Van Mourik Broekmanweg 6
2628 XE Delft
Postbus 49
2600 AA Delft

www.tno.nl

T +31 88 866 30 00
F +31 88 866 30 10

TNO-rapport

TNO 2015 R11474

Een raamwerk van indicatoren voor de bescherming van persoonsgegevens; Nederland ten opzichte van andere EU-landen

Datum	10 december 2015
Auteur(s)	Arnold Roosendaal Merel Ooms Jaap-Henk Hoepman
Exemplaarnummer	
Oplage	
Aantal pagina's	48 (incl. bijlagen)
Aantal bijlagen	
Opdrachtgever	WODC
Projectnaam	Bescherming van de privacy van burgers
Projectnummer	060.17318

Inhoudsopgave

Managementsamenvatting

Vanuit de Tweede Kamer is de vraag gekomen hoe de positie van Nederland is wat betreft de bescherming van privacy van burgers door de overheid in vergelijking met andere Europese landen. Dit kan onderzocht worden in een benchmarkstudie waarin Nederland op dit terrein wordt vergeleken met een aantal andere Europese landen. Om deze studie goed op te zetten is er eerst een kader nodig van de onderwerpen die deze vergelijking moet beslaan, welke bronnen gebruikt kunnen worden, welke onderzoeksmethoden gehanteerd kunnen worden en met welke landen Nederland het beste vergeleken kan worden. De voorliggende rapportage geeft een overzicht van dit kader. De daadwerkelijke benchmark zal in een vervolgonderzoek plaatsvinden.

In deze rapportage is een raamwerk neergezet voor het bepalen van de relevante onderwerpen voor de vergelijking. Per onderwerp is een uitwerking gemaakt 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. In het onderzoek is, in lijn met de vraagstelling vanuit het WODC, de focus gelegd op bescherming van persoonsgegevens in plaats van op privacy in den brede. 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.

Tevens is een selectie van landen gemaakt waarmee vergeleken kan worden. De geselecteerde landen zijn Frankrijk, Duitsland, Verenigd Koninkrijk, Ierland, een Scandinavisch land, een Zuid-Europees land, en een Oost-Europees land (dat nog maar kort lid is van de EU). Deze landen zijn geselecteerd aan de hand van de criteria betreffende de houding ten aanzien van privacy, mate van openheid in hoe burgers met elkaar omgaan (zoals het meer of minder makkelijk delen van gegevens), opvallende aspecten met betrekking tot strengheid of soepelheid van regelgeving en toezicht, en de implementatie van Europese regelgeving binnen het bestaande juridisch kader of systeem in een land (civil law of common law) en eventuele legacy van verouderde regelgeving. Aanbevolen wordt om in het vergelijkend onderzoek vijf landen inclusief Nederland te betrekken. De definitieve selectie is aan de onderzoekers van het vervolgproject. Datzelfde geldt voor de definitieve selectie van indicatoren. De selectie zal afhangen van de toegang tot bronnen en kennis van methoden die de onderzoekers zullen hebben, evenals van het beschikbare budget voor het onderzoek.

Een begeleidingscommissie die vanuit het WODC is ingesteld heeft input en commentaar geleverd. Daarnaast is door enkele externen een review gepleegd.

1 Inleiding

1.1 Aanleiding

Op 26 november 2014 dienden Tweede Kamerleden Schouw (D66) en Oosenbrug (PvdA) een motie in waarin zij de regering verzochten om onderzoek uit te laten voeren naar de positie van Nederland met betrekking tot de bescherming van de privacy van haar burgers. De achtergrond van de motie is dat er onduidelijkheid bestaat over de mate waarin Nederland de privacy van haar burgers beschermt, en welke positie Nederland hierin inneemt ten opzichte van andere Europese landen. In het licht van de aankomende Algemene Verordening Gegevensbescherming die de Europese Richtlijn Gegevensbescherming uit 1995 zal gaan vervangen, is het belangrijk om te weten wat de positie van Nederland is ten opzichte van andere Europese landen op het gebied van bescherming van persoonsgegevens. Met de Verordening zal er immers een regime komen dat gelijkelijk van toepassing zal zijn in alle Europese lidstaten. Hoewel de motie spreekt over bescherming van privacy vraagt het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) in de 'Verkorte startnotitie WODC onderzoek' om dit onderzoek te richten op de bescherming van persoonsgegevens, om met het oog op de werkbaarheid de breedte van het onderzoek af te bakenen. TNO heeft van het WODC opdracht gekregen om in reactie op de motie een raamwerk op te zetten voor dit benchmarkonderzoek. In deze rapportage wordt daarom een kader ontworpen met daarin onderwerpen binnen de bescherming van persoonsgegevens. die uitgewerkt worden in indicatoren en geoperationaliseerd in variabelen. Deze variabelen kunnen in verschillende landen gemeten worden om daarmee een vergelijking te kunnen maken. Ook wordt een overzicht en beschrijving gegeven van een voorselectie van Europese landen buiten Nederland die vanuit inhoudelijk oogpunt interessant zijn om mee te nemen in de vergelijking.

De vragen die beantwoord worden zijn:

1. Welke indicatoren kunnen worden gebruikt om te komen tot een vergelijking van Europese landen aangaande de bescherming van de privacy van de burgers?
2. Met welke andere landen binnen de Europese Unie kan Nederland het beste worden vergeleken?

Ten behoeve van onze onderzoeksvraag hanteren we de definitie van persoonsgegevens uit de Richtlijn Bescherming Persoonsgegevens (Richtlijn 95/46/EG): "iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon".[1]

In dit raamwerk staat de bescherming van persoonsgegevens van burgers door de Nederlandse overheid centraal. De reden hiervoor is dat in de motie gevraagd is hoe 'Nederland' de privacy van 'haar' burgers beschermt, waarbij wij menen dat hiermee de overheid bedoeld wordt. De meeste indicatoren meten dus iets dat de overheid of een instituut dat is opgericht vanuit de overheid zoals de

[1] Artikel 2(a) uit de Richtlijn.

toezichthouder, wel of niet doet, en hoe ze dit doen. Voorbeelden zijn het vormen van beleid of het geven van voorlichting. Op een aantal punten is echter ook aandacht voor de bescherming van persoonsgegevens door bedrijven of andere organisaties buiten de overheid.[2] Vaak gaat het daarbij om de doorwerking van overheidsbeleid (waaronder regelgeving) in de praktijk bij organisaties waaronder ook de overheid. De meeste indicatoren gaan dus over bescherming van persoonsgegevens waar de overheid op een bepaalde manier een hand in heeft en niet over activiteiten waar de overheid geen betrokkenheid bij heeft. Alleen bij het eerste onderwerp (situatieschets) wordt hier een uitzondering op gemaakt. De reden hiervoor is dat de context van een land (zoals de culturele achtergrond) invloed heeft op de manier waarop de overheid van een land opereert op het gebied van bescherming van persoonsgegevens. Daarbij komt onder andere aan bod wat burgers doen om hun persoonsgegevens te beschermen, wat burgerrechtenorganisaties doen, wat de toon in de media is over bescherming van persoonsgegevens en wat de standpunten zijn van politieke partijen over dit onderwerp.

In dit onderzoek wordt gekeken naar de bescherming van persoonsgegevens door de overheid vanuit haar administratieve rol en de invulling die organisaties hieraan geven. Ook de verwerking van persoonsgegevens voor de uitvoering van de politietaak is meegenomen. De activiteiten van inlichtingen- en veiligheidsdiensten vormen echter geen onderdeel van dit onderzoek om de scope te beperken. Bovendien is het type toepassingen in dat kader van een andere aard en is het moeilijk om deze activiteiten internationaal te vergelijken omdat het beleid hierop nationaal bepaald wordt en dus sterk verschillend is.

1.2 Methode en raamwerk

Het doel van dit onderzoek is om indicatoren op te stellen ter voorbereiding van een vergelijkend onderzoek naar de mate waarin Nederland de persoonsgegevens van haar burgers beschermt ten opzichte van andere Europese landen. Deze rapportage bevat 1) een lijst met indicatoren die gezamenlijk een beeld geven van de mate waarin persoonsgegevens worden beschermd in een land, en 2) een overzicht van Europese landen die als basis kunnen dienen voor een vergelijkende studie op basis van de indicatoren. Hieronder wordt kort beschreven hoe het raamwerk is opgebouwd. In hoofdstuk 2 wordt verder toegelicht hoe de verzameling en selectie van de verschillende onderdelen van het raamwerk hebben plaatsgevonden.

1.2.1 Onderwerpen

Om tot een lijst van indicatoren te komen, zijn eerst een aantal onderwerpen opgesteld die fungeren als categorieën waarbinnen indicatoren geformuleerd kunnen worden die iets zeggen over de mate waarin een land de persoonsgegevens van haar burgers beschermt. Deze onderwerpen zeggen nog weinig over waar precies naar gekeken moet worden om dit te meten, maar zorgen ervoor dat de vraagstelling vanuit verschillende deelaspecten wordt belicht, zoals

[2] In deze rapportage zal over ‘organisaties’ gesproken worden als het over zowel de overheid als het bedrijfsleven gaat. Wanneer specifiek het bedrijfsleven wordt bedoeld dan zal deze benaming gebruikt worden en wanneer het alleen over de overheid gaat zal deze benaming gebruikt worden.

beleid of toezicht en handhaving. Om cultuur en maatschappelijk perspectief mee te nemen naast beleidsmatige en wettelijke indicatoren is er in het rapport een onderdeel ‘situatieschets’ opgenomen waaronder zaken vallen als de betrokkenheid van burgers en bedrijven, aandacht in de media en opvallende zaken die in een land spelen rond de bescherming van persoonsgegevens.

1.2.2 Indicatoren

Per onderwerp is vervolgens een lijst van indicatoren opgesteld die binnen het kader van dat onderwerp relevant zijn voor de bescherming van persoonsgegevens in een land. Een voorbeeld van een indicator die binnen het onderwerp ‘beleid’ valt is ‘bestaand beleid’. Een indicator geeft binnen een onderwerp een weergave van hoe een land op een bepaald gebied de persoonsgegevens van haar burgers beschermt, zonder nog volledig geoperationaliseerd te zijn.

1.2.3 Variabelen

Per indicator zijn er een aantal variabelen opgesteld die gezamenlijk een indicator operationaliseren en hier een compleet beeld van geven. Wanneer er informatie wordt verzameld over deze variabelen kunnen uitspraken gedaan worden over in hoeverre de persoonsgegevens op het gebied van een indicator beschermd worden, zoals de rol die de overheid speelt of organisaties die maatregelen treffen.

1.2.4 Landenselectie

In een tweede deel van deze rapportage wordt een voorselectie gemaakt van Europese landen, buiten Nederland, waarin de indicatoren onderzocht kunnen worden. Om het vervolgonderzoek overzichtelijk te houden is het aan te bevelen het totale aantal te vergelijken landen, inclusief Nederland, op ongeveer vijf te houden. De selectie van landen waarmee de vergelijking wordt uitgevoerd dient daarom een gevarieerd overzicht op te leveren van de mate waarin Nederland de privacy van haar burgers beschermt ten opzichte van een aantal andere landen binnen de Europese Unie. Dat betekent dat de vergelijking zowel een beeld moet opleveren van sterk verschillende factoren, maar ook van meer genuanceerde verschillen of juist overeenkomsten tussen Nederland en andere landen. De verschillen kunnen ingegeven worden door verschillen in wettelijke en politieke systemen, de mate waarin en hoe lang het onderwerp privacy de aandacht heeft en de duur van het EU-lidmaatschap van een land en daarmee samenhangende geschiedenis qua wetgeving (al wel of niet langere tijd Europese wetgeving), maar ook door verschillen in culturele opvattingen binnen landen. Een cultuur van openheid en transparantie levert bijvoorbeeld een andere positie op dan een meer gesloten cultuur. De invloed van cultuur zal echter zijn weerslag vinden in alle gedefinieerde criteria, deze wordt daarom niet als apart criterium onderscheiden. Echter, deze invloed wordt geoperationaliseerd in de andere criteria voor landenselectie. Hoe dit wordt gedaan wordt toegelicht in hoofdstuk 8. Als gevolg van bovenstaande zal de selectie van landen plaatsvinden aan de hand van de volgende criteria:

- 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

De geselecteerde landen, onderwerpen, indicatoren en variabelen zijn gebaseerd op eerder onderzoek, een brainstorm met het projectteam, en inbreng vanuit de begeleidingscommissie vanuit het WODC. Er heeft tevens een consultatie per email plaatsgevonden met externe experts op het gebied van bescherming van persoonsgegevens en methoden van onderzoek, waarin met name de volledigheid van de indicatoren is getoetst. De externe experts die het rapport becommentarieerd hebben zijn:

- Marjon Schols (Ministerie van BZK), methodisch expert
- Jascha Wieldraaijer (Ministerie van BZK), methodisch expert
- Simone Fennell- van Esch (Privacy Company), juridisch expert

2 Raamwerk

In dit hoofdstuk wordt verder toegelicht op welke manier de onderwerpen, indicatoren en variabelen zijn geselecteerd. Aan het einde van dit hoofdstuk wordt een overzicht gegeven van de geselecteerde onderwerpen en indicatoren. De variabelen worden vervolgens in hoofdstuk drie tot en met zeven per onderwerp en indicator genoemd en uitgewerkt.

