or quality marks like in some other countries.
- Transparency is low in all countries investigated.
- The budget and number of employees of the Dutch Data Protection Authority are in line with other countries.
- Sanction options of the Dutch Data Protection Authority are in line with other countries.

- The Dutch Data Protection Authority maintains a very limited dialogue (at an individual level) with those under supervision and does not process citizen complaints.
- The Dutch Data Protection Authority is well-known among citizens.

Combining these conclusions, it can be argued that personal data are well-protected in the Netherlands. With the group of countries compared in this research, Germany is frontrunner in most aspects and Italy and Romania are at the other end of the spectrum. The Netherlands perform above average in most aspects. For instance, there are high levels of awareness and self-reliance of citizens; there is extensive attention for personal data protection in the political debate and the media; the Netherlands is a frontrunner regarding data breach notification laws, privacy impact assessments, societal debate, and information campaigns; the budgets, numbers of employees and sanction options of supervisory authorities are adequate; and the Dutch Data Protection Authority is well-known among citizens.
Further improvement is possible in the Netherlands with regard to the budgets, influence and notoriety of civil rights organizations, the number of privacy officers in organization, certification and quality marks for the security of personal data, transparency, processing citizen complaints, and dialogue between supervisory authorities on the one hand and those under supervision and civil rights organizations on the other hand. However, it has to be mentioned that transparency is low in all countries investigated, that the GDPR will (further) improve a number of these issues and that the Dutch government has already initiated (further) improvements on a number of topics. This confirms the proactive approach of the Dutch government regarding the protection of privacy and personal data. Because of his attitude, the Netherlands is well-prepared for the GDPR and likely to be able address future (specifically technological) developments that may affect the protection of personal data.

Literatuur

Andersson Elffers Felix (2017), *Organisatorische vertaling Verordening & Richtlijn gegevensbescherming*, Utrecht: Andersson Elffers Felix. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/eindrapportage_aef.pdf.

Andersson Elffers Felix (2013), *Media-analyse identiteitsmanagement*, Utrecht: AEF. http://www.aef.nl/aef-onderzoekt-identiteitsmanagement-in-europa.

AP (2016), *Jaarverslag 2015*, Den Haag: AP.

AP (2017), *Jaarverslag 2016*, Den Haag: AP. https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_jaarverslag_2016.pdf.

Bamberger, K.A. and Mulligan, D.K. (2015), 'Empirical Findings – United Kingdom, In *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. The MIT Press.

Bapat, A. and Smith, A. (2017), 'United Kingdom Data Protection 2017'. *International Comparative Legal Guides*. https://iclg.com/practice-areas/data-protection/data-protection-2017/united-kingdom#chaptercontent12.

Barry, A. (2013), 'reland should consider laws that would jail cyber bullies'. TheJournal.ie. https://www.thejournal.ie/cyber-bullying-ireland-1162881-Nov2013/.

Bauman, T. (2014), 'Ireland: The Country that Sets Big Tech's Internet Privacy Policies'. *The Sovereign Investor Daily*. http://thesovereigninvestor.com/asset-protection/ireland-sets-big-tech-internet-privacy-policies/.

Bennefeld, C. (2016), 'So ungeschützt sind deutsche Surfer im Netz', Handelsblatt.com, http://www.handelsblatt.com/technik/sicherheit-im-netz/datenschutz-in-deutschland-so-ungeschuetzt-sind-deutsche-surfer-im-netz/14592766.html.

Biermann, K. and Jacobsen, L. (2013). 'Eine Datenschutzbeauftragte, die Daten nicht schützen will', Zeit Online, http://www.zeit.de/digital/datenschutz/2013-12/datenschutz-beauftragte-vosshoff-bundestag-gewaehlt.

Big Brother Watch (2012), Protecting Civil Liberties: The 2015 Big Brother Watch Manifesto. *Big Brother Watch*.

Big Brother Watch (2012), The Price of Privacy: How local authorities spent £515m on CCTV in four years. *Big Brother Watch*.

Blick, A. (2012), Mapping the Path to Codifying – or not Codifying – the UK's Constitution. The Existing Constitution, Series paper 2. Centre for Political and Constitutional Studies, King's College London.

Boddewyn, J.J. (1985), 'The Swedish Consumer Ombudsman System and Advertising Self-Regulation', *The Journal of Consumer Affairs*, Vol. 19, No. 1, p. 140-162.

Bohan, A. and Carney, A. (2017), Ireland Data Protection 2017. *International Comparative Legal Guides*. https://iclg.com/practice-areas/data-protection/data-protection-2017/ireland#chaptercontent1.

Bongers, F., Jager, C.J., & Velde, R. te (2015), *Big data in onderwijs en wetenschap*. Utrecht: Dialogic.

Borking, J.J.F.M. (2010), *Privacyrecht is code: Over het gebruik van privacy enhancingtechnologies* (proefschrift, Universiteit Leiden). Deventer: Kluwer.

Braunmühl P. von (2015), *Regulierte Selbstregulierung im Datenschutz*, https://berliner-datenschutzrunde.de/node/145.

Brockdorff, N. (2012), *Quantitative Measurement of End-User Attitudes Towards Privacy*. Work Package 7 of Consent. http://www.consent.law.muni.cz/.

Cabinet Office (2008), Cross Government Actions: Mandatory Minimum Measures. http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf.

Cannataci, J. (2016), Report of the Special Rapporteur on the right to privacy, 8 March 2016.

Cavoukian, A. (2009), Privacy by Design: The 7 Foundational Principles, Information and Privacy Commissioner of Ontario, Toronto, Ontario, August 2009.