2.1 Keuze van de onderwerpen en indicatoren

Zoals in paragraaf 1.2 werd aangegeven zijn er eerst onderwerpen geformuleerd, die een kader geven voor de indicatoren die informatie geven voor de benchmark van de bescherming van persoonsgegevens. De theoretische basis voor de keuze van deze onderwerpen en de volgorde waarin zij staan wordt gevormd door de inrichting van de conventionele beleidscyslus (Jann & Wegrich, 2007) en theorie over beleidscomponenten (Howlett, 2009). De conventionele beleidscyclus bestaat uit verschillende fasen in een beleidsproces, namelijk: agenda-setting, policy formulation, decision making, implementation and evaluation. In de onderwerpen komt ‘agenda-setting’ terug in de situatieschets, waarin de problematiek en de context daarvan toegelicht wordt. De fasen ‘policy formulation en ‘desicion making’ komen terug in de onderwerpen beleid en wet- en regelgeving. Daar vallen onder andere de vorming van beleid onder en de regels die gelden. De fase ‘implementation’ komt terug in het onderwerp implementatie. Daarbij wordt onder andere gekeken naar de uitwerking van beleid en regelgeving in de praktijk. De fase ‘evaluation’ komt niet nadrukkelijk terug in de onderwerpen. Het onderzoek zelf vormt deels een evaluatie van in hoeverre een land erin slaagt om persoonsgegevens te beschermen. Indien voorhanden zou gebruik gemaakt kunnen worden van evaluatiestudies die zijn uitgevoerd om de effectiviteit van beleid op het gebied van bescherming persoonsgegevens te meten. Omdat de beschikbaarheid hiervan mogelijk beperkt en wisselend zal zijn per land zijn deze evaluaties niet als onderwerp opgenomen, maar er zou onder ‘situatieschets’ of ‘beleid’ aandacht aan besteed kunnen worden indien er in een land relevante studies beschikbaar zijn.

Op basis van bovenstaande indeling is het mogelijk om de rol van de overheid vanuit verschillende perspectieven te benaderen. Primair ontstaat een beeld van wat de overheid zelf doet, bijvoorbeeld op het gebied van regelgeving. Secundair ontstaat een beeld van wat organisaties (waaronder de overheid) doen als gevolg van beleid en regelgeving door de overheid. In dit rapport wordt uitgegaan van factoren waarbij de overheid direct of indirect invloed heeft op de bescherming van persoonsgegevens. De toezichthouder vormt enigszins een uitzondering hierop. Deze is onafhankelijk en kan dus een eigen beleid voeren en eigen prioriteiten stellen. Ook kan de toezichthouder zelf bepalen welke handhaving opportuun wordt geacht. De wetgeving over de functie en bevoegdheden van de toezichthouder wordt door de nationale overheid vastgesteld maar gebaseerd op Europese regelgeving, de Algemene Richtlijn Gegevensbescherming (95/46/EG). In dit rapport zijn de onderwerpen uit deze richtlijn opgenomen. De indicatoren zijn dus alleen van toepassing voor de onderlinge vergelijking van Europese lidstaten en zouden aangepast moeten worden om deze op grotere internationale schaal

relevant te maken. Specifieke punten waarop geen discretionaire bevoegdheid bestaat, en waar dus geen verschil op zal treden tussen lidstaten, zijn om die reden achterwege gelaten.

In een overzicht van beleidscomponenten van Howlett (2009) worden verschillende beleidsniveaus geformuleerd. Er zijn in beleid doelen en middelen die een hoog abstractieniveau hebben (macro niveau), maar ook die op het niveau van beleidsprogramma's geoperationaliseerd worden (meso niveau) en een praktische uitwerking daarvan (micro niveau). Deze beleidsniveaus komen terug doordat de onderwerpen en indicatoren verschillende maten van abstractie kennen. Zo zijn de onderwerpen beleid en wet- en regelgeving overwegend theoretisch van aard en staan de onderwerpen situatieschets en implementatie dicht bij de praktijk. Bij die laatste gaat het meer om wat er in de praktijk gebeurt en minder over wat er afgesproken is.

De onderwerpen en de invulling daarvan komt ook deels voort uit eerder monitoringsonderzoek. In de e-Privacy Quickscan die TNO in opdracht van het ministerie van Economische Zaken heeft uitgevoerd in 2013 (Van Veenstra et al., 2013) werden de indicatoren ingedeeld in drie categorieën die een plek vinden in het huidige kader. De eerste categorie 'instrumenten' is in deze opzet beleid en wet -en regelgeving geworden. De tweede categorie 'bewustwording' komt terug in indicatoren over voorlichting. Tenslotte de derde categorie 'houding van burgers' komt terug in de betrokkenheid van burgers en de rol van burgerrechtenorganisaties. Ten aanzien van deze laatste categorie is ook gekeken naar de resultaten uit het rapport 'Privacybeleving op het internet in Nederland' (Roosendaal et al., 2015).

In het totale raamwerk dat ontstaat door de onderwerpen, indicatoren en variabelen worden zowel formele en meer theoretische (wat is er wettelijk vastgelegd) als materiële en meer praktische (wat gebeurt er in de praktijk) aspecten meegenomen. Een voorbeeld van een theoretisch aspect is de indicator 'wet- en regelgeving op het gebied van bescherming van persoonsgegevens' en een praktische indicator is 'media-aandacht voor de bescherming van persoonsgegevens'. Wanneer alleen theoretische factoren meegenomen zouden worden dan zou er een beperkt beeld ontstaan doordat gemist zou worden wat er in de praktijk gebeurt. Andersom zou een beperking tot de praktijk inhouden dat onbekend is binnen welke theoretische kaders activiteiten plaatsvinden.

2.2 Keuze van de variabelen

De variabelen die in deze rapportage zijn opgenomen om de indicatoren te meten zijn relatief uitgebreid en lopen uiteen qua onderwerp en methode om deze te kunnen onderzoeken. Om te voorkomen dat de scope van het onderzoek (op basis van het raamwerk dat in dit rapport wordt beschreven) te breed wordt of het teveel werk gaat kosten, wordt aan het eind van iedere paragraaf waarin een indicator wordt toegelicht een advies gegeven aan de onderzoekers voor de selectie van de variabelen. Daarbij worden ook overwegingen gegeven voor het wel of niet meenemen van bepaalde variabelen in het uiteindelijke onderzoek. De onderzoekers kunnen deze overwegingen meenemen in hun uiteindelijke keuze. Bij

dit advies wordt een aantal criteria meegenomen die helpen om een goede selectie te maken. Deze criteria zijn de volgende:

1. **Meetbaarheid**: is iets te meten?
2. **Relevantie**: hoe cruciaal is het om dit te weten?
3. **Haalbaarheid**: hoeveel tijd en energie kost het om dit te doen?
4. **Coherentie**: sluit het goed aan bij de andere indicatoren en variabelen en meten de variabelen een indicator?

Van sommige indicatoren of variabelen schatten wij in dat deze moeilijk te meten zijn of veel werk kosten, maar wel relevant zijn voor het onderwerp. In dit rapport hebben wij deze er omwille van compleetheid wel in laten staan maar in het advies aan de onderzoekers worden de overwegingen hieromtrent genoemd. De onderzoekers kunnen besluiten of deze belangrijk genoeg zijn om er in te laten en te kijken hoe dit gemeten kan worden of dat deze niet worden meegenomen.

De variabelen zijn zo concreet mogelijk gesteld maar bieden ook ruimte voor de onderzoekers die de benchmark gaan uitvoeren om keuzes te maken voor de exacte formulering en afbakening. Dit omdat de beschikbare bronnen en exacte informatie per land kunnen verschillen. Uiteindelijk dient er een indicatie te worden gegeven van de benoemde aspecten van bescherming van persoonsgegevens in de verschillende landen. In sommige gevallen wordt aanbevolen om de periode die onderzocht wordt te beperken, zoals een periode waarin berichtgeving in de media onderzocht wordt of het aantal klachten dat bij de toezichthouder is binnengekomen. De onderzoekers kunnen na verdere verdieping het beste zelf kiezen welke tijdsperiode hiervoor passend is.

Voor iedere variabele worden één of meerdere methoden benoemd waarmee deze mogelijk gemeten zou kunnen worden. We geven suggesties voor verschillende methoden omdat niet bij ons bekend is wat de omvang van het uiteindelijke onderzoek zal zijn. Om dezelfde reden worden waar mogelijk verschillende bronnen benoemd die geraadpleegd kunnen worden om de informatie te vergaren.

2.3 Overzicht

In Tabel 1 is een overzicht gegeven van de onderwerpen en indicatoren die uitgewerkt worden in hoofdstuk drie tot en met zeven. De indicatoren worden in paragrafen uitgewerkt waarbij een overzicht wordt gegeven van de variabelen die informatie geven over deze indicator.

Tabel 1 Overzicht onderwerpen en indicatoren

Onderwerp	Indicatoren
1. Situatieschets	Betrokkenheid van burgers en bedrijven Rol van de politiek Aandacht in de media Incidenten Rol van burgerrechtenorganisaties
2. Beleid	Bestaand beleid Beleidsvorming

	Rol van de overheid in het maatschappelijk debat Voorlichting door de overheid
3. Wet- en regelgeving	Wetten met impact op bescherming persoonsgegevens Regulering vanuit de overheid
4. Implementatie	Zelfregulering/gedragscodes Invulling rol privacy officer Algemeen technische en organisatorische maatregelen Transparantie door organisaties
5. Toezicht en handhaving	Algemene kenmerken van de toezichthouder Rolinvulling van de toezichthouder Bevoegdheden van de toezichthouder Handhaving door de toezichthouder Opvatting over toezichthouder bij burgers en bedrijven

3 Situatieschets

Het eerste onderwerp in dit raamwerk is de situatieschets. In dit gedeelte van het onderzoek wordt een overzicht gegeven van de algemene situatie rondom de bescherming van persoonsgegevens in een land. Hierdoor krijgt de lezer van het onderzoek een beter beeld van de context waarin persoonsgegevens in een bepaald land beschermd worden. Daarbij moet er rekening mee gehouden worden dat politieke systemen verschillen per land, en dat dit invloed kan hebben op de manier waarop de bescherming van persoonsgegevens georganiseerd is. Typische indicatoren die van belang zijn voor de context in een land zijn de mate waarin burgers en bedrijven betrokkenheid tonen bij de bescherming van persoonsgegevens, de rol van politieke partijen en de aandacht die in de media aan dit onderwerp besteed wordt. In dit onderwerp komen componenten terug die te maken hebben met de mate waarin het onderwerp leeft (hoe belangrijk vindt men het, wordt er in de media veel over gesproken), bedreigingen die er zijn voor de privacy van persoonsgegevens (incidenten) en de druk die er binnen een land is om ervoor te zorgen dat de overheid en andere organisaties persoonsgegevens beschermen (de rol van burgerrechtenorganisaties).

3.1 Betrokkenheid burgers en bedrijven

Een indicator die inzicht geeft in de situatie rond de bescherming van persoonsgegevens in een land is de betrokkenheid van burgers en bedrijven bij dit onderwerp. Dit komt onder andere naar voren in de kennis die zij hierover hebben, hoe belangrijk zij dit vinden en de activiteiten die zij ondernemen om persoonsgegevens te beschermen. Dit kan uitgedrukt worden in de variabelen uit Tabel 2 Variabelen betrokkenheid burgers en bedrijven Tabel 2 ‘Variabelen betrokkenheid burgers en bedrijven’.

Tabel 2 Variabelen betrokkenheid burgers en bedrijven

Variabele	Methode en bronnen
Weten burgers wat er met hun persoonsgegevens gedaan wordt door organisaties? (Bijvoorbeeld: wat wordt er verzameld en door wie)	Desk research[3] (secundaire analyses op bestaande surveys, rapporten en verslagen van eerder onderzoek[4]), nieuwe survey of focusgroepen met burgers
Hoe belangrijk vinden burgers de bescherming van hun persoonsgegevens?	Desk research (secundaire analyses op bestaande surveys, rapporten en verslagen van eerder onderzoek), nieuwe survey of focusgroepen met burgers

[3] Desk research zal in veel gevallen moeten worden uitgevoerd door country correspondents of anderen die de taal spreken in een land. Een deel van de benodigde informatie zal vermoedelijk in het Engels beschikbaar zijn, maar een groot deel ook niet.
[4] Voorbeelden van bronnen: Privacybeleving op het internet in Nederland (2015), Special Eurobarometer (2015).

Variabele	Methode en bronnen
Hebben burgers het gevoel controle te hebben over wat er met hun persoonsgegevens gebeurt?	Desk research (secundaire analyses op bestaande surveys, rapporten en verslagen van eerder onderzoek), nieuwe survey of focusgroepen met burgers
Wat doen burgers om hun persoonsgegevens te beschermen? (Bijvoorbeeld: beveiliging, vragen om verwijdering gegevens, weigeren gegevens af te staan)	Desk research (secundaire analyses op bestaande surveys, rapporten en verslagen van eerder onderzoek), nieuwe survey of focusgroepen met burgers
Zijn er protestacties vanuit burgers geweest die te maken hadden met bescherming van persoonsgegevens? Zo ja hoeveel en waar gingen deze over?	Media analyse (Lexis Nexis), expert interviews (burgerrechtenorganisaties, beleidsmakers)
Wat is de houding van bedrijven met betrekking tot de bescherming van persoonsgegevens? (Vinden zij dit belangrijk en hoe uit zich dat?)	Interviews (selectie van bedrijven die data verwerken), desk research (secundaire analyses op bestaande surveys, rapporten en verslagen van eerder onderzoek), nieuwe survey
Welke kennis hebben bedrijven over de bescherming van persoonsgegevens? (hoe kunnen zij dit doen, kennen zij de toezichthouder)	Interviews (selectie van bedrijven die data verwerken), desk research (secundaire analyses op bestaande surveys, rapporten en verslagen van eerder onderzoek), nieuwe survey

Conclusie indicator

De eerste vier van de variabelen bij deze indicator gaan over hoe burgers denken over de bescherming van persoonsgegevens. Deze informatie is goed meetbaar, al is het voor dit onderzoek mogelijk niet relevant genoeg voor een aparte survey omdat het handelen van de overheid centraal staat. Dit is echter wel te overwegen wanneer er voldoende variabelen te meten zijn in het onderzoek om een survey te vullen. Een alternatief is om één of meerdere focusgroepen te organiseren met burgers. Het krijgen van informatie over de houding van burgers is het meest haalbaar wanneer deze informatie uit bestaande monitors gehaald kan worden. Dit type informatie wordt nationaal en internationaal regelmatig bijgehouden in monitors van overheden. TNO heeft in 2015 bijvoorbeeld de monitor 'Privacybeleving op het internet in Nederland ontwikkeld, en op Europees niveau is er de Special Eurobarometer (laatste versie uit maart 2015). De informatie zal echter niet 100% vergelijkbaar zijn wanneer deze uit verschillende nationale monitors komt en is niet in ieder land jaarlijks beschikbaar.

De variabele met de vraag naar protestacties van burgers is te meten door een media analyse of expert interviews met bijvoorbeeld burgerrechtenorganisaties of beleidsmakers. Het is wel relevant maar behoort niet tot de kern van dit onderzoek. Wanneer er wordt besloten om een media analyse te doen of deze experts te spreken dan is het haalbaar en kan deze vraag meegenomen worden.

De houding van bedrijven ten aanzien van bescherming persoonsgegevens is meetbaar via een nieuwe of bestaande survey of via interviews met een selectie

van bedrijven. Deze variabele moet dan nog wel verder gespecificeerd worden. Bij de afbakening van de groep bedrijven kan het beste gekeken worden naar bedrijven die afkomstig zijn uit het land dat bestudeerd wordt en daar ook actief zijn. Buitenlandse bedrijven die in een land actief zijn (zoals Amerikaanse bedrijven) kunnen anders omgaan met de bescherming van persoonsgegevens, al zullen ook zij gehouden worden aan de lokale wet- en regelgeving. Het kan echter moeilijker zijn om van die bedrijven informatie te verkrijgen omdat zij op grotere afstand staan van een land en dit vaker grote bedrijven zijn die minder toegankelijk zijn.

3.2 Rol van de nationale politiek

Een andere indicator die een indruk geeft van de situatie in een land is de rol van de nationale politiek ten aanzien van bescherming van persoonsgegevens. Enerzijds gaat dat om hoe vaak dit onderwerp wordt besproken in het parlement van een land, maar daarnaast is het van belang op welke manier hierover gedacht wordt door de politieke partijen. Er zou gekozen kunnen worden voor de grootste partijen van een land, aangezien deze partijen een groot deel van het volk vertegenwoordigen. Omdat echter niet alleen vanwege de positie op het gebied van bescherming van persoonsgegevens gekozen wordt voor een politieke partij wordt aanbevolen ook te kijken naar de standpunten van kleinere partijen. Deze reflecteren immers ook vaak de punten waarop zij kritiek hebben als oppositie. Bij deze indicator vormt het een uitdaging om te bepalen wanneer iets valt onder het onderwerp bescherming persoonsgegevens. In de inleiding werd al een definitie van persoonsgegevens gegeven die gebruikt kan worden. Vervolgens kan er bijvoorbeeld een lijst met zoektermen opgesteld worden die verwijzen naar onderwerpen waarbij persoonsgegevens beschermd worden of de bescherming hiervan juist bedreigd wordt (zoals het verzamelen van telecommunicatiegegevens).

Tabel 3 Variabelen rol van de nationale politiek

Variabele	Methode en bronnen
Hoe vaak worden onderwerpen rond de bescherming van persoonsgegevens besproken in het parlement van een land?[5]	Desk research (archieven op overheidswebsites, verslagen parlementaire debatten, stemmingen voor wetsvoorstellen of moties omtrent bescherming persoonsgegevens)
Welke standpunten hebben politieke partijen over de bescherming van persoonsgegevens? (vinden zij veiligheid mogelijk belangrijker dan privacy, wat moet volgens hen vastgelegd zijn in wetten en wat hoort volgens hen onder zelfregulering)	Desk research (o.a. partijprogramma's en standpunten op websites politieke partijen), interviews (selectie van politieke partijen: partijbureaus of woordvoerders)
Zijn politieke partijen in dialoog met belangenorganisaties over de bescherming van persoonsgegevens?	Interviews (selectie van politieke partijen: partijbureaus of woordvoerders, belangenorganisaties)

[5] Het is van belang om deze informatie te duiden via landenspecifieke factoren zoals het politieke systeem in een land.

Conclusie indicator
Op het gebied van de meetbaarheid van de eerste variabele is het vooral een uitdaging om het onderwerp af te bakenen. Er kan voor gekozen worden om een aantal onderwerpen te kiezen op het gebied van bescherming persoonsgegevens en om in een bepaalde periode te kijken hoe vaak het aan bod komt in het parlement. Deze variabele is erg relevant voor het onderwerp en goed haalbaar door het bestuderen van documenten uit archieven van overheidswebsites, zoals verslagen parlementaire debatten, stemmingen voor wetsvoorstellen of moties omtrent bescherming persoonsgegevens. Een vereiste hiervoor en voor veel van het desk research voor dit onderzoek is wel dat er per land een native speaker beschikbaar is om deze analyse goed te kunnen doen.
De standpunten van politieke partijen zijn over het algemeen te achterhalen via hun partijprogramma's. Wel kan het zo zijn dat de bescherming van persoonsgegevens niet aan bod komt in een partijprogramma, terwijl ze er wel een standpunt over hebben. Wanneer deze informatie niet in partijprogramma's naar voren komt kan besloten worden om interviews te houden met woordvoerders of werknemers van partijbureaus. Deze variabele is relevant voor het achterhalen van de rol van de politiek naast het beleid dat wordt gemaakt door de overheid.
De mate van contact tussen politieke partijen en belangenorganisaties (in Nederland bijvoorbeeld Thuiswinkel.org of de Consumentenbond) over dit onderwerp is het beste te achterhalen via interviews met beide groepen. Mogelijk is dit ook te achterhalen op basis van evenementen waar zowel de politiek als belangenorganisaties vertegenwoordigd waren, zoals debatten of congressen. De kans is dan groot dat zij contact hebben.

3.3 Aandacht in de media

De hoeveelheid media-aandacht voor het onderwerp bescherming van persoonsgegevens en gerelateerde onderwerpen geeft een indicatie over hoe sterk dit onderwerp leeft in een land. Wanneer er veel over geschreven wordt is de kans groot dat het onderwerp leeft bij de bevolking van een land. Hierbij moet vanzelfsprekend rekening gehouden worden met de omvang van een land omdat in een groter land ook meer mediabronnen zullen zijn. Vervolgens is het van belang om niet alleen naar de hoeveelheid berichten te kijken maar ook naar wat de inhoudelijke strekking is van de berichtgeving. Zijn de media bijvoorbeeld overwegend kritisch over het gebruik van persoonsgegevens door organisaties of beargumenteert men dat regelgeving op dit gebied vooral hinderlijk is voor economische groei? De strekking zal mede afhankelijk zijn van de politieke kleur van een medium. Met media worden zowel online als offline media bedoeld, en zowel geschreven als audiovisueel.

Tabel 4 Variabelen aandacht in de media

Variabele	Methode en bronnen
Welke onderwerpen gerelateerd aan bescherming persoonsgegevens worden besproken in de media?	Media-analyse (Lexis nexis database)
Hoe vaak komen onderwerpen gerelateerd aan bescherming persoonsgegevens in de media?	Media-analyse (Lexis nexis database)

Hoe is de inhoudelijke strekking van de berichtgeving over bescherming van persoonsgegevens?	Media-analyse (Lexis nexis database)

Conclusie indicator
De variabelen die vallen onder de indicator 'aandacht in de media' zijn grotendeels meetbaar op basis van databases met mediaberichten, zoals Lexis Nexis. Via deze bronnen kan op een relatief snelle manier inzicht gekregen worden in deze indicatoren. Een beperking is echter dat deze databases doorgaans alleen gedrukte media bevatten zoals meer 'traditionele' kranten. Online blogs, nieuwswebsites en videomateriaal worden dan gemist. Er zal verder een afbakening gemaakt moeten worden in de onderwerpen waarop gezocht wordt. Dit kan gedaan worden door een selectiekader op te stellen voor de keywords waarop gezocht wordt in de databases. Dit kan overeen komen met de afbakening voor de variabelen binnen de indicator 'rol van de politiek'. Ook moet rekening gehouden worden met de politieke kleur van de media. Deze indicator is erg relevant omdat deze veel informatie geeft over hoeveel en hoe er in een land gesproken wordt over bescherming van persoonsgegevens. Het is echter alleen haalbaar om dit te achterhalen als er voldoende ruimte is om deze analyse te doen. Het zal een relatief omvangrijke, mogelijk losstaande, analyse zijn binnen het onderzoek. De onderzoekers en opdrachtgevers moeten bepalen of het daarvoor relevant genoeg is.

3.4 Incidenten

Deze indicator draait om de vraag of er incidenten rond de bescherming van persoonsgegevens in een land zijn geweest (zoals datalekken, rechtszaken, economische schade) die verband houden met (eventuele) niet-adequate bescherming en zo ja welke. Dit kunnen zowel grote incidenten zijn als kleinere incidenten met veel impact waarbij persoonsgegevens onvoldoende beschermd waren (bijvoorbeeld op het gebied van informatiebeveiliging). Het plaatsvinden van incidenten geeft mogelijk aan dat de bescherming niet op orde was, maar betekent ook dat het bewustzijn van het belang van bescherming van persoonsgegevens mogelijk vergroot is. In Nederland kunnen deze incidenten bijvoorbeeld zaken zijn die bij de ombudsman terecht zijn gekomen. Een relevante vervolgvraag om te onderzoeken is of dit incidenten zijn of dat er structurele problemen zijn met de bescherming van persoonsgegevens in het desbetreffende land. Een structureel probleem kan bijvoorbeeld blijken uit een opeenvolging van vergelijkbare incidenten.

Tabel 5 Variabelen incidenten

Variabele	**Methode en bronnen**
Zijn er grote incidenten of kleinere incidenten met veel impact in een land geweest waarbij de bescherming van persoonsgegevens niet goed geregeld was? Zo ja, welke? (bijv. datalekken, rechtszaken, economische schade)	Media-analyse (Lexis nexis database), desk research (rapporten, adviezen en jaarverslagen toezichthouder), interviews (toezichthouder)
Wat is er gebeurd in reactie op deze incidenten?	Desk research (rapporten, adviezen en jaarverslagen toezichthouder), interviews (toezichthouder)

Zijn er in een land structurele problemen die spelen rond de bescherming van persoonsgegevens?	Media-analyse (Lexis nexis database), desk research (rapporten, adviezen en jaarverslagen toezichthouder), interviews (toezichthouder)

Conclusie indicator
De eerste twee variabelen van deze indicator zijn goed meetbaar middels een media-analyse of interviews met bijvoorbeeld de toezichthouder(s). Ook kunnen verslagen van de toezichthouder(s) bestudeerd worden om bijvoorbeeld de reactie op incidenten te achterhalen. Een media-analyse hiervoor zou onderdeel kunnen zijn van de analyse in het kader van de indicator 'aandacht in de media'. Omwille van de afbakening kan er ook voor worden gekozen om alleen incidenten te bestuderen die bij de toezichthouder gemeld zijn. In alle gevallen bestaat er een risico van incompleetheid.
Interessant aan deze indicator is dat er internationale incidenten kunnen zijn waar landen verschillend op reageren. Wanneer deze zich voordoen kan per land gekeken worden hoe hiermee om is gegaan en een vergelijking worden gemaakt. Het is ook een optie om te vergelijken tussen landen welke type incidenten gemeld zijn bij de toezichthouder(s) en of dit echt incidenten zijn of structurele problemen lijken te zijn. Informatie hierover zal mogelijk verkrijgbaar zijn in jaarverslagen of andere rapporten van de toezichthouder(s).
De laatste variabele over 'structurele problemen' is relevant om te achterhalen of er sprake is van incidenten of dat er structurele problemen zijn op het gebied van bescherming van persoonsgegevens. Incidenten worden gezien als iets dat eenmalig voor komt en 'toevallig' of 'ongelukkig' is. Een structureel probleem is iets dat vaker is voorgekomen en duidt op fouten in een systeem. Deze informatie kan het beste achterhaald worden op basis van een interview met de toezichthouder of uit hun jaarverslagen gehaald worden. Zij kunnen mogelijk ook een inschatting geven of incidenten structureel zijn of niet. Deze informatie is moeilijker uit een media-analyse af te leiden.

3.5 Rol van burgerrechtenorganisaties

Ook belangrijk voor de situatie rondom bescherming van persoonsgegevens in een land is hoe burgerrechtenorganisaties hun rol en positie zien. Dit zijn organisaties die niet wettelijk zijn opgericht zoals de toezichthouder, maar als burgerbeweging zijn ontstaan en vanuit die positie opkomen voor rechten van burgers. Er zijn in Nederland een aantal burgerrechtenorganisaties actief op het gebied van bescherming van persoonsgegevens, zoals online privacy of privacy in de leefomgeving. Bekende voorbeelden zijn Bits of Freedom, Privacy First en Vrijbit. Zijn zij vooral bezig met optreden tegen inbreuk op privacy van persoonsgegevens of nemen zij nog een andere positie in zoals het faciliteren van debatten, of zoeken zij andere manieren om invloed uit te oefenen?