CBP (2008), Informatiebeveiliging in ziekenhuizen voldoet niet aan de norm. Den Haag: CBP.

CBP (2010), Onderzoek van het College bescherming persoonsgegevens (CBP) naar bestandskoppelingen door de SIOD voor de ontwikkeling van risicoprofielen, z2009-00672, mei 2010, Den Haag: CBP.

CBP (2013), Beveiliging van persoonsgegevens. Den Haag: CBP.

CENSIS (2012), *Il valoredellaprivacynell'epocadellapersonalizzazione dei media*.

CentERdata (2016), Tilburg University, *Study on consumers' attitudes towards Terms and Conditions*, final report. Publications Office of the EU, Luxembourg 2016, doi:10.2818/950733.

Chopin, I. and Germaine-Sahl, C. (2013), Developing Anti-discrimination Law in Europe. European Commission, Directorate General for Justice. October 2013.

Commission of the European Communities (EC) (2009), *Commission recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identificatio*n, Brussels, 2009.

Competition & Markets Authority (2015), The commercial use of consumer data: Report on the CMA's call for information. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf.

Council of Europe (2001), The implications for Council of Europe Member States of the Ratification of the Rome Statute of the International Criminal Court, Progress Report, Sweden, consult/icc 37.

Cullen, P. (2009), 'Bord Gáis Failed to Say Stolen Laptop Data Not Encrypted', *The Irish Times*. http://www.irishtimes.com/news/bord-g%C3%A1is-failed-to-say-stolen-laptop-data-not-encrypted-1.787045.

CONSENT (2012), Consumer sentiment regarding privacy on user generated content (UGC) services in the digital economy. https://www.consent.law.muni.cz/.

Cuijpers, C.M.K.C. (2006), Verschillen tussen de Wbp en richtlijn 95/46/EG en de invloed op de administratieve lasten- en regeldruk, 22 juni 2006. See www.actal.nl.

Custers, B.H.M. (2016), 'Etnisch profileren is wettelijk verboden en dat moet zo blijven', *Trouw*, 7 juni 2016, p. 17.

Custers, B.H.M., Oerlemans, J.J., Vergouw, S.J. (2015), *Het gebruik van drones. Een verkennend onderzoek naar onbemande luchtvaartuigen*. Meppel: Boom Lemma Uitgevers.

Custers B.H.M., J.J. Oerlemans & Pool R.L.D. (2016), 'Ransomware, cryptoware en het witwassen van losgeld in Bitcoins', *Strafblad* 14(2): 87-95

Custers, B., Van der Hof, S., Schermer, B., Appleby-Arnold, S., Brockdorff, N. (2013), 'Informed Consent in Social Media Use. The Gap between User Expectations and EU

Personal Data Protection Law', *SCRIPTed, Journal of Law, Technology and Society*, Volume 10, Issue 4, p. 435-457.

Custers, B., Van der Hof, S., Schermer, B. (2014), 'Privacy Expectations of Social Media Users. The Role of Informed Consent in Privacy Policies', *Policy & Internet*, Vol. 6, No. 3, p. 268-295.

Custers B.H.M. & Zwenne G.J. (2009), 'Aandachtspunten voor het College Bescherming Persoonsgegevens', *Openbaar Bestuur* 19(8): 14-17.

Data Protection Commissioner (2013), Global Privacy Enforcement Network Internet 'Privacy Sweep'. https://www.dataprotection.ie/documents/GPEN2013.pdf.

Data Protection Commissioner (2016), Data Protection Commissioner welcomes Budget 2017 increase in funding. https://www.dataprotection.ie/docs/13-10-2016-Data-Protection-Commissioner-welcomes-Budget-2017-increase-in-funding/1601.htm.

Data Protection Commissioner (2016), Annual Report of the Data Protection Commissioner of Ireland. https://www.dataprotection.ie/docimages/documents/DP-C%20AR2015_FINAL-WEB.pdf.

Data Protection Commissioner (undated), The GDPR and You: Preparing for 2018. https://www.dataprotection.ie/docimages/documents/The%20GD-PR%20and%20You.pdf.

DDMA (2016), Hoe Nederlanders denken over data en privacy, Amsterdam: DDMA.

Deegan, G. (2016), 'Cyber attack victim firm Loyaltybuild in Clare has €18m loss', *Irish Examiner*. http://www.irishexaminer.com/business/cyber-attack-victim-firm-loyalty-build-in-clare-has-18m-loss-379472.html.

DellEMC (2014), EMC Privacy Index, https://www.emc.com/campaign/privacy-index/index.htm.

Department for Business, Innovation and Skills (2014), Personal Data: Review of the midata voluntary programme. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/327845/bis-14-941-review-of-the-midata-voluntary-programme-revision-1.pdf.

Department of the Taoiseach (2016), Minister Dara Murphy highlights Ireland's preparations for new EU-wide data protection rules in keynote address. http://www.taoiseach.gov.ie/eng/Taoiseach_and_Government/About_the_Ministers_of_State/Minister/MoS_Murphy_s_Press_Releases/Dara.html.

Digital Rights Ireland Limited (2016), Income and Expenditure Account for the year ended 31 December 2015.

Dörr, D. and Aernecke, E. (2012). A never ending story: Caroline v Germany. In D. Dörr and R.L. Weaver (Eds.), *The right to privacy in the light of media convergence*. Berlin: De Gruyter.

Dubbeld, L. (2007), Functionarissen voor de gegevensbescherming: onzichtbare privacybeschermers, *Privacy & Informatie,* 2007, aflevering 2, p. 69-70.