Tabel 6 Variabelen rol van burgerrechtenorganisaties

Variabele	**Methode en bronnen**
Welke burgerrechtenorganisaties zijn actief in een land en hoe groot is hun achterban?	Desk research (websites burgerrechtenorganisaties,

Variabele	Methode en bronnen
	jaarverslagen en rapporten burgerrechtenorganisaties, overheidswebsites), interviews (selectie van burgerrechtenorganisaties in een land, politici, beleidsmakers)
Wat is de rol van burgerrechtenorganisaties? (bijvoorbeeld protesteren tegen inbreuk op privacy, facilitering debatten)	Desk research (websites burgerrechtenorganisaties, jaarverslagen en rapporten burgerrechtenorganisaties, overheidswebsites), interviews (selectie van burgerrechtenorganisaties in een land, politici, beleidsmakers)
Hebben burgerrechtenorganisaties zichtbare invloed op overheidsbeleid? (Een indicatie zou zijn dat zij geconsulteerd worden in wetgevingsprocessen)	Desk research (websites burgerrechtenorganisaties, jaarverslagen en rapporten burgerrechtenorganisaties, overheidswebsites, beleidsstukken, parlementsverslagen, internetconsultatie.nl), interviews (selectie van burgerrechtenorganisaties in een land, politici, beleidsmakers)
Met welke onderwerpen houden burgerrechtenorganisaties zich bezig binnen het thema bescherming persoonsgegevens?	Desk research (websites burgerrechtenorganisaties, jaarverslagen en rapporten burgerrechtenorganisaties, overheidswebsites), interviews (selectie van burgerrechtenorganisaties in een land, politici, beleidsmakers)
Hoe bekend zijn de burgerrechtenorganisaties bij burgers en bedrijven?	Desk research (websites burgerrechtenorganisaties, jaarverslagen en rapporten burgerrechtenorganisaties, overheidswebsites, bestaande data over bekendheid bij burgers), interviews (selectie van burgerrechtenorganisaties in een land, selectie van bedrijven als deze geïnterviewd worden voor andere onderdelen, politici, beleidsmakers)
Hoeveel klachten krijgen zij binnen en wat voor type klachten zijn dit?	Desk research (websites burgerrechtenorganisaties, jaarverslagen en rapporten burgerrechtenorganisaties, overheidswebsites), interviews (selectie van

Variabele	Methode en bronnen
	burgerrechtenorganisaties in een land)

Conclusie indicator
De variabelen bij deze indicator zijn het beste te meten door interviews te houden met de belangrijkste burgerrechtenorganisaties in de verschillende landen. Er kan afgewogen worden of het relevant genoeg is om hen te spreken, afhankelijk van de omvang van het onderzoek. Aangezien deze organisaties ook een politiek belang hebben zullen hun antwoorden gekleurd zijn. Het is daarom goed om als tegenhanger ook politici of beleidsmakers te vragen naar de rol van burgerrechtenorganisaties. Wanneer zij voor andere onderdelen van het onderzoek geïnterviewd worden kunnen hier vragen over worden opgenomen.
De bekendheid bij burgers en bedrijven is mogelijk het meest lastig om te meten. Als deze informatie bekend is bij de burgerrechtenorganisaties kan deze meegenomen worden in het onderzoek, of dit kan gevraagd worden in een survey of focusgroep met burgers, of in interviews met bedrijven, wanneer deze gedaan zouden worden.

4 Beleid

Binnen dit onderwerp wordt een beeld geschetst van welk beleid er vanuit de nationale overheid gevoerd wordt om persoonsgegevens te beschermen. Daarbij gaat het zowel om beleid dat gericht is op de overheid zelf als beleid dat op andere organisaties en burgers gericht is. Door dit in kaart te brengen wordt het mogelijk om landen te vergelijken op wat zij in beleid doen en hoe streng dit beleid is. Daarbij kan gedacht worden aan overheidscampagnes, begrotingen, de aandacht voor privacy in het onderwijs, etc. Er wordt voor de nationale overheid als onderzoekseenheid gekozen omdat dit het beste vergelijkbaar is tussen landen. Ieder land heeft een nationale overheid, maar lokale overheden zijn verschillend georganiseerd. In de landen waar ook op meer lokaal of regionaal niveau beleid wordt gemaakt op het gebied van privacy kan een uitzondering worden gemaakt en kan dit ook worden meegenomen om te voorkomen dat belangrijke wetgeving over het hoofd wordt gezien.

4.1 Bestaand beleid

De eerste indicator geeft weer welk beleid er is op het gebied van bescherming van persoonsgegevens. Dat beleid kan zowel intern, op de overheid zelf, als extern gericht zijn. Hierin kunnen ook bepaalde vaste onderdelen van beleid vergeleken worden tussen landen, zoals of er beleid is rondom het uitvoeren van Privacy Impact Assessments als vast onderdeel van het wetgevingsproces. Een Privacy Impact Assessment (PIA) is een beoordeling die door organisaties uitgevoerd kan worden om te bepalen of het gebruik van een bepaalde technologie of een nieuwe dienst gevolgen heeft voor de privacy van gebruikers. Het is een controlemechanisme aan de hand waarvan bekeken kan worden of het bedrijf in overeenstemming met de privacyregelgeving handelt (Van Veenstra et al., 2013). In Nederland is een PIA vanuit de overheid een verplicht onderdeel van het integraal afwegingskader bij de totstandkoming van nieuwe wetgeving. Dit kader bevat een aantal stappen die volbracht moeten worden voordat nieuwe wetgeving doorgevoerd kan worden.

Tabel 7 Variabelen bestaand beleid

Variabele	Methode en bronnen
Welk beleid wordt er vanuit de nationale overheid gevoerd om persoonsgegevens van burgers te beschermen?[6]	Desk research (overheidswebsites, beleidsdocumenten, parlementaire verslagen), interviews (beleidsmakers)
Is er vanuit de nationale overheid speciaal beleid voor specifieke sectoren en, zo ja, welk beleid voor welke sector?	Desk research (overheidswebsites, beleidsdocumenten, parlementaire verslagen), interviews (beleidsmakers)

[6] Het gaat zowel om intern beleid gericht op de overheid zelf als extern gericht op andere organisaties en burgers.

Variabele	Methode en bronnen
Is een risicoanalyse en/of een Privacy Impact Assessment (PIA)[7] wettelijk verplicht voor overheidsbeleid dat raakt de aan bescherming van persoonsgegevens en, zo ja, op welk moment moet deze uitgevoerd worden en welke rol heeft het?	Desk research (overheidswebsites, beleidsdocumenten, parlementaire verslagen, website toezichthouder, verslagen toezichthouder), interviews (beleidsmakers, toezichthouder)
Is er een risicoanalyse en/of PIA voorgeschreven voor organisaties (buiten de overheid) en, zo ja, op welk moment moet deze uitgevoerd worden?	Desk research (overheidswebsites, beleidsdocumenten, parlementaire verslagen), interviews (beleidsmakers)

Conclusie indicator
Bij het in kaart brengen van het beleid vanuit de overheid op het gebied van bescherming van persoonsgegevens is het in verband met de meetbaarheid van belang om in de variabele af te bakenen wanneer er in het beleid echt sprake is van bescherming van persoonsgegevens. Een overzicht van bestaand beleid is erg relevant voor dit onderzoek omdat dit het beleidsmatig kader in een land weergeeft. In eerste instantie kan gekeken worden naar algemeen beleid. Vervolgens kan voor een aantal sectoren gekeken worden of er speciaal beleid is op dit gebied. Deze informatie kan verkregen worden op basis van desk research, maar mogelijk ook via interviews met beleidsmakers of de toezichthouder. Ook de vraag of een Privacy Impact Assessment is voorgeschreven voor overheden en bedrijven kan middels deze bronnen beantwoord worden. Het is goed haalbaar om deze informatie te achterhalen, zeker wanneer de interviews en het desk research gebruikt kunnen worden voor het verzamelen van informatie over meerdere indicatoren.

4.2 Beleidsvorming

Bij deze indicator wordt nagegaan in hoeverre er in de vorming van nieuw beleid rekening wordt gehouden met privacy en de bescherming van persoonsgegevens, bijvoorbeeld bij de opkomst van nieuwe ontwikkelingen zoals big data of privacy by design.

Tabel 8 Variabelen beleidsvorming

Variabele	Methode en bronnen
In hoeverre wordt er in beleidsvisies en beleidsdoelen expliciet rekening gehouden met bescherming van persoonsgegevens?	Desk research (kamerbrieven, beleidsdocumenten, kabinetsvisies), interviews (beleidsmakers van verantwoordelijke ministeries, experts op het gebied van

[7] Uit een risicoanalyse kan een Privacy Impact Assessment (PIA) volgen.

Variabele	Methode en bronnen
	bescherming persoonsgegevens)
Welke onderwerpen spelen er in een land die mogelijk consequenties kunnen hebben voor de bescherming van persoonsgegevens en hoe wordt hier in beleid rekening mee gehouden? (Bijvoorbeeld het elektronisch patiëntendossier, regelgeving over cookies, cameratoezicht)	Desk research (kamerbrieven, beleidsdocumenten, kabinetsvisies), interviews (beleidsmakers van verantwoordelijke ministeries, experts op het gebied van bescherming persoonsgegevens)

Conclusie indicator
De variabele 'In hoeverre wordt er in beleidsvisies en beleidsdoelen rekening gehouden met bescherming van persoonsgegevens?' is relevant omdat dit laat zien in hoeverre het vanzelfsprekend is voor een overheid om rekening te houden met de bescherming van persoonsgegevens. Tegelijkertijd is het een moeilijke variabele om te meten omdat het kan gaan om een breed scala aan onderwerpen dat kan raken aan de bescherming van persoonsgegevens. De beleidsvisies en -doelen die echt binnen het gebied van bescherming van persoonsgegevens vallen kunnen buiten beschouwing worden gelaten, aangezien ervanuit kan worden gegaan dat dit hierin meegenomen is. Het gaat dan om onderwerpen die hieraan gerelateerd zijn vanwege de verwerking van persoonsgegevens, zoals zorg, mobiliteit of energie. Ons advies is om een afbakening te maken van een aantal beleidsterreinen en op deze terreinen te onderzoeken of bescherming van persoonsgegevens meegenomen wordt. Bij de keuze voor de beleidsterreinen en onderwerpen voor deze indicator kunnen de resultaten uit de situatieschets als uitgangspunt worden genomen. Daarin wordt onderzocht met welke onderwerpen burgerrechtenorganisaties bezig zijn en welke onderwerpen in de media van een land belicht worden. Er kan ook voor gekozen worden om een aantal onderwerpen te kiezen dat in Nederland speelt en te vergelijken hoe hier in andere landen in beleid rekening mee wordt gehouden.

4.3 Rol van de overheid in het maatschappelijk debat

Deze indicator gaat over de rol die de centrale overheid[8] speelt in het maatschappelijk debat over bescherming van persoonsgegevens. Hierbij kan gedacht worden aan de manier waarop nieuw beleid of wet- en regelgeving wordt gepresenteerd, de boodschap die de overheid uitdraagt in de media, of er bijvoorbeeld internetconsultaties onder burgers worden gedaan bij nieuwe wetgeving en of men in gesprek gaat met belangenorganisaties. Relevant is of een overheid meer proactief of reactief deelneemt aan het maatschappelijk debat. Wanneer zij proactief is draagt zij een visie uit, neemt zij deel aan debatten en congressen. Wanneer zij reactief is zal zij vooral reageren wanneer er iets aan de hand is.

[8] Onder de centrale overheid verstaan wij hier: de regering, het staatshoofd, de ministeries, de rechterlijke macht, de Hoge Colleges van Staat, adviescolleges en zelfstandige bestuursorganen.

Tabel 9 Variabelen rol van de overheid

Variabele	Methode en bronnen
Neemt de overheid proactief of reactief deel aan het maatschappelijk debat over de bescherming van persoonsgegevens?	Interviews (beleidsmakers van verantwoordelijke ministeries, experts op het gebied van bescherming), desk research (bijdragen van beleidsmakers aan congressen en debatten, participatie in online discussies)
Voert de overheid gesprekken met belangenorganisaties en burgerrechtenorganisaties die de bescherming van persoonsgegevens adresseren?	Interviews (beleidsmakers van verantwoordelijke ministeries, burgerrechtenorganisaties, belangenorganisaties)
Wat doet de overheid om de mening van burgers en bedrijven mee te nemen in haar vorming van beleid, wet- en regelgeving? (Bijvoorbeeld internetconsultaties)	Interviews (beleidsmakers van verantwoordelijke ministeries, experts op het gebied van bescherming), desk research (internetconsultaties)

Conclusie indicator
De eerste variabele over de rol van de overheid in het maatschappelijk debat is niet gemakkelijk te meten maar het is wel een relevante indicator. Daarvoor is in ieder geval een definitie van proactiviteit en reactiviteit nodig. In de introductie van deze paragraaf is een begin gemaakt met een definitie van proactiviteit en reactiviteit die door de onderzoekers uitgewerkt kan worden. Ook moet worden afgebakend wat het ‘maatschappelijk debat’ is en waar dit gevoerd wordt. Hiervoor kan bijvoorbeeld bekeken worden in hoeverre beleidsmakers aanwezig zijn bij congressen en debatten over het onderwerp. Deze vraag kan middels desk research onderzocht worden door prominente congressen en debatten op te zoeken en na te gaan of er een rol van de overheid was in het programma. Deze vraag kan ook in interviews met beleidsmakers, toezichthouders, belangenorganisaties, burgerrechtenorganisaties of andere experts op het gebied van bescherming van persoonsgegevens verkend worden. De onderzoekers kunnen beoordelen of deze variabele in het totaalonderzoek relevant genoeg is. Zo ja dan kan verder onderzocht worden hoe deze meetbaar gemaakt kan worden.
De vraag wat de overheid doet om de mening van burgers en bedrijven mee te nemen in haar beleid is goed meetbaar via een combinatie van desk research en interviews.
De variabele ‘Voert de overheid gesprekken met belangenorganisaties en burgerrechtenorganisaties die de bescherming van persoonsgegevens kunnen adresseren?’ is te meten door interviews te houden met betrokkenen vanuit de overheid en/of belangenorganisaties, maar zal moeilijk meetbaar zijn op basis van desk research.

4.4 Voorlichting door de overheid

Een voorwaarde dat burgers en organisaties zorgvuldig kunnen omgaan met persoonsgegevens is dat zij hier goede voorlichting over krijgen, onder andere vanuit de overheid. Het gaat er bijvoorbeeld om dat mensen weten wat er kan

gebeuren met hun gegevens en hoe zij hun gegevens kunnen beschermen (o.a. welke rechten zij hebben).

Tabel 10 Variabelen voorlichting door de overheid

Variabele	Methode en bronnen
In hoeverre doet de overheid aan informatievoorziening voor burgers over persoonsgegevens en de bescherming daarvan?	Desk research (overheidswebsites, voorlichtingswebsites, website toezichthouder(s)), interviews (beleidsmakers van verantwoordelijke ministeries, toezichthouder(s), burgerrechtenorganisaties, experts op het gebied van bescherming persoonsgegevens)
In hoeverre doet de overheid aan informatievoorziening voor organisaties over persoonsgegevens en de bescherming daarvan?	Desk research (overheidswebsites, voorlichtingswebsites, website toezichthouder(s)), interviews (beleidsmakers van verantwoordelijke ministeries, toezichthouder(s), belangenorganisaties, experts op het gebied van bescherming persoonsgegevens)
In hoeverre faciliteert de overheid voorlichting door andere partijen? (Bijvoorbeeld door subsidies uit te geven voor voorlichting door andere partijen)	Desk research (overheidswebsites, voorlichtingswebsites, website toezichthouder(s)), interviews (beleidsmakers van verantwoordelijke ministeries, toezichthouder(s), belangenorganisaties, experts op het gebied van bescherming persoonsgegevens)

Conclusie indicator
De informatievoorziening door de overheid over bescherming van persoonsgegevens voor burgers en organisaties is goed meetbaar via desk research op overheidswebsites of interviews met beleidsmakers, toezichthouders, belangenorganisaties en experts op het gebied van de bescherming van persoonsgegevens van bijvoorbeeld universiteiten. Deze indicator is relevant omdat de voorlichting die wel of niet gegeven wordt een indicatie is voor het belang dat een overheid hecht aan de bescherming van persoonsgegevens.

5 Wet- en regelgeving

Binnen het onderwerp wet- en regelgeving kan bestudeerd worden welke wet- en regelgeving in een land van toepassing is. Vervolgens kan bekeken worden hoe deze wordt uitgevoerd en functioneert in de praktijk. Landen kunnen verschillende (soorten) wetgeving hanteren en daarnaast kunnen er nuanceverschillen bestaan tussen landen in hoe zij invulling geven aan Europese regelgeving, zoals welke bewaartermijnen worden gehanteerd voor persoonsgegevens of welke beperkingen er zijn rond gebruik van gegevens. Zo zijn er verschillen in de implementatie van het toestemmingsvereiste voor het plaatsen van cookies, waarbij Nederland aanvankelijk de strengste vorm had geïmplementeerd terwijl andere landen minder zware vereisten stelden (Van Veenstra et al., 2013).

5.1 Wetten met impact op bescherming persoonsgegevens

Deze indicator geeft aan welke formele wetten en regels er zijn die impact hebben op de bescherming van persoonsgegevens in een land. Dit kan zowel gaan om wetten die persoonsgegevens beschermen als om wetten die de bescherming van persoonsgegevens beperken.

De belangrijkste wetten met impact op het gebied van bescherming van persoonsgegevens in Nederland zijn:

- Wet bescherming persoonsgegevens: implementatie van de EU Data Protection Directive (DPD)
- Wet politiegegevens
- Wet justitiële en strafvorderlijke gegevens
- Telecommunicatiewet: hierin zijn wijzigingen aangebracht op basis van de EU ePrivacy Directive. Hieronder valt ook de zogenaamde ‘cookiewet’, die als doel heeft de gebruiker/internetter controle te geven over de cookies of andere technologieën die op zijn of haar apparatuur worden geplaatst of gelezen

Veel van deze wetten vormen een implementatie van Europese regelgeving. Er kan tussen de landen vergeleken worden hoe deze regelgeving op nationaal niveau geïmplementeerd is om te zien in hoeverre de landen verschillende benaderingen hanteren in deze wetten en dus op een andere manier omgaan met de bescherming van persoonsgegevens. In sommige gevallen, bijvoorbeeld in het Verenigd Koninkrijk, kan de wetssystematiek anders zijn dan in Nederland. Dit dient dan meegenomen te worden.

Tabel 11 Variabelen wetten

Variabele	Methode en bronnen
Welke wetten zijn er in een land die positieve of negatieve impact hebben op de bescherming van persoonsgegevens?	Desk research (overheidswebsites, kamerbrieven, parlementaire verslagen, website en verslagen

Variabele	**Methode en bronnen**
	toezichthouder), interviews (beleidsmakers, toezichthouder(s), experts op het gebied van wetgeving rond bescherming persoonsgegevens)
Hoe worden privacybelangen afgewogen in wetten die niet gericht zijn op bescherming persoonsgegevens, maar daar wel invloed op hebben?	Desk research (overheidswebsites, kamerbrieven, parlementaire verslagen, website en verslagen toezichthouder), interviews (beleidsmakers, toezichthouder(s), experts op het gebied van wetgeving rond bescherming persoonsgegevens)
Hoe streng is Europese wetgeving op het gebied van bescherming van persoonsgegevens in een land geïmplementeerd? (Data Protection Directive, ePrivacy Directive) Zijn er nog aanvullende wetten of plichten bovenop het minimum vereiste uit de Richtlijnen?	Desk research (overheidswebsites, kamerbrieven, parlementaire verslagen, website en verslagen toezichthouder), interviews (beleidsmakers, toezichthouder, experts op het gebied van wetgeving rond bescherming persoonsgegevens)
Welke rechten of plichten worden door deze wetten vastgesteld? Bijvoorbeeld: • Welke bewaartermijnen en verwerkingstermijnen worden gehanteerd? • Welke beperkingen rond gebruik zijn er? • Welke verwerkingsgronden en andere waarborgen worden gehanteerd? • Welke gegevens mogen worden uitgewisseld met derden? • Welke gegevens mogen worden hergebruikt? • Is er een geheimhoudingsplicht en waarvoor geldt deze? • Hoe wordt de meldplicht datalekken geïmplementeerd? • Welke regels gelden rondom opslag van gegevens? • Hoe is de wetgeving omtrent cookies geïmplementeerd? • In hoeverre is er sprake van netneutraliteit?	Desk research (overheidswebsites, kamerbrieven, parlementaire verslagen, website en verslagen toezichthouder), interviews (beleidsmakers, toezichthouder, experts op het gebied van wetgeving rond bescherming persoonsgegevens)

Variabele	Methode en bronnen
Hoe functioneren de wetten in de praktijk? Zijn ze duidelijk genoeg en worden ze nageleefd?	Desk research (jaarverslagen en rapporten toezichthouders, wetgevingsadviezen), jurisprudentie, interviews (beleidsmakers, toezichthouder, experts op het gebied van wetgeving rond bescherming persoonsgegevens)
Bestaat er veel sectorale wetgeving op het gebied van bescherming van persoonsgegevens in een land en zo ja, wat betekent dit? (is deze bijvoorbeeld anders geregeld in verschillende sectoren[9], zoals de telecomsector of de zorgsector?) Om welke wetten gaat het?	Interviews (beleidsmakers, toezichthouder, experts op het gebied van wetgeving rond bescherming persoonsgegevens)
Is sectorale wetgeving vaak gericht op de verwerking van bijzondere persoonsgegevens? Worden hier dan meer bevoegdheden of meer eisen vastgesteld?	Interviews (beleidsmakers, toezichthouder, experts op het gebied van wetgeving rond bescherming persoonsgegevens)
Is er sprake van spanningen tussen wetten in een land? (In Nederland kan het bijvoorbeeld sterk verschillen welke wetgeving van toepassing is afhankelijk van waar informatie opgeslagen is)	Interviews (beleidsmakers, toezichthouder, experts op het gebied van wetgeving rond bescherming persoonsgegevens)

Conclusie indicator

Met het in kaart brengen van de relevante wetten per land wordt een eerste overzicht verkregen. Het vergelijken van de concrete implementaties van Europese regelgeving kan goede inzichten opleveren en is daarom een waardevolle exercitie. Interviews met beleidsmakers, toezichthouders en andere experts op het gebied van wetgeving rond bescherming van persoonsgegevens kunnen aanvullende informatie geven over het functioneren van wetten. Een volledige procesevaluatie op het functioneren van wetten in de praktijk is vermoedelijk te omvangrijk als onderdeel van de benchmark. Daarom kan het verstandig zijn om het te beperken tot het verkrijgen van informatie op basis van interviews met experts en bestaande evaluaties en rapporten. Ook het in kaart brengen van de sectorale wetgeving is waardevol, omdat daarin vaak nuances optreden en specifieke verschillen kunnen optreden. Het verkrijgen van inzicht in de mate van bescherming van persoonsgegevens door deze sectorale wetten vereist dat deze wetten ook tot op zekere hoogte worden geanalyseerd. Op algemeen niveau kan via interviews met de eerder genoemde experts achterhaald worden of sectorale wetgeving tot meer of juist minder bescherming van persoonsgegevens leidt.
Via interviews kunnen ook inzichten verkregen worden in eventuele spanningen tussen verschillende wetten. Het verkrijgen van een volledig overzicht kan echter

[9] Sectorale wetgeving kan in Nederland ook gekoppeld zijn aan beleid van ZBO's. Het beleid wordt dan opgesteld en uitgevoerd door de ZBO's en niet door de centrale overheid. Voor de vergelijking met andere landen moet onderzocht worden of daar ZBO's actief zijn.

lastig zijn, omdat sectorale wetgeving vanwege het domein gebonden karakter vaak niet geheel door één expert wordt overzien. Opvallende spanningen kunnen dus mogelijk in kaart gebracht worden en vergeleken worden tussen landen, maar er is een vrij groot risico dat het beeld dat zo verkregen wordt incompleet is. Hier adviseren we de onderzoekers dus om opvallende zaken op te nemen, maar geen concrete vergelijking tussen landen te doen.

5.2 Regulering vanuit de overheid

Regulering valt onder beleid dat vanuit de overheid wordt gemaakt op persoonsgegevens te beschermen. Hier valt ook wetgeving onder. Bij de indicator 'regulering vanuit de overheid' is aandacht voor andere vormen van regulering dan regulier beleid of wetgeving. Wanneer alleen gekeken wordt naar beleid en wetgeving mist er een aantal manieren waarop vanuit de overheid op een alternatieve manier invloed kan worden uitgeoefend op de bescherming van persoonsgegevens. De overheid kan bijvoorbeeld de ontwikkeling van zelfregulering door brancheorganisaties aanmoedigen. Van zelfregulering is sprake op de terreinen waar meer vrijheid wordt gegeven door de overheid. Indien de overheid zelfregulering steunt of aanmoedigt kan dit een aanwijzing zijn dat bedrijven zelf actief met bescherming van persoonsgegevens bezig zijn, waardoor de overheid zich terughoudender opstelt. Het kan ook te maken hebben met de cultuur in een land, in sommige landen is zelfregulering meer gangbaar dan in andere landen.

Tabel 12 Variabelen regulering vanuit de overheid

Variabele	Methode en bronnen
Hoe wordt bescherming van persoonsgegevens door organisaties gereguleerd door de overheid?	Desk research (overheidswebsites, rapporten toezichthouder), interviews (beleidsmakers, toezichthouder, selectie van organisaties, belangenorganisaties, experts op het gebied van wetgeving rond bescherming persoonsgegevens)
Wordt zelfregulering door het bedrijfsleven op het gebied van bescherming van persoonsgegevens aangemoedigd door de overheid of niet? Zo ja, op welke manier(en)?	Desk research (overheidswebsites, rapporten toezichthouder), interviews (beleidsmakers, toezichthouder, selectie van organisaties, belangenorganisaties, experts op het gebied van wetgeving rond bescherming persoonsgegevens)

Conclusie indicator

Voor deze indicator is het voor de meetbaarheid van belang dat er duidelijk wordt bepaald wanneer er sprake is van beleid of wetgeving en wanneer er sprake is van andere vormen van regulering. Zelfregulering door het bedrijfsleven is hier een voorbeeld van. Daarbij wordt de regulering van bepaalde aspecten van bescherming van persoonsgegevens aan bedrijven overgelaten. Binnen dit kader kan dan middels desk research van overheidswebsites en/of rapporten van de toezichthouder en interviews met partijen zoals beleidsmakers, de toezichthouder en een selectie van organisaties achterhaald worden welke regulering er is.

6 Implementatie

Dit hoofdstuk bevat indicatoren die inzicht geven in hoe organisaties in de praktijk vorm geven aan de implementatie van beleid en regelgeving. Het gaat dus om de invulling in de praktijk binnen organisaties. Wat doen organisaties om persoonsgegevens te beschermen? Stellen zij bijvoorbeeld een privacy officer aan en welke rol heeft deze? Welke andere technische en organisatorische maatregelen nemen zij? Op welke wijze dragen zij bij aan transparantie richting burgers of consumenten? Met deze vragen wordt een antwoord verkregen op de vraag hoe de bescherming van persoonsgegevens geborgd is in de praktijk van organisaties.

6.1 Zelfregulering/gedragscodes

Sommige onderdelen van de bescherming van persoonsgegevens worden door de overheid en haar wetgeving overgelaten aan organisaties zelf. Zij krijgen op sommige gebieden ruimte voor ‘zelfregulering’. De reden hiervoor is dat zij soms zelf het beste kunnen inschatten wat zij kunnen doen en hoe kan worden tegemoetgekomen aan de behoeften in een branche en onderling tot standaard afspraken kunnen komen over een zorgvuldige omgang met persoonsgegevens. Dit kan ook wel ‘co-regulering’ genoemd worden: de overheid zet het kader neer in een wet en dit kan nader worden ingevuld door bedrijven. Een nadeel hiervan is dat er wel toezicht moet zijn vanuit de overheid, de branche of de organisaties zelf omdat persoonsgegevens anders mogelijk niet goed beschermd worden, bijvoorbeeld wanneer bedrijfsbelang boven het belang van privacy gaat.
Een voorbeeld van zelfregulering is dat organisaties een gedragscode[10] vaststellen. Zij spreken bijvoorbeeld op het gebied van internetreclame af hoe zij zich zullen gedragen. Een brancheorganisatie kan hier het voortouw in nemen. Een kritiekpunt op zelfregulering in tegenstelling tot officiële regulering kan zijn dat het ook een manier kan zijn van de overheid om organisaties buiten de overheid aansprakelijk te laten zijn voor de bescherming van persoonsgegevens in plaats van zij zelf. Bedrijven kunnen op hun beurt zelfregulering gebruiken om aansprakelijkheden af te wimpelen en om bevoegdheden voor gebruik van persoonsgegevens te creëren. Om deze reden is vaak sprake van geconditioneerde zelfregulering, waarbij de overheid zelf enkel kaders schetst waarbinnen zelfregulering mogelijk is (Dorbeck-Jung 2006, p. 13). Het is dus van belang om te kijken hoe effectief zelfregulering is en of hier goed toezicht op gehouden wordt.