Dutton, W.H., and Blank, G. (2013), Cultures of the Internet. The Internet in Britain. Oxford Internet Survey 2013. http://oxis.oii.ox.ac.uk/reports.

Eddy, M. (2016), 'Reports of Attacks on Women in Germany Heighten Tension Over Migrants'. *The New York Times*. 5th January 2016.

Edwards, E. (2014), 'Loyaltybuild Reopens for Business after Huge Data Breach', *The Irish Times*. http://www.irishtimes.com/news/consumer/loyaltybuild-reopens-for-business-after-huge-data-breach-1.1722266.

Edwards, E. (2016), 'Civil Service Payroll System to Be Audited Following Data Breach', *The Irish Times*. http://www.irishtimes.com/news/ireland/irish-news/civil-service-payroll-system-to-be-audited-following-data-breach-1.2691360.

Edwards, E. (2016), 'Data Protection Commissioner Helen Dixon accuses lawyers of "digital ambulance chasing"', *The Irish Times*. http://www.irishtimes.com/business/technology/data-protection-commissioner-helen-dixon-accuses-lawyers-of-digital-ambulance-chasing-1.2712459.

Edwards, E. (2016), 'Independence of Data Protection Commissioner questioned', *The Irish Times*. https://www.irishtimes.com/business/technology/independence-of-data-protection-commissioner-questioned-1.2513682.

Essen, J. van (2014), CBP een waakhond zonder tanden? Mr-online, 1 december 2014. http://www.mr-online.nl/opinie/432-wetgeving/25169-cbp-een-waakhond-zonder-tanden.

European Commission (2010), Data protection: Commission requests UK to strengthen powers of national data protection authority, as required by EU law. http://europa.eu/rapid/press-release_IP-10-811_en.htm?locale=en.

European Commission – Seventh Framework Programme (2012), *Consumer sentiment regarding privacy on user generated content (UGC) services in the digital economy – Italy Report*.

European Commission – Seventh Framework Programme (2012). *Consumer sentiment regarding privacy on user generated content (UGC) services in the digital economy – Germany Report*.

European Union (2015), Special Eurobarometer 431 'Data protection'.

European Union Agency for Fundamental Rights (2010), Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II).
http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf.

Expertgroep EZ (2016), Licht op de digitale schaduw; verantwoord innoveren met big data, Den Haag: ministerie van Economische Zaken.

Fitzsimons, L. and Sherry, S. (2017), *Brexit: the impact on General Data Protection Regulation.* Eversheds Sutherland.
http://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/Data-Protection/brexit_impact_on_gdpr_170616.

Garante per la Protezione dei Dati Personali (2014), *Relazioneannuale 2014.*

Garante per la Protezione dei Dati Personali (2015), *Relazioneannuale 2015*.

Groot, H. de (1625), *De iure belli acpacis*. Pariisis: Apud Nicalaum Buon.

Hawkes, B. (2016), The Irish DPA and Its Approach to Data Protection. In D. Wright and P. De Hert (Eds.), *Enforcing Privacy* Cham: Springer International Publishing.

Hermida, J. (2004), *Legal basis for national space legislation* Dordrecht: Kluwer.

HM Government (2013), Information Economy Strategy https://www.gov.uk/government/publications/information-economy-strategy.

HM Government (2016), Cyber Security Regulation and Incentives Review, December 2016. Department for Culture Media & Sport. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579442/Cyber_Security_Regulation_and_Incentives_Review.pdf.

Hoffmeister, F. (2002), International agreements in the legal order of the candidate countries. In: A. Ott and K. Inglis (Eds), *Handbook on European Enlargement*. The Hague: Asser Press, p. 209.

Holvast, J. (2005), 'Interview met Jacob Kohnstamm', *Privacy & Informatie*, 2005-3, p. 114-119.

Hooghiemstra, T.F.M. (2002), Privacy bij ICT in de zorg. Bescherming van persoonsgegevens in de informatie-infrastructuur voor de gezondheidszorg. Den Haag: Cbp, A&V 2002 nr. 26.

Hooghiemstra, T., Oud, J.,Radema, M., Spruit, M., en Wielaard, P. (2016), Onderzoek naar de beveiliging van patiëntgegevens, Den Haag: PBLQ. Zie: https://www.rijksoverheid.nl/documenten/rapporten/2016/12/01/onderzoek-naar-de-beveiliging-van-patientgegevens.

Hornung, G. (2012), A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012 (2012), 9 *SCRIPTed*64-81.

House of Commons, Science and Technology Committee (2014), Responsible Use of Data, Fourth Report of Session 2014-15. https://www.publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf.

House of Commons, Science and Technology Committee (2016), The big data dilemma: Government Response to the Committee's Fourth Report of Session 2015-16, Fifth Special Report of Session 2015-16. https://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/992/992.pdf.

Hulshof, M. en Veen, M. van der (2017), '21 ideeën voor een beter internet', *Volkskrant*, 17 juni 2017. http://www.volkskrant.nl/media/21-ideeen-voor-een-beter-internet~a4501135/

Information Commissioner's Office (undated), The Information Commissioner's response to the European Commission's consultation on the legal framework for the fundamental right to protection of personal data. http://ec.europa.eu/justice/news/consulting_public/0003/contributions/public_authorities/ico_uk_en.pdf.

Information Commissioner's Office (2013), Data Protection Regulatory Action Policy.

Information Commissioner's Office (2014), Conducting privacy impact assessments: code of practice. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

Information Commissioner's Office (2015), Data protection rights. What the public want and what the public want from Data Protection Authorities. https://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf.