Tabel 13 Variabelen zelfregulering/gedragscodes

Variabele	Methode en bronnen
Op welke manier (anders dan informatiebeveiliging) beschermen organisaties de persoonsgegevens waar zij mee werken? Wordt intern beleid bijvoorbeeld aangesloten op standaarden (ISO standaarden, Richtsnoeren van het Cbp)/de toezichthouder?	Desk research (bestaand onderzoek, rapporten toezichthouder), Interviews (toezichthouder, belangenorganisaties, brancheorganisaties, selectie

[10] Op grond van hoofdstuk V van de Richtlijn Bescherming Persoonsgegevens.

Variabele	Methode en bronnen
	van organisaties, experts op het gebied van bescherming persoonsgegevens)
Vindt er zelfregulering door organisaties plaats en zo ja op welke manier?	Desk research (rapporten toezichthouder, beleidsstukken), Interviews (toezichthouder, belangenorganisaties, brancheorganisaties, selectie van organisaties, experts op het gebied van bescherming persoonsgegevens)
Hoeveel gebruik wordt er gemaakt van gedragscodes? In welke branches? Worden deze gedragscodes voorgelegd aan de toezichthouder?	Desk research (rapporten toezichthouder), Interviews (toezichthouder, belangenorganisaties, brancheorganisaties, selectie van organisaties, beleidsmakers experts op het gebied van bescherming persoonsgegevens)
Hoe vindt de handhaving van gedragscodes plaats? (Is er bijvoorbeeld onafhankelijk toezicht zoals een onafhankelijke geschillencommissie)	Desk research (rapporten toezichthouder), Interviews (toezichthouder, belangenorganisaties, brancheorganisaties, selectie van organisaties, beleidsmakers, experts op het gebied van bescherming persoonsgegevens)

Conclusie indicator
De informatie over zelfregulering door organisaties (zowel bedrijven als overheid) kan deels verkregen worden middels desk research en via interviews met de toezichthouder, belangenorganisaties, beleidsmakers en/of een selectie van organisaties. Veel initiatieven komen vanuit brancheorganisaties (zoals in Nederland VNO NCW). Een hoge mate van zelfregulering kan betekenen dat de overheid zelf minder actief is op het gebied van bescherming van persoonsgegevens aangezien zij dan veel aan ‘de markt’ overlaat. De bescherming hoeft in dat geval niet per sé minder goed te zijn, maar de rol van de overheid is wel anders dan wanneer een overheid meer zelf in de hand houdt. In beide gevallen is de uiteindelijke bescherming van persoonsgegevens afhankelijk van het toezicht en de handhaving die plaatsvinden.

6.2 Invulling rol privacy officer

Het hangt van regelgeving in een land af of organisaties verplicht zijn om een privacy officer aan te stellen of niet. De privacy officer is een functie waar binnen een organisatie (overheid of bedrijfsleven) de verantwoordelijkheid ligt voor de

naleving van wetgeving en (intern) beleid op het gebied van bescherming persoonsgegevens. Hoe groot de rol van een privacy officer is (fulltime of parttime) geeft aan hoeveel autoriteit en onafhankelijkheid deze heeft. Wanneer het een rol is die iemand vervult naast reguliere andere werkzaamheden is het risico op ondersneeuwen groot. Tevens kunnen dan verschillende interne belangen conflicteren. Wanneer de privacy officer doorzettingsmacht heeft en daadwerkelijk processen stil kan leggen en deze functie fulltime en onafhankelijk bekleed is, is de invloed naar verwachting veel sterker.

Tabel 14 Variabelen invulling rol privacy officer

Variabele	**Methode en bronnen**
Hoeveel organisaties (zowel overheid als bedrijfsleven) hebben een privacy officer? (bijvoorbeeld een percentage van de grote organisaties)	Desk research (rapporten toezichthouder(s), register functionarissen gegevensbescherming[11]), interviews (toezichthouder, belangenorganisaties, experts op het gebied van bescherming persoonsgegevens)
Hoe wordt de functie van privacy officer doorgaans ingevuld in een land? • De rol (is het bij de meeste organisaties een echte functie of iets wat iemand erbij doet?) • Bevoegdheden • Onafhankelijkheid • Activiteiten	Desk research (rapporten toezichthouder(s), register functionarissen gegevensbescherming), interviews (toezichthouder, belangenorganisaties, experts op het gebied van bescherming persoonsgegevens, privacy officers)

Conclusie indicator
Informatie over de functie van een privacy officer is te achterhalen via het register functionarissen gegevensbescherming en via interviews met enkele organisaties. Mogelijk is er informatie beschikbaar op basis van eerder uitgevoerde surveys bij organisaties over hoe zij persoonsgegevens beschermen die zij verwerken. De functie van een privacy officer (of deze er is en hoe die wordt ingevuld) zegt iets over hoe serieus een overheid en bedrijven in een land de bescherming van persoonsgegevens nemen. Wanneer er in het kader van andere indicatoren interviews gehouden worden met enkele organisaties is het goed haalbaar om ook informatie over het bestaan en de invulling van de functie van privacy officer bij hen te achterhalen. Deze vraag is ook via een survey te beantwoorden, maar mogelijk niet relevant genoeg om er een aparte survey voor uit te zetten.

[11] Uit het register functionarissen gegevensbescherming kan alleen informatie gehaald worden wanneer registratie een plicht is in een land. Er kunnen ook privacy officers zijn officieel security officers zijn, dus hanteer een niet te specifieke focus op de term privacy officer.

6.3 Algemeen technische en organisatorische maatregelen

Deze indicator geeft inzicht in de vraag of organisaties zoals aanbieders van diensten waarbij informatie wordt verwerkt passende technische en organisatorische maatregelen treffen ten behoeve van het beschermen van persoonsgegevens van hun klanten. Een voorbeeld is of organisaties in de telecommunicatie de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten goed op orde hebben. Informatie hierover kan onder andere verkregen worden door te kijken naar de mate waarin organisaties zicht hebben op hoe zij deze bescherming op orde hebben, hoe zij dit doen en of zij gebruik maken van principes als Privacy by Design waarbij in de ontwerpfase van een product al rekening wordt gehouden met bescherming van persoonsgegevens. Aanvullend kan onderzocht worden of het ook voor gebruikers inzichtelijk is hoe organisaties hun persoonsgegevens verwerken.

Tabel 15 Variabelen algemeen technische en organisatorische maatregelen

Variabele	Methode en bronnen
In hoeverre hebben organisaties zicht op hoe zij de bescherming van persoonsgegevens op orde hebben?	Desk research (bestaand onderzoek, rapporten toezichthouder(s), rapporten belangenorganisaties), interviews (toezichthouder, belangenorganisaties, selectie van organisaties, experts op het gebied van bescherming persoonsgegevens)
In hoeverre wordt gewerkt vanuit het principe van Privacy by Design?	Interviews (toezichthouder, belangenorganisaties, selectie van organisaties, experts op het gebied van bescherming persoonsgegevens)
Is het inzichtelijk voor gebruikers hoe organisaties persoonsgegevens (verder) verwerken?	Desk research (transparency reports van organisaties, bestaand onderzoek o.a. onder burgers, rapporten toezichthouder(s), rapporten belangenorganisaties), interviews (burgers, toezichthouder, belangenorganisaties, selectie van organisaties, experts op het gebied van bescherming persoonsgegevens)
Hoe beveiligen organisaties persoonsgegevens die ze verwerken? (Bijvoorbeeld via standaard ISO certificeringen of gedragscodes)	Desk research (rapporten toezichthouder(s), rapporten belangenorganisaties), interviews (toezichthouder, belangenorganisaties, selectie van organisaties, experts op het

	gebied van bescherming persoonsgegevens)

Conclusie indicator
De algemene technische en organisatorische maatregelen die organisaties treffen zijn mogelijk moeilijk meetbaar omdat deze informatie gevoelig kan zijn. Ook het inzicht bij organisaties in de manier waarop zij bescherming van persoonsgegevens op orde hebben is erg lastig te meten. Een oplossing kan zijn om bestaande surveys te zoeken waarin anoniem onderzoek is gedaan naar de manier waarop organisaties de gegevens die zij verwerken beschermen. Daarnaast kan het zijn dat de toezichthouder hier informatie over heeft, die via hun verslagen of middels een interview verkregen kan worden. Ook experts op het gebied van de bescherming van persoonsgegevens in een land kunnen hier informatie over hebben.

6.4 Transparantie door organisaties

Landen kunnen verschillen in de mate van transparantie die organisaties (zowel overheid als bedrijfsleven) tonen ten aanzien van welke data zij verwerken en wat zij hier mee doen. In Europese landen gelden op grond van de DPD informatieverplichtingen rondom de verwerking van persoonsgegevens door organisaties. Deze informatie wordt vaak weergegeven in privacy policies die gebruikers van een dienst kunnen lezen voordat zij de dienst gaan gebruiken. Wanneer organisaties transparant zijn over hun dataverwerkingspraktijken kunnen burgers of consumenten beter inschatten hoe en hoe goed hun persoonsgegevens beschermd worden. Meer transparantie betekent niet automatisch dat gegevens beter beschermd worden in een land. Verplichtingen rond transparantie kunnen echter wel leiden tot betere bescherming doordat organisaties mogelijk hun praktijken aanpassen aan wat ze denken dat gebruikers zullen accepteren. Daarnaast staat of valt de effectiviteit van transparantie met het daadwerkelijk lezen van de privacy policies door gebruikers.

Tabel 16 Variabelen transparantie door organisaties

Variabele	Methode en bronnen
In hoeverre lezen burgers/consumenten de privacy policies van de diensten die ze gebruiken?	Desk research (bestaand onderzoek), survey (nieuw opzetten en verschillende vragen beantwoorden), focusgroepen (representatie van burgers uit een land)
Hoe duidelijk vinden burgers/consumenten privacy policies van de diensten die ze gebruiken over wat er met hun gegevens gedaan wordt?	Desk research (bestaand onderzoek), survey (nieuw opzetten en verschillende vragen beantwoorden), focusgroepen (representatie van burgers uit een land)
Op welke manieren zijn organisaties transparant over welke persoonsgegevens zij registreren en wat zij hiermee doen?	Analyse van privacy policies (selectie van organisaties), interviews (toezichthouder,

	burgerrechtenorganisaties, belangenorganisaties, selectie van organisaties)

Conclusie indicator
Informatie over transparantie en de manier waarop consumenten dit ervaren kan deels verkregen worden uit bestaande surveys waarvan onze inschatting is dat die er in veel landen regelmatig zullen zijn, of kan opgenomen worden in een nieuwe survey onder burgers waarin ook vragen opgenomen worden over voornoemde indicatoren. Meer algemene informatie over hoe transparant organisaties zijn zonder de mening van consumenten te vragen kan ook verkregen worden middels interviews met bijvoorbeeld de toezichthouder, burgerrechtenorganisaties of organisaties zelf. Deze indicator behoort niet tot de kern van het onderzoek dus kan achterwege worden gelaten indien informatie moeilijk te verkrijgen is.

7 Toezicht en handhaving

Dit onderwerp behandelt de bescherming van persoonsgegevens en handhaving door de toezichthouder. Een toezichthouder is een onafhankelijk orgaan dat belast is met het toezicht op de naleving van de wetgeving. Toezicht in deze context is het verzamelen van informatie over de vraag of bij een zaak voldaan is aan de gestelde eisen voor bescherming van persoonsgegevens, het vormen van een oordeel daarover en eventueel interveniëren. Op grond van de Richtlijn Bescherming Persoonsgegevens is iedere EU lidstaat verplicht om een toezichthouder te hebben op het gebied van bescherming persoonsgegevens. In Nederland is dit het College Bescherming Persoonsgegevens (CBP) in het algemeen en de Autoriteit Consument en Markt (ACM) voor de telecomsector. Maar in ieder land kunnen verschillende soorten toezichthouders bestaan met verschillende rollen, bevoegdheden en activiteiten. De manier waarop deze functie ingevuld wordt en hoe er daadwerkelijk gehandhaafd wordt geeft een indicatie over de manier waarop een land de persoonsgegevens van haar burgers beschermt.

In dit hoofdstuk wordt 'toezichthouder' in enkelvoud gebruikt in de variabelen, maar in de praktijk kunnen er meerdere toezichthouders in een land zijn waarvoor de vragen apart beantwoord zullen moeten worden.

7.1 Algemene kenmerken van de toezichthouder

Allereerst zijn er algemene variabelen die iets zeggen over het functioneren van de toezichthouder(s), zoals welke toezichthouders er zijn en op welke doelgroepen en domeinen deze zich richten. Er kunnen verschillende toezichthouders bestaan voor verschillende doelgroepen en domeinen. Ook de omvang van de toezichthouder in fte's en het beschikbare budget kan verschillen. Hierbij moet rekening worden gehouden met de grootte van een land en het aantal inwoners.

Tabel 17 Variabelen algemene kenmerken van de toezichthouder

Variabele	Methode en bronnen
Welke toezichthouder(s) is/zijn er in een land?[12]	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (beleidsmakers, toezichthouders, experts op het gebied van bescherming persoonsgegevens)
Op welke doelgroepen is het toezicht en de handhaving door de toezichthouders gericht? Heeft de toezichthouder bijvoorbeeld speerpunten vastgelegd (bijvoorbeeld toezicht en handhaving gericht op app aanbieders of een bepaalde	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (beleidsmakers,

[12] Deze vragen zijn voor de leesbaarheid in enkelvoud geformuleerd, maar moeten in meervoud gesteld worden in het geval er meerdere toezichthouders aanwezig zijn in een land.

Variabele	Methode en bronnen
sector)?	toezichthouders, experts op het gebied van bescherming persoonsgegevens)
Over welke domeinen houden de toezichthouders toezicht?	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (beleidsmakers, toezichthouders, experts op het gebied van bescherming persoonsgegevens)
Wat is de omvang in fte en budget van de toezichthouder in relatie tot de omvang van een land qua inwoners en de sector waarin deze opereert?[13]	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (beleidsmakers, toezichthouders, experts op het gebied van bescherming persoonsgegevens)

Conclusie indicator
De variabelen die onder deze indicator vallen zullen in de meeste landen goed te meten zijn via onder andere het bestuderen van de websites en verslagen van toezichthouders, en het houden van interviews met hen, beleidsmakers en experts.

7.2 Rolinvulling van de toezichthouder

Hoewel de aanwezigheid van een toezichthouder dus verplicht is, kan de invulling van de functie van toezichthouder en de rol die zij voor zichzelf zien verschillen. De primaire taak van de toezichthouder is om toe te zien op de juiste naleving van de regelgeving op het gebied van bescherming van persoonsgegevens en indien nodig handhavend op te treden. Een toezichthouder kan die taak echter op verschillende wijzen invulling geven, bijvoorbeeld door veel voorlichting te geven, actief organisaties te adviseren bij technologische ontwikkelingen, of door alleen strikt te handhaven. De invulling van de rol is voorbehouden aan de toezichthouder zelf. Hoewel de overheid hier dus niet bepalend is, is er uiteraard wel een samenspel tussen de toezichthouder en de regelgeving en het beleid vanuit de overheid. Omdat de rolopvatting van de toezichthouder ook sterk beeldbepalend kan zijn voor hoe binnen een land naar gegevensbescherming wordt gekeken, hebben we dit onderwerp wel opgenomen in deze studie.
De bevoegdheden van de toezichthouder geven aan hoeveel invloed deze heeft. Dit kan per land verschillen. Wanneer een toezichthouder meer bevoegdheden heeft, en deze ook daadwerkelijk gebruikt in handhavend optreden (zie ook 7.3), is de kans groot dat er in een land serieuzere aandacht wordt besteedt aan de bescherming van persoonsgegevens dan wanneer deze beperkt zijn. Bij bevoegdheden kan gedacht worden aan het geven van boetes (bijvoorbeeld aan

[13] Hoeveel budget per bepaald aantal inwoners, hoeveel tijd (fte) per bepaald aantal inwoners. Is nader te bepalen door de onderzoekers.

organisaties die regels rondom de bescherming van persoonsgegevens overtreden), administratieve sancties, etc.

Tabel 18 Variabelen rolinvulling van de toezichthouder

Variabele	**Methode en bronnen**
Welke rol of rollen vervult de toezichthouder? (bijv. voorlichter/handhaver/combinatie)	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (toezichthouders, beleidsmakers, experts op het gebied van bescherming persoonsgegevens)
Wat zijn de belangrijkste activiteiten van de toezichthouder en in welke verhouding? Zijn er bepaalde activiteiten geprioriteerd? (bijv. klachten afhandelen, voorlichten)	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (toezichthouders, beleidsmakers, experts op het gebied van bescherming persoonsgegevens)
Doet de toezichthouder aan voorlichting, wat dan en voor wie?	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (toezichthouders, beleidsmakers, experts op het gebied van bescherming persoonsgegevens)
Overlegt de toezichthouder op regelmatige basis met marktpartijen?[14]	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (toezichthouders, beleidsmakers, belangenorganisaties, selectie van organisaties, experts op het gebied van bescherming persoonsgegevens)
Op basis waarvan maakt de toezichthouder de beslissing om actie te ondernemen? (bijvoorbeeld wanneer er een bepaald aantal klachten binnenkomt, of vanwege een focus op bepaalde onderwerpen)[15]	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (toezichthouders, beleidsmakers, experts op het

[14] Het is aan de onderzoekers om in te vullen wat op regelmatige basis is. Dit kan ééns per jaar zijn of vaker. Het kan gaan om overleg met individuele partijen of met een groep marktpartijen of brancheorganisaties.
[15] Soms zijn toezichthouders verplicht om te acteren in bepaalde situaties.

Variabele	Methode en bronnen
	gebied van bescherming persoonsgegevens)
Adviseert de toezichthouder ook bij wetgeving? En hoe wordt door de overheid met adviezen omgegaan?	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (toezichthouders, beleidsmakers, experts op het gebied van bescherming persoonsgegevens)
Op welke manier kan een burger steun vragen en krijgen van de toezichthouders?	Desk research (websites(s) en rapporten van toezichthouder(s), overheidswebsites), interviews (toezichthouders, beleidsmakers, burgerrechtenorganisaties, experts op het gebied van bescherming persoonsgegevens)
Welke bevoegdheden heeft de toezichthouder? (bijvoorbeeld boetes opleggen, administratieve sancties toepassen, e.d.)	Desk research (website en rapporten toezichthouder, overheidswebsites, wetten, beleidsdocumenten), interviews (toezichthouder, beleidsmakers, experts op het gebied van bescherming persoonsgegevens)

Conclusie indicator
Deze indicator levert een genuanceerder beeld op over de rolopvatting van de toezichthouder naast de middelen die de toezichthouder tot haar beschikking heeft. De indicator is goed te meten en levert een kwalitatieve indicatie op van de rol van de toezichthouder. De uitkomsten passen ook bij de situatieschets, omdat ze een beeld schetsen van de situatie in een land en de wijze waarop bescherming van persoonsgegevens wordt aangepakt in een land. Voor de totale beeldvorming is deze indicator dus van waarde. De variabelen zijn te meten via desk research van websites en verslagen van toezichthouders en overheidsdocumenten. Daarnaast kunnen interviews gehouden worden met in ieder geval de toezichthouders en mogelijk kunnen ook vragen gesteld worden aan beleidsmakers, burgerrechtenorganisaties en experts op het gebied van de bescherming van persoonsgegevens.

7.3 Handhaving door de toezichthouder

De toezichthouder heeft bepaalde bevoegdheden, die in paragraaf 7.2 genoemd zijn, maar het is daarmee nog niet zeker of en hoe zij hier gebruik van maakt. De mate waarin de wet gehandhaafd wordt en eventuele sancties die opgelegd worden

door de toezichthouder geven een indicatie van de activiteit van de toezichthouder. Hierbij moet er wel rekening mee gehouden worden dat het aantal incidenten per land kan verschillen. Bovendien moet er rekening gehouden worden met de omvang van een land en het inwoneraantal.

Tabel 19 Variabelen handhaving door de toezichthouder

Variabele	**Methode en bronnen**
Hoeveel klachten komen er binnen bij de toezichthouder? (bijvoorbeeld in het laatste jaar)	Desk research (website en rapporten toezichthouder(s)), interviews (toezichthouder(s))
Wat voor type klachten komen er binnen bij de toezichthouder?	Desk research (website en rapporten toezichthouder(s)), interviews (toezichthouder(s))
Hoeveel handhavingen (boetes, etc.) door de toezichthouder hebben plaatsgevonden (bijvoorbeeld in het afgelopen jaar)?	Desk research (website en rapporten toezichthouder(s), overheidswebsites), interviews (toezichthouder(s))
Hoeveel civiele rechtszaken vinden er plaats over bescherming van persoonsgegevens (waar de toezichthouder niet optreedt)? (bijvoorbeeld in het afgelopen jaar)	Desk research (uitspraken van gerechtshof), interviews (experts op het gebied van wetgeving rond bescherming van persoonsgegevens)
Hoeveel rechtszaken via de toezichthouder vinden er plaats over bescherming van persoonsgegevens? En wat is daarvan de uitkomst (voorbeelden geven)?	Desk research (website en rapporten toezichthouder(s)), interviews (toezichthouder(s))

Conclusie indicator
Deze indicator zegt indirect iets over de rol van de overheid omdat de toezichthouder doorgaans in relatie tot de overheid staat, in Nederland is het CBP bijvoorbeeld een zelfstandig bestuursorgaan. Het handelen en beleid van een toezichthouder is bovendien van invloed op de overheid, die ook onder toezicht staat van de toezichthouder. Een beeld wordt verkregen van het aantal klachten in relatie tot het aantal handhavingsactiviteiten. Vanuit de jaarverslagen is deze indicator eenvoudig te meten.

7.4 Opvattingen over de toezichthouder bij burgers en bedrijven

Deze indicator draait om de vraag hoe burgers en bedrijven denken over de toezichthouder. Dit geeft een indruk van in hoeverre deze door hen wordt gezien als een partij die de persoonsgegevens van individuele personen beschermt. Wanneer burgers hen niet als beschermer van persoonsgegevens zien dan betekent dit mogelijk (maar niet zeker) iets over de manier waarop persoonsgegevens in een land beschermd worden, maar het kan ook te maken hebben met de profilering van de toezichthouder. Mogelijk doet een toezichthouder wel goed werk, maar meer op de achtergrond en minder in het zicht van burgers. In dat geval zegt de bekendheid van burgers met een toezichthouder vooral iets over het bewustzijn van burgers.

Tabel 20 Variabelen opvattingen over de toezichthouder

Variabele	**Methode en bronnen**
In hoeverre zijn burgers bekend met de nationale toezichthouder(s) en wat zij doen?	Desk research (website en rapporten toezichthouder, bestaande survey, bestaand onderzoek), interviews (toezichthouder), nieuwe survey (burgers, alleen als er voor meer variabelen een survey uitgezet wordt), focusgroepen (representatie burgers uit een land)
Hoe denken burgers over de toezichthouder(s)?	Desk research (website en rapporten toezichthouder, bestaande survey, bestaand onderzoek), interviews (toezichthouder), nieuwe survey (burgers, alleen als er voor meer variabelen een survey uitgezet wordt), focusgroepen (representatie burgers uit een land)
Zijn organisaties bekend met de toezichthouder(s) en wat zij doen?	Desk research (website en rapporten toezichthouder, bestaande survey, bestaand onderzoek), interviews (toezichthouder, belangenorganisaties, selectie organisaties)
Hoe denken organisaties over de toezichthouder(s)? (Vinden zij bijvoorbeeld dat zij terechte beslissingen nemen voor de bescherming van persoonsgegevens?)	Desk research (website en rapporten toezichthouder, bestaande survey, bestaand onderzoek), interviews (toezichthouder, belangenorganisaties, selectie organisaties)

Conclusie indicator
Deze indicator geeft een beeld van de wijze waarop burgers en organisaties de rol van de toezichthouder ervaren en zegt dus iets over hun beleving daarvan. Waarschijnlijk is de informatie niet allemaal voorhanden, waardoor een nieuwe survey of bijvoorbeeld focusgroepen met burgers noodzakelijk kunnen zijn om de informatie te verzamelen. De mening van bedrijven kan gepeild worden via brancheorganisaties en belangenorganisaties. Deze indicator is minder prominent in dit onderzoek en kan achterwege worden gelaten wanneer er geen aanvullend onderzoek wordt gedaan onder burgers.

8 Landenselectie

8.1 Selectieproces landen

Om een goed beeld te verkrijgen van de bescherming van privacy van burgers in Nederland zal aan de hand van de indicatoren een vergelijking gemaakt worden met enkele andere Europese landen. De volgende criteria zijn opgesteld voor de selectie van de landen:

1. Spectrum van landen die bekend staan om strenge en soepele houding ten opzichte van privacybescherming
2. Land met vergelijkbare benadering van gegevensbescherming als Nederland
3. Land met andere benadering van gegevensbescherming dan Nederland
4. Maturiteit van landen op het gebied van privacybescherming

De invulling van de genoemde criteria is afhankelijk van de cultuur van de bevolking in een land. Deze heeft invloed op de mate waarin bescherming van persoonsgegevens belangrijk wordt gevonden en hoe dit zich in de praktijk uit. Bijvoorbeeld in Spanje en Portugal wordt het verstrekken van persoonlijke informatie relatief problematisch gevonden in vergelijking tot een aantal Noord Europese landen (Eurobarometer, 2015). In Zweden, Finland en Denemarken is er ten opzichte van het Europese gemiddelde een hoge mate van vertrouwen in andere mensen (Huijboom, 2010). Dit vertaalt zich onder andere in een bereidheid om meer persoonlijke informatie te delen. Bekend is dat het in Zweden relatief normaal is om bijvoorbeeld gegevens over inkomen met anderen te delen, terwijl dit bijvoorbeeld in Nederland veel minder gebruikelijk is.

Op grond van deze criteria kan de volgende longlist worden opgesteld:

1. Frankrijk
2. Duitsland
3. Verenigd Koninkrijk
4. Ierland
5. Roemenië (of ander Oost-Europees land)
6. Spanje/Italië/Portugal
7. Zweden

De landen worden in de volgende paragraaf kort besproken. Daaruit zal ook blijken waarom deze landen interessant en geschikt zijn voor de vergelijkende studie.

Om tot een definitieve selectie van landen te komen is van belang welke criteria prioriteit krijgen. Tevens is het van belang om de vergelijking daadwerkelijk goed uit te kunnen voeren. De benodigde informatie moet dus in de te vergelijken landen goed te verkrijgen zijn, bijvoorbeeld via openbare bronnen of op basis van expertinterviews.

8.2 Selectie van landen

In deze paragraaf worden de verschillende landen van de longlist kort besproken en worden opvallende aspecten uitgelicht. Tenzij anders aangegeven, zijn de percentages die hierbij worden genoemd afkomstig uit de Eurobarometer van maart 2015.[16]

8.2.1 Frankrijk

Frankrijk is op het gebied van het implementeren van regelgeving op het gebied van privacy over het algemeen vergelijkbaar met Nederland. De toezichthouder in Frankrijk (CNIL) is in Europa relatief gezien erg actief op het gebied van handhaving,[17] maar neemt ook op het gebied van voorlichting een vooraanstaande positie in.[18] De positie is op het vlak van voorlichting enigszins vergelijkbaar met de rolopvatting van destijds de OPTA en nu de ACM in Nederland. Ook heeft Frankrijk in de implementatie van Europese wetgeving op het gebied van privacy vaak een vergelijkbare vorm gekozen als Nederland.[19] In algemene zin is Frankrijk dus zowel op het gebied van wetgeving als van toezicht op bescherming van persoonsgegevens vergelijkbaar met Nederland. Alleen kan de CNIL al enkele jaren boetes op leggen tot 300.000 euro voor datalekken, terwijl dat in Nederland tot 1 januari 2016 nog slechts 4500 euro was (daarna wordt dit 810.000 euro). Tot voor kort beschikte de Franse toezichthouder in dit opzicht dus wel over zwaardere middelen dan het Nederlandse CBP.