Information Commissioner's Office (2016), Information Commissioner's Annual Report and Financial Statements 2015/16. https://ico.org.uk/media/about-the-ico/documents/1624517/annual-report-2015-16.pdf.

Information Commissioner's Office (2016), Consultation on ICO's Privacy notices code of practice: summary of responses. https://ico.org.uk/media/about-the-ico/consultations/1625139/ico-privacy-notices-code-of-practice-consultation-summary-20161006.pdf.

Inspectie SZW (2015), Suwinet 2015. Vervolgonderzoek 'veilig omgaan met elkaars gegevens', Den Haag: Inspectie SZW. https://www.inspectieszw.nl/...veilig-omgaan-met-elkaars-gegevens/Suwinet-2015.pdf.

IPSOS (2014), Nederlander minder onverschillig over privacy, 11 maart 2014. http://site.ipsos-nederland.nl/politiekebarometer/Berichten/PersBericht_1264_Nederlander_minder_onverschillig_over_privacy.html.

Ipsos MORI (2012), Stakeholder Perceptions 2012, Prepared for the ICO. https://ico.org.uk/media/about-the-ico/documents/1042371/stakeholder-perceptions-2012.pdf.

Irish Independent Staff (2015), 'Data Office Still Underfunded despite €1m Boost in Budget'. *Independent.ie*. http://www.independent.ie/business/technology/news/data-office-still-underfunded-despite-1m-boost-in-budget-34126722.html.

Italian Chamber of Deputies (2012), Reasoned Opinion on Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Janssen, H.L. (2003), *Constitutioneleinterpretatie.* Dissertatie UM, Den Haag: SDU 2003.

Jigsaw Research (2008), Information Commissioner's Office Stakeholder Perceptions Study. https://ico.org.uk/media/1042339/ico-stakeholder-perception-study-research-report.pdf.

Kelleher, D. (2015), *Privacy and Data Protection Law in Ireland*. Haywards Heath: Bloomsbury Professional (2nd ed.).

Kennedy, E. (2008), 'Victims of BoI Laptop Theft Treble to 31,500'. *Independent.ie*. http://www.independent.ie/irish-news/victims-of-boi-laptop-theft-treble-to-31500-26442003.html.

Kerkmann, C. (2015), 'Transatlantische Daten-Blockade', Handelsblatt.com, http://www.handelsblatt.com/my/technik/it-internet/attacke-auf-google-und-co-transatlantische-daten-blockade/12506476.html

Keulen, E. van (2016), Zorgen om privacy (infographic), 10 juni 2016. http://www.emerce.nl/research/zorgen-om-privacy.

Kommers, D.P. (2012), *The Constitutional Jurisprudence of the Federal Republic of Germany*. Durham NC, Duke University Press.

Koning, B. de (2016), 'Welke partij heeft zijn beloftes over privacy het meest waargemaakt?', *De Correspondent*, 6 februari 2016.

Kool, L., Timmer, J., Royakkers, L. en Van Est, R. (2017), *Opwaarderen. Borgen van publieke waarden in de digitale samenleving*. Den Haag: Rathenau Instituut. Zie https://www.rathenau.nl/nl/file/2797/Opwaarderen_Rathenau_Instituut.pdf.

Koops, B.J., Roosendaal, A., Kosta, E., Lieshout, M. van, en Oldhoff, E. (2016), Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX, Delft: TNO. See https://www.rijksoverheid.nl/documenten/rapporten/2016/02/12/privacy-impact-assessment-wet-op-de-inlichtingen-en-veiligheidsdiensten-20xx.

Kuner, C. (2012), 'The European Commission's Proposed Data Protection Regulation. A Copernican Revolution in European Data Protection Law', *Bloomberg BNA Privacy and Security Law Report*, 1-15.

Labour (2016), Standing Up for Ireland's Future: Labour Manifesto 2016. https://www.labour.ie/download/pdf/labour_manifesto_2016.pdf.

Lewis, P. (2011), 'You're being watched: there's one CCTV camera for every 32 people in UK'. *The Guardian*. https://www.theguardian.com/uk/2011/mar/02/cctv-cameras-watching-surveillance.

Lieshout, M. van, Kool, L., Bodea, G., Schlechter, J., & Schoonhoven, B. van (2012), Stimulerende en remmende factoren van Privacy by Design in Nederland, Delft: TNO.

Lillington, K. (2015), 'Strong data protection laws better for EU than sniping', *The Irish Times*. https://www.irishtimes.com/business/technology/strong-data-protection-laws-better-for-eu-than-sniping-1.2185370.

Logue, F. (2016), 'Data protection chief must not distance herself from complainants', *The Irish Times*. http://www.irishtimes.com/business/technology/data-protection-chief-must-not-distance-herself-from-complainants-1.2750669.

Malsch, M., Dijkman, N. & Akkermans, A. (2015), *Het zichtbare slachtoffer. Privacy van slachtoffers binnen het strafproces*. (WODC/NSCR/VU) Boom Uitgeverij.

Manolea, B. (2007), Institutional framework for personal data protection in Romania, p. 1. https://www.apti.ro/DataProtection_ro.pdf.

Martijn, M., en Tokmetzis, D. (2016), *Je hebt wel iets te verbergen*. Amsterdam: De Correspondent BV.

McConnell, D. (2015), 'Labour brings two separate bills targeting online bullying'. *Independent.ie*. http://www.independent.ie/irish-news/politics/labour-brings-two-separate-bills-targeting-online-bullying-31149776.html.

McGeveran, W. (2016), 'Friending the Privacy Regulators', *Arizona Law Review*, 58, 959-1025. https://papers.ssrn.com/abstract=2820683.

McIntyre, T.J. (2014), 'The State Must Be More Mindful of Your Private Data', *Independent.ie*. http://www.independent.ie/opinion/the-state-must-be-more-mindful-of-your-private-data-30524449.html

McIntyre, T.J. (2014), 'Why Ireland Must Protect Privacy of Irish Emails and Internet Usage from Surveillance', *The Irish Times*. http://www.irishtimes.com/opinion/why-ireland-must-protect-privacy-of-irish-emails-and-internet-usage-from-surveillance-1.2044384.

McIntyre, T.J. (2015), 'Europe Has Failed in Duty to Protect Citizens over Web Privacy Threat'. *Independent.ie*. http://www.independent.ie/opinion/comment/europe-has-failed-in-duty-to-protect-citizens-over-web-privacy-threat-31589481.html.

MerrionStreet.ie (2015), 'Minister Murphy launches Government Data Forum', *MerrionStreet.ie*. http://merrionstreet.ie/en/News-Room/Releases/Minister_Murphy_launches_Government_Data_Forum_.html.

Ministerie van Economische Zaken (2016), Aanbieding rapport expertgroep big data en privacy, brief van de minister van Economische Zaken aan de Tweede Kamer, 4 oktober 2016.

Ministerie van Onderwijs, Cultuur en Wetenschap (2016), Big data in onderwijs, cultuur en wetenschap, brief van de minister van Onderwijs, Cultuur en Wetenschap aan de Tweede Kamer, 28 juni 2016.

Ministerie van Veiligheid en Justitie (2016), Kabinetsstandpunt over het WRR-rapport Big Data in een vrije en veilige samenleving, brief van de minister van Veiligheid en Justitie aan de Tweede Kamer, 11 november 2016.

Mirani, L. (2013), 'The reason American tech firms like Ireland isn't just the low taxes', *Quartz*. https://qz.com/124133/the-reason-american-tech-firms-like-ireland-isnt-just-the-low-taxes/.

Mulligan, J. (2014), 'Massive Data Breach at Paddy Power Bookmakers', *Independent.ie*. http://www.independent.ie/business/irish/massive-data-breach-at-paddy-power-bookmakers-30474614.html.

Mulligan, D.K. and Bamberger, K.A. (2015), *Privacy on the Ground in the United States and Europe*, MIT Press.

Neuerer, D. (2017), 'Bundesregierung zerstreitet sich über Datenschutz', Handelsblatt.com. http://www.handelsblatt.com/politik/deutschland/merkel-gegen-datensparsamkeit-bundesregierung-zerstreitet-sich-ueber-datenschutz/19237484.html.

Norberg, P.A., Horne, D.R., and Horne, D.A. (2007), 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors', *Journal of Consumer Affairs*, Vol. 41, No.1, p. 100-126.

O'Brien, R., Holden, M. and Hosenball, M. (2013), 'British spy agency taps cables, shares with NSA: Guardian', *Reuters*. http://www.reuters.com/article/us-usa-security-britain-idUSBRE95K0ZV20130621.

Oerlemans, J.J., Custers, B.H.M., Pool, R.L.D. & Cornelisse, R. (2016), *Cybercrime en witwassen. Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*. Den Haag: Boom Juridische Uitgevers.

O'Keeffe, C. (2016), 'New laws to combat online abuse such as cyberbullying and revenge porn'. *Irish Examiner*. http://www.irishexaminer.com/ireland/new-laws-to-combat-online-abuse-such-as-cyberbullying-and-revenge-porn-422963.html.

Olsthoorn, P. (2016), *Big data voorfraudebestrijding*. The Hague: WRR.

Ottes, L. (2016), *Big Data in de zorg*, Den Haag: WRR.

Pateraki A. (2017). Germany Data Protection 2017 – Free Access. https://iclg.com/practice-areas/data-protection/data-protection-2017/germany#chaptercontent1.

Pintens, W. (1998), *Inleiding tot de rechtsvergelijking*, Leuven: Universitaire Pers Leuven.

Politie (2016), Verbeterplan Wet politiegegevens en Informatiebeveiliging. Zie: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2016/05/27/tk-bijlage-verbeterplan-wet-politiegegevens-en-informatiebeveiligign/tk-bijlage-verbeterplan-wet-politiegegevens-en-informatiebeveiligign.pdf.

Privacy First (2015), Visie op privacy 2.0, visiedocument, Amsterdam: Privacy First. See: https://www.privacy-first.nl/index.php?option=com_k2&view=item&layout=item&id=117&Itemid=156.

Privacy First (2016), *Jaarverslag 2015*, Amsterdam: Privacy First, juni 2016.

Privacy International (2015), Audited Financial Statements and Trustees' Report for the year ended 31 January 2015. https://privacyinternatio-nal.org/sites/default/files/Audited%20Financial%20Statement%202014-2015.pdf.

Privacy International (2015), *The right to Privacy in Sweden.* Stakeholder report for the UNHRC Universal Periodic Report, 2nd cycle 2012-2016 (21st session, January 2015 for Sweden).

Regan, P. M. (2002), *Privacy and commercial use of personal data: policy developments in the US*. Rathenau Institute Privacy Conference, Amsterdam, Jan 2002.

Regeerakkoord (2012), Bruggen slaan. Regeerakkoord VVD-PvdA, 29 oktober 2012.