8.2.2 Duitsland

Duitsland staat over het algemeen bekend als een erg kritisch land op het gebied van privacy. Recent heeft dit ook weer tot discussie geleid, doordat Duitsland de onderhandelingen voor de nieuwe Algemene Verordening Gegevensbescherming vertraagde vanwege de angst dat een lager beschermingsniveau zou volgen dan onder de huidige regelgeving, terwijl juist een betere bescherming gewenst is.[20] Niet alleen de toezichthouder is streng en handhaaft de wetgeving strikt, zoals bijvoorbeeld blijkt uit de verschillende maatregelen tegen bijvoorbeeld Facebook, dat instellingen binnen Duitsland heeft moeten aanpassen.[21] Ook de Duitse bevolking zelf lijkt vrij kritisch te zijn. Er zijn voorbeelden bekend dat mensen de straat opgingen om de weg te blokkeren voor Google Streetview auto's.[22] Opvallend is ook dat Duitsland als enige land vanaf het begin de dataretentie richtlijn (Richtlijn 2006/24/EG) heeft aangevochten wegens strijd met de constitutie.[23] Pas later volgden andere landen en inmiddels worden nationale implementaties teruggedraaid of aangepast.

---

[16] European Commission, Special Eurobarometer 431, Data Protection, March 2015.
[17] Bijvoorbeeld op het gebied van het gebrek aan opt-out mogelijkheden bij de Google diensten: http://www.guardian.co.uk/technology/2012/oct/15/google-privacy-policy.
[18] A. van Veenstra e.a., Quickscan e-Privacy. TNO 2015 R11474, 2013, p. 52.
[19] Idem.
[20] Zie bijvoorbeeld: http://www.lexology.com/library/detail.aspx?g=6e7e524a-b57c-440e-b100-580172126dcf.
[21] Zie bijvoorbeeld het oordeel van de Hamburgse toezichthouder met de opdracht tot aanpassing van de Facebook tracking systemen: https://www.datenschutz-hamburg.de/news/detail/article/trackingverdacht-bei-facebook.html?tx_ttnews%5BbackPid%5D=186&cHash=3978094d546a3f7276c1193dd02be52b.
[22] Zie: http://www.streetviews.nl/google-streetview-stuit-in-duitsland-op-protest/.
[23] Zie: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html.

Tenslotte heeft Duitsland een bijzondere inrichting van het systeem van toezichthouders, waarbij de afzonderlijke Länder ieder een eigen toezichthouder hebben, vergelijkbaar met het CBP, maar er ook een federale toezichthouder is voor constitutionele zaken (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)*).

8.2.3 Verenigd Koninkrijk

Het Verenigd Koninkrijk is vooruitstrevend op het gebied van het voorschrijven en aanbevelen van technologieën en organisatorische maatregelen ten behoeve van privacybescherming, zoals PIA's en dataportabiliteit.[24] Privacy Impact Assessments zijn in het Verenigd Koninkrijk al langere tijd gemeengoed en een verplicht onderdeel bij de invoering van nieuwe wetgeving. Ook de toezichthouder, de Information Commissioner's Office (ICO) is erg actief in het geven van voorlichting, zowel aan burgers als organisaties. Op de website staan bijvoorbeeld voorlichtingsfilmpjes over telemarketing en voor burgers en bedrijven is er een hulplijn (die enkel jaren geleden zelfs nog Hotline heette) voor informatie of het indienen van een klacht.[25] Daar staat wel tegenover dat de Engelse overheid veel privacybeperkende maatregelen invoert, zoals op het gebied van surveillance. Cameratoezicht (CCTV) is erg intensief[26], en er is ook een belangrijke relatie tussen de Engelse inlichtingendienst (GCHQ) en de fel bekritiseerde NSA.[27] Dat het beschermen van de privacy van burgers toch belangrijk wordt gevonden in het Verenigd Koninkrijk blijkt uit de grote mate van bezorgdheid van burgers over het gebrek aan controle over persoonlijke informatie. In het Verenigd Koninkrijk maakt 79% van de bevolking zich grote zorgen over het niet hebben van controle over hun gegevens in het algemeen, terwijl dit in Nederland 47% is.
Het Verenigd Koninkrijk is tevens interessant om in de vergelijking te betrekken, omdat hier een Common Law systeem geldt, terwijl de rest van Europa een Civil Law systeem hanteert. Een belangrijk gevolg is dat in het Verenigd Koninkrijk Europese wetgeving rechtstreeks wordt geïmplementeerd,[28] waardoor er mogelijk minder gebruik gemaakt wordt van discretionaire bevoegdheden waarmee nuances in de strengheid van deze wetgeving kunnen worden aangebracht op nationaal niveau. Het betreft dan meer of strengere vereisten dan door de Richtlijn als minimum voorgeschreven zijn.

8.2.4 Ierland

Ook in Ierland heersen grote zorgen onder burgers over het niet hebben van controle over persoonlijke gegevens (79%). Bovendien is Ierland interessant vanwege de aanwezigheid van de Europese hoofdkantoren van enkele grote Amerikaanse dataverwerkers, zoals Facebook en Google. Dat betekent dat er relatief veel aandacht wordt geschonken aan de wijze waarop de toezichthouder zijn handhavende taak vervult. In dit kader is bijvoorbeeld de recente uitspraak van

---

[24] A. van Veenstra e.a., Quickscan e-Privacy. TNO 2015 R11474, 2013, p. 51.
[25] Zie: https://ico.org.uk/concerns/.
[26] In 2013 was er in het Verenigd Koninkrijk zelfs één camera per 11 inwoners: http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html.
[27] Zie; https://www.privacyinternational.org/illegalspying.
[28] Zo wordt in het algemeen in het Verenigd Koninkrijk rechtstreeks aangesloten op de tekst van een Richtlijn, waarbij als uitgangspunt geldt dat een minimum implementatie wordt verkozen. Zie ook: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229763/bis-13-775-transposition-guidance-how-to-implement-european-directives-effectively-revised.pdf.

het Europese Hof van Justitie in de Schrems-zaak van belang. Vanwege verschillende opvattingen van toezichthouders in Ierland, Oostenrijk en Duitsland werd geoordeeld dat iedere nationale toezichthouder zelfstandig kan bepalen of aan de vereisten uit de Europese regelgeving op het gebied van bescherming van persoonsgegevens is voldaan.[29] De soepele houding van de Ierse toezichthouder ten aanzien van Facebook (als grote dataverwerker) was aanleiding tot het stellen van prejudiciële vragen aan het Europese Hof.

8.2.5 Roemenië (Oost-Europees land)

Een Oost-Europees land is goed om in de vergelijking te betrekken, omdat een aantal van deze landen vrij recent tot de Europese Unie is toegetreden. Met de toetreding is de Europese regelgeving op het gebied van privacybescherming ook voor die landen van kracht geworden. Deze landen hebben daarom een kans tot implementatie, waarbij er geen of weinig sprake is van legacy problemen[30] en meer vanuit een nieuw startpunt regelgeving en handhaving opgezet kan worden. Bij landen die reeds langere tijd regelgeving hebben op allerlei gebieden die geraakt worden door regelgeving aangaande bescherming van persoonsgegevens betekent de implementatie van een Richtlijn vaak dat ook veel bestaande andere wetgeving aangepast dient te worden. Roemenië is in 2007 lid geworden van de Europese Unie en heeft een volledig nieuw regelgevend kader voor bescherming persoonsgegevens opgezet. Op basis van het Europese kader is in 2001 een wet ingevoerd over de bescherming van persoonsgegevens en in 2005 is de bijbehorende toezichthouder in het leven geroepen.[31]

8.2.6 Spanje/Italië/Portugal (Zuid-Europees land)

Om een beeld te krijgen van de invloed van culturele diversiteit tussen landen en wat dat betekent voor de privacybescherming in die landen wordt aanbevolen om in de vergelijking ook een Zuid-Europees en een Noord-Europees land op te nemen. Met name sociaal-maatschappelijke verschillen ten aanzien van de mate van openheid en bereidheid tot het delen van gegevens door burgers kunnen perspectief bieden voor de vergelijking. Landen waarvan de bevolking een relatief hoge mate van vertrouwen heeft in de overheid worden ook gekenmerkt door een grotere bereidheid van burgers tot het delen van informatie (Huijboom 2010). De bereidheid tot het delen van informatie hangt dus samen met het vertrouwen in de overheid. Een overheid die actief beleid voert en handhaaft op zorgvuldige omgang met persoonsgegevens kan mogelijk een opener sociaal-maatschappelijk klimaat stimuleren.

In Zuid-Europese landen heerst bijvoorbeeld een andere opvatting over het delen van gegevens dan in Nederland. Op basis van de Eurobarometer blijkt bijvoorbeeld dat zowel in Spanje als in Portugal minder dan 30% van de bevolking het eens is met de stelling dat het verstrekken van persoonlijke informatie geen probleem is. In Nederland is dat percentage 48%. Bovendien is in Spanje de afgelopen 5 jaar de instemming met de stelling dat het delen van gegevens een groeiend onderdeel is

[29] Zie: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.
[30] In het Verenigd Koninkrijk bracht bijvoorbeeld de implementatie van de richtlijn Oneerlijke Handelspraktijken de noodzaak met zich mee om 23 andere wetten aan te passen. Een uitgebreid juridisch system dat over vele jaren is opgebouwd kan dan dus behoorlijk in de weg zitten. Zie: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229763/bis-13-775-transposition-guidance-how-to-implement-european-directives-effectively-revised.pdf, p. 9.
[31] Zie: http://www.dataprotection.ro/index.jsp?page=about&lang=en.

van het moderne leven met 15% gedaald naar 67%, terwijl dit voor Nederland nog steeds 86% is.
In Zuid-Europa heerst ook het meeste gevoel volledige controle te hebben over persoonlijke gegevens. In Portugal is 25% het met die stelling eens, terwijl dit in Nederland slechts 9% is. Het is interessant om een genuanceerder beeld te verkrijgen van de samenhang tussen bereidheid tot delen van gegevens, het vertrouwen in de overheid, en of meer geslotenheid leidt tot een groter gevoel van controle van burgers over hun gegevens. Meer geslotenheid kan immers ook samenhangen met de angst voor onzorgvuldig gebruik van gegevens. In ieder geval is in Zuid-Europese landen duidelijk een andere sociaal-maatschappelijk opvatting over controle over gegevens en de bereidheid tot het delen van informatie als aspect van de informatiemaatschappij.

8.2.7 Zweden (Noord-Europees land)

Tenslotte is het aan te bevelen een Noord-Europees land in de vergelijking te betrekken. De algehele cultuur met betrekking tot openheid als tegenhanger van privacy is daar anders dan in Nederland. Voor de stelling dat de meeste mensen vertrouwd kunnen worden geldt gemiddeld in Europa dat 35,8% het daarmee eens is. In Noord-Europese landen ligt dat percentage substantieel hoger, zoals in Finland 55,5% en in Denemarken zelfs 58,3% (Huijboom, 2010). In Zweden, Finland en Denemarken is in lijn hiermee een grote instemming met de stelling dat het ontsluiten van informatie een toenemend onderdeel van het moderne leven is (in alle drie de landen zowel in 2010 als 2015 meer dan 80%, Eurobarometer 2015). Het vertrouwen in de overheid kan ook samenhangen met de beperkte hoeveelheid informatie die de overheid van burgers vraagt. In Zweden en Finland is respectievelijk slechts 27 en 31% van de burgers het eens met de stelling dat de overheid steeds meer informatie vraagt. Het Europese gemiddelde ligt hiervoor op 56% en Nederland zit met 64% boven dit gemiddelde (Eurobarometer 2015).

9 Tot besluit

In dit rapport is een set aan indicatoren opgesteld op basis waarvan een vergelijkend onderzoek uitgevoerd kan worden naar de positie van Nederland ten opzicht van enkele andere Europese landen op het gebied van de bescherming van persoonsgegevens door de overheid. Op basis van criteria die genoemd zijn in paragraaf 2.2 is een selectie uit de indicatoren voorgesteld, waarbij met name een te lage relevantie of een te moeilijke haalbaarheid als redenen golden om indicatoren uit te sluiten van het onderzoek.

Veel van de informatie zal verkregen kunnen worden op basis van desk research en interviews. In een aantal gevallen zal een referent vanuit de te vergelijken landen aan te bevelen of noodzakelijk zijn voor een goede uitvoering van het onderzoek. Voor enkele indicatoren zal gebruik gemaakt moeten worden van media analyse en eventueel text mining technologie. De kans is groot dat dit een te groot onderzoek oplevert, waardoor deze indicatoren waarschijnlijk niet meegenomen kunnen worden.

Tevens is een voorstel gedaan voor een aantal landen waarmee Nederland vergeleken kan worden en waarmee een goed beeld van de positie van Nederland binnen Europa verkregen kan worden.

Literatuurlijst

Dorbeck-Jung, B. & Oude Vrielink-Van Heffen, M (2006) Op weg naar bruikbare overheidsregulering? In: Recht der Werkelijkheid, Tijdschrift voor de Sociaal-Wetenschappelijke Bestudering van het Recht, 2006, p. 9-18.
Howlett, M. (2009).Governance modes, policy regimes and operational plans: A multi-level nested model of policy instrument choice and policy design, *Policy Science,* 42:73–89

Huijboom, N. (2010). Joined-Up ICT Innovation in Government, Dissertatie, Erasmus Universiteit Rotterdam, 2010, p. 67

Jann, W. & Wegrich, K. (2007). *Theories of the Policy Cylce, in: Handbook of Public Policy Analysis, Theory, Politics and Methods*. Boca Raton: Taylor & Francis Group

Roosendaal et al. (2015). Privacybeleving op het internet in Nederland. TNO report.

TNS Opinion & Social (2015). Special Eurobarometer 431. Data Protection.

Veenstra, A.F. van, Roosendaal, A., Schoonhoven, B. van, Schols, M., Bakker, T. (2013). Quickscan e-privacy. TNO report