Romano C. (2015), *Cookie Law, unaleggeche non piace. Tramulte, petizioni e tanta confusion*. http://it.ibtimes.com/cookie-law-una-legge-che-non-piace-tra-multe-petizioni-e-tanta-confusione-1404832

Roosendaal, A., Ooms, M., Hoepman, J.H. (2015), *Een raamwerk van indicatoren voor de bescherming van persoonsgegevens. Nederland ten opzichte van andere landen*. Delft: TNO (WODC), 2015.

Roosendaal, A., Nieuwenhuis, O., Ooms, M., Bouman-Eijs, A., en Huijboom, N. (2015), *Privacybeleving op het internet in Nederland*. Den Haag: TNO.

Sandee, R. (2014), 'Het zwarte gat van de internetconsultatie', *SC Online*, 28 oktober 2014. Zie: http://www.sconline.nl/achtergrond/het-zwarte-gat-van-de-internetconsultatie.

Şandru, S. (2013), 'About data protection and data retention in Romania', *Masaryk University Journal of Law and Technology*. Vol. 7, No. 2, p. 379-399.

Schendel, S. van (2016), *Het gebruik van Big Data door de mivd en aivd*, The Hague: WRR.

Schneier, B. (2009), 'State Data Breach Notification Laws: Have They Helped?' *Information Security*, January 2009.

Schröder, C. (2015), Die Unsichtbare, Zeit Online. http://www.zeit.de/2015/51/andrea-vosshoff-datenschutz-telekommunikation.

Schulze Greiving, V., Kulve, H. te, Konrad, K., Kuhlman, S., Pinkse, P. (2016), Nanotechnologie in dienst van veiligheid en justitie. Twente: Universiteit Twente, Department of Science, Technology and Policy Studies (STePS).

Siggins, L. (2016), 'Private investigator fined €7,500 over data protection breaches'. *The Irish Times*. https://www.irishtimes.com/news/ireland/irish-news/private-investigator-fined-7-500-over-data-protection-breaches-1.2824210.

Sloot, B. van der, Broeders, D., & Schrijvers, E. (2016), *Exploring the Boundaries of Big Data*. Amsterdam: Amsterdam University Press.

Sloot, B. van der, Schendel, S. van (2016), *International and comparative legal study on Big Data*. The Hague: WRR.

Taylor, C. (2016), 'Ireland seen as contender for data-driven investments'. *The Irish Times*. https://www.irishtimes.com/business/technology/ireland-seen-as-contender-for-data-driven-investments-1.2870112.

Teeffelen, K. van (2015), 'Organisaties zijn banger voor reputatieschade bij schending privacy', *Trouw*, 29 april 2015.

Tolboom, M., & Mazor, L. (2006), *Bekendheid en beleving informatieplicht onder burgers. Kwantitatiefonderzoekonder burgers*. Amsterdam: TNS-NIPO Consult.

Törngren, D. (2010), Department of Constitutional Law, Ministry of Justice Sweden, Memorandum 23 april 2010, Questionnaire for Member States on the implementation of Directive 95/46/EC.

Trilateral Research & Consulting (2013), Privacy impact assessment and risk management. Report for the Information Commissioner's Office.
https://ico.org.uk/media/1042196/trilateral-full-report.pdf.

UNCTAD (2016), *Data protection regulations and international data flows. Implications for trade and development*. United Nation Conference on Trade and Development (UNCTAD) New York: UN.

Van der Leest (2014), 'We zijn allemaal naakt', *Joop*, 3 september 2014. http://www.joop.nl/opinies/we-zijn-allemaal-naakt.

Van der Leij, J.B.J. (2015), *Privacyrecht en slachtoffers. Een studie naar de grondslagen en juridische kaders van privacy van slachtoffers*, (WODC) Den Haag: Boom Uitgevers.

Veld, P., Meijer, A., Schurink, M (2017), De Digidelta: samen versnellen; evaluatie van de nationale commissaris digitale overheid. Den Haag: ABDTopconsult. https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-evaluatie-nationaal-commissaris-digitale-overheid.

Versmissen, J.A.G. Terstegge, J.H.J., Siemers, K.M., en Tran, T.H. (2016), Evaluatie Toetsmodel PIA Rijksdienst. Utrecht: Privacy Management Partners.

Vodafone (2016), Big Data: A European Survey on the Opportunities and Risks of Data Analytics. http://www.vodafone-institut.de/bigdata/links/VodafoneInstitute-Survey-BigData-Highlights-en.pdf.

Vries, J. de (2013), 'Blijf af van onze privacy', *Trouw*, 14 juni 2014. http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/3459001/2013/06/14/Blijf-af-van-onze-privacy.dhtml.

Weckler, A. (2015), 'German Jeers at Irish Data Privacy May Help Us', *Independent.ie*. http://www.independent.ie/business/technology/news/german-jeers-at-irish-data-privacy-may-help-us-31266778.html.

Weckler, A. (2015), 'Tsunami of Data Breaches Strikes Irish Companies as Half Report Incidents', *Independent.ie*. http://www.independent.ie/business/technology/tsunami-of-data-breaches-strikes-irish-companies-as-half-report-incidents-34382305.html.

Weckler, A. (2015), 'Safe Harbour Is Gone but Europe Is Still Afraid to Tackle the US on Privacy', *Independent.ie*. http://www.independent.ie/business/technology/safe-harbour-is-gone-but-europe-is-still-afraid-to-tackle-the-us-on-privacy-31591450.html.

William Fry and Forbes (2016), Europe for Big Data. http://www.william-fry.com/docs/default-source/reports/william-fry-europe-for-big-data-report.pdf?sfvrsn=0.

Winter, H.B., Jong, P.O. de, Sibma, A., Visser, F.W.,Herweijer, M., Klingenberg A.M., Prakken, H. (2009), Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk, Groningen.

Woods, T. (2012), *How the Catholic Church Built Western Civilization*. Regnery Publishing, Inc.

Wright, D., en Hert, P. de (2012), *Privacy Impact Assessment*, Heidelberg: Springer.

WRR (2016), *Big data in een vrije en veilige samenleving*. Amsterdam: Amsterdam University Press.

Zeeuw, J. de (2009), 'De FG en de evaluatie van de WBP', *Privacy & Informatie*, afl. 2, april 2009, p. 91-93.

Zwenne, G.J., Duthler, A.W., Groothuis, M., Kielman, H., Koelewijn, W., en Mommers, L. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, Den Haag: WODC.

Appendix A. **Begeleidingscommissie**

Dit onderzoek is begeleid door een commissie met de volgende samenstelling:

- Prof. dr. Dennis Broeders (voorzitter)
  WRR, Erasmus Universiteit Rotterdam

- Mr. dr. Bas van der Leij
  WODC

- Mr. Just Stam
  Ministerie van Veiligheid en Justitie – DGRR

- Mr. dr. Heleen Janssen
  Ministerie van Binnenlandse Zaken en Koninkrijksrelaties – CZW

- Mr. Lotte Valkenburg
  Ministerie van Veiligheid en Justitie – DW

- Mr. Corrie Ebbers
  Ebbers Juridisch Advies, onafhankelijk privacy adviseur

Appendix B. **Geraadpleegde experts en instanties**

De volgende personen en instanties hebben informatie verschaft over de situatie aangaande de bescherming van privacy en persoonsgegevens in hun respectievelijke landen:

Nederland
- Koosje Verhaar
  Autoriteit Persoonsgegevens

Duitsland
- Sebastian Eschrich
  Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Prof. dr. Thomas Hoeren
  Institut für Informations-, Telekommunikations- und Medienrecht, Munster University

Zweden
- Johanna Carlsson
  Division for Constitutional Law Ministry of Justice Government Offices of Sweden
- David Törngren
  Division for Constitutional Law Ministry of Justice Government Offices of Sweden

Verenigd Koninkrijk
- Alain Kapper
  Information Commissioner's Office
- Andrew Charlesworth LLB
  University of Bristol

Ierland
- Dr. TJ McIntyre
  University College Dublin
- Dr. Paul Lambert
  Trinity College Dublin

Frankrijk
- Emmanuel Laforet
  Adjoint au chef de bureau du droit constitutionnel et du droit public général
  Direction des Affaires civiles et du Sceau, Ministère de la justice

Roemenië
- Prof. univ. dr. Ioana Vasiu
  Babeș-Bolyai University, Cluj-Napoca
- Bogdan Manolea
  APTI – Asociația pentru Tehnologie și Internet (Association for Technology and Internet)
- Oana Luisa Dumitru
  National Supervisory Authority for Personal Data Processing

Italy
- Paolo Balboni
  European Privacy Association
- Garante per la protezione dei dati personali

Appendix C. **Gebruikte vragenlijst**

Questionnaire
This questionnaire consists of five substantive parts and one part with general questions. Please provide answers to as many questions as possible, also when you cannot answer questions with a lot of detail or when answers are based on your expert knowledge rather than based on specific scientific research. In case you have detailed or supplementary information in reports or on specific websites, you can also send us these reports (or parts thereof) or links to relevant websites directly, but please indicate which parts answer which questions. Do not worry if these sources are not in English, we can take care of translating any relevant parts as long as you indicate where we should be looking.

In case you cannot answer a question, please skip this question. If you know of any people who may be able to answer these questions, we would appreciate it if you would notify us and send contact details to i.n.georgieva@law.leidenuniv.nl.

The aim of our research is to look at country specific approaches towards the protection of personal data. Please refer to national laws and regulations as much as possible, as referring to EU personal data protection law will not reveal the distinctions we are looking for.

Part I – General Situation
In order to provide a general description regarding the situation on protection of personal data in your country we would like information on the following topics:

1.1 What is the general situation regarding personal data protection?
What is the level of **awareness** of citizens and companies regarding personal data protection? Do citizens know which organizations are collecting their personal data and for which purposes? Are citizens aware of their rights? What is the **importance** of personal data protection according to citizens and companies? Is **compliance** the main concern for companies, does reputation play a role or are there other arguments to value data protection? Do citizens **feel in control** regarding what happens to their personal data? What **actions** do citizens take to protect their personal data and how often? (like taking security measures, using privacy settings, request for removal of their data, refuse consent for data processing and file complaints at companies and/or data protection authorities).

1.2 What is the role of national politics regarding personal data protection?

How often is personal data protection a subject of **debate in the national parliament** of your country? What are the viewpoints of the **major political parties** in your country on privacy and personal data protection? When debating privacy versus security, what is more important? Do they favor regulation or self-regulation? Is there a **dialogue** between political parties and civil rights organizations? What is the **general policy** on privacy and data protection of the current government? Please provide any policy documents, like coalition agreements or cabinet programs. Are there any recent developments in policies? Are there **information campaigns** on privacy or data protection initiated by the government or others?

1.3 Is there media attention for privacy and personal data protection?

Which topics related to privacy and data protection are discussed in the **media**? Is there a **nationwide debate** on privacy or data protection? How often are these topics in the media and in which media? What is the **attitude** of these news items towards privacy and data protection?

1.4 Have there been incidents regarding privacy and personal data protection?

Have there been incidents like **data breaches**, **data leaks**, **lawsuits**, and **economic damage**? Were there large or smaller incidents with high impact? Please describe the most relevant cases. What were the reactions to these incidents? Have citizens or organizations protested with regard to personal data protection? If so, how many people were involved and what were their concerns?

1.5 What is the role of civil rights organizations?

Which **civil rights organizations** are active and how large is their support? What role do they take (e.g., protesting or facilitating debates)? Do civil rights organizations actually influence government policies? Are they consulted when new legislation is prepared? Are these organizations well-known among citizens and companies? How many complaints and of what types do they receive?

Part II – National Government Policies

In order to describe national government policies regarding the protection of personal data in your country we would like information on the following topics:

2.1 What is the national government's policy regarding personal data protection?

Is there a general policy? Are there sector specific policies? Are risk analyses or Privacy Impact Assessments (PIAs) mandatory? How and when should PIAs be executed?

2.2 What is the role of privacy and personal data protection when creating new policies?

How does the government anticipate on new developments like **big data**, **internet of things**, **quantified self**, etc.? Is **privacy by design** used? Do privacy and personal data protection play a role in policy-making in other domains?

2.3 Which role does the national government take in the societal debate on privacy and personal data protection?

Does the government take an active or a reactive approach towards the societal debate? Is there a **dialogue** between the government and civil rights organizations? Does the government take opinions of citizens and companies into account when creating new policies and legislation (e.g. via **internet consultations**)?

2.4 Does the government provide information on personal data protection?

Are there **information campaigns** on privacy or data protection initiated by the government or others? Do these campaigns address citizens or companies or both? Does the government subsidize projects for creating further awareness?

Part III – Laws and regulations

In order to describe national laws and regulations regarding personal data protection in your country we would like information on the following topics:

3.1 Which laws and regulations constitute the implementation of EU Directive 95/46/EC?

Is the EU Directive implemented only at the level of **minimum requirements** or are there **additional provisions**? Are there any tensions between this legislation and other existing legislation?

3.2 Which other laws and regulations see to the protection of personal data?

Are there any **sector specific laws and regulations** relevant to personal data protection? Does this legislation concern sensitive categories of personal data?

3.3 Are there any other types of regulation applicable?

Are there any forms of **decentralized regulation**? Does **self-regulation** exist? Is self-regulation encouraged by the national government?

Part IV - Implementation

In order to describe the practical implementation of legislation and policies regarding the protection of personal data in your country we would like information on the following topics:

4.1 How is the protection of personal data ensured in practice in organizations?

Do organizations use **self-regulation** or **codes of conduct**? Are DPAs consulted regarding self-regulation or codes of conduct? How are codes of conduct enforced? How do organizations protect personal data (apart from information security)? Are internal policies connected to standards (like **ISO standards**, **DPA guidelines**, etc.)?

4.2 How many organizations (both government agencies and companies) have privacy officers?

How is the role of **privacy officer** implemented? Is this a full-time job or a task of an employee with other tasks? What are the authorities of the privacy officer? Does the privacy officer have an independent position? What are the activities of the privacy officer?

4.3 What technological and organizational measures are implemented by organizations to protect personal data?

Is the protection of personal data monitored within organizations? Are principles of **Privacy by Design** and **need-to-know** (role-based access) implemented? How is **information security** implemented (e.g., ISO certificates, codes of conduct)?

4.4 How much transparency is there regarding data collection and processing?
Do citizens read and understand **privacy policies**? Do organizations offer personalized **privacy settings**? How do organizations try to be transparent about collecting and processing personal data?

Part V – Regulatory Authorities and Enforcement
In order to describe the role of regulatory authorities and the enforcement of regulations regarding the protection of personal data in your country we would like information on the following topics:

5.1 What are the relevant regulatory/supervisory authorities (including DPAs) in the area of personal data protection and on which domains do they focus?
Are there any specific **target groups** for the regulatory authorities? What are the **budget** and the **number of employees** of each regulatory authority?

5.2 What is the role of the regulatory authorities (including DPAs)?
What are the **main activities** of the regulatory authorities (e.g., dealing with complaints, raising public awareness, monitoring compliance, providing advice, etc.)? What are their **priorities**? Is there a **dialogue** between the authorities and organizations under supervision? When do the authorities decide to start an investigation and when to impose sanctions? Do the authorities advice on proposed legislation? Do the authorities support citizens? What are the **competences** of the regulatory authorities (e.g., imposing fines, administrative sanctions, etc.)?

5.3 How do the regulatory authorities (including DPAs) use their competences?
How many **complaints** do the authorities receive? What types of complaints are these? In how many cases is there an act of enforcement (e.g., fines, administrative sanctions, etc.)? What sanctions are imposed? How many civil and criminal **lawsuits** are there in which the regulatory authorities do not play a role? What is the outcome of such lawsuits?

5.4 How do citizens and companies see the regulatory authorities?
Do citizens/companies know the regulatory authorities and are they aware of their activities? How do citizens/companies see the regulatory authorities? Do companies fear data protection authorities?

Part VI – General Questions

6.1 Do you know of literature that answers (several of) these questions for your country or any of the other countries mentioned?

6.2 Do you know of any comparisons between EU countries on one or more of the topics in this questionnaire?

6.3 Do you know any experts in your country that we should contact? If so, we would welcome contact details.

6.4 Do you have any contacts at your national or local Data Protection Authority that we can contact for this research?