Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

32 761 Verwerking en bescherming persoonsgegevens

Nr. 49

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 24 mei 2013

In deze brief geef ik mede namens de Staatssecretaris van Veiligheid en Justitie en de minister van Binnenlandse Zaken en Koninkrijksrelaties, de Kabinetsvisie op e-privacy. Kern van deze visie is goede bescherming van persoonsgegevens en de persoonlijke levenssfeer van de eindgebruiker van online diensten door bedrijven. Tegelijkertijd onderkent het kabinet het economisch belang van de ontwikkeling van online-diensten en het belang van het bieden van ruimte voor innovatie. Een goede bescherming van persoonsgegevens en de persoonlijke levenssfeer draagt bij aan het digitale vertrouwen van betrokkenen en daarmee aan de groei van digitale diensten.

Voorliggende brief richt zich op het gebruik van data in en door de private sector. In de brief en notitie van 29 april 2011 (Kamerstuk 32 761, nr. 1) is de visie op de rol van de overheid en de daarmee samenhangende ICT-veiligheid reeds aan de orde gesteld.[1] Een goede bescherming van persoonsgegevens is ook bij overheidsdiensten van groot belang.

In deze brief wordt een aantal randvoorwaarden geïdentificeerd die nodig zijn voor een goede bescherming van persoonsgegevens en de persoonlijke levenssfeer in private verhoudingen. Ook worden concrete acties benoemd om de positie van de eindgebruiker en een zorgvuldige omgang met diens persoonsgegevens te verbeteren. Een internationale aanpak is vereist daar bescherming van e-privacy een bij uitstek mondiale aangelegenheid is.

Met deze brief geeft het kabinet tevens uitvoering aan de motie van de leden Gesthuizen en Verhoeven (Kamerstuk 24 095, nr. 294) en de moties van het lid Recourt c.s. (Kamerstuk 32 761, nrs. 10 en 11).

[1] «Notitie privacybeleid «(29 april 2011) en «Kabinetsreactie WRR-rapport iOverheid» (25 oktober 2011)

kst-32761-49
ISSN 0921 - 7371
's-Gravenhage 2013

1. Bescherming van persoonsgegevens

Veel Nederlanders maken gebruik van innovatieve, online toepassingen. Deze toepassingen bieden de eindgebruiker vaak gratis, handige diensten. Het gebruik van deze diensten gaat gepaard met het vrijgeven van persoonsgegevens, waarvan bedrijven gebruik maken. Deze persoonsgegevens zijn voor bedrijven interessant en geld waard. Persoonsgegevens vertegenwoordigen dus in toenemende mate een belangrijke economische waarde. Door deze persoonsgegevens af te geven kunnen handige diensten afgenomen worden, maar ontstaat ook een privacyrisico.
Daarom moet worden voorzien in een goede bescherming van persoonsgegevens, zonder dat dit ten koste gaat van het gebruikersgemak en het innovatief vermogen van de interneteconomie.
Volgens een onderzoek van Ernst&Young kan vertrouwen in ICT veel opleveren:
1 miljard extra omzet voor internethandel in Nederland in 2014.[2] Verwacht wordt dat dit vertrouwen er ook toe zal leiden dat meer bedrijven productiviteitsslagen maken (bijvoorbeeld door telewerken, of automatisering van datastromen). Vertrouwen in ICT en online diensten zal de economische groei stimuleren.

1.1. Meer digitaal vertrouwen

Het zijn vaak de gratis, handige diensten waarmee het vertrouwen in ICT gemakkelijk kan worden geschaad. De eindgebruiker lijkt weinig grip te hebben op de ontwikkelingen op het terrein van de gegevensverwerking en het gebruik ervan. De gebruikers zijn zich niet altijd bewust, of op de hoogte van wat derden met hun persoonsgegevens doen, en welke impact dat heeft in de online wereld. Uit onderzoek van de Europese Commissie onder eindgebruikers in de EU-lidstaten (Eurobarometer) blijkt dat er zelfs ernstige twijfel bestaat bij internetgebruikers over de bescherming van persoonsgegevens en de persoonlijke levenssfeer bij vooral private bedrijven.[3] Dit komt het digitaal vertrouwen niet ten goede.

Het is voor de eindgebruiker niet altijd duidelijk wat er met de gegevens gebeurt die hij moet aanleveren bij het afnemen van online diensten. Dat komt ook uit het eerder genoemde Eurobarometeronderzoek naar voren. Er is sprake van informatieasymmetrie.

Tegelijkertijd moeten consumenten akkoord gaan met privacyvoorwaarden om gebruik te kunnen maken van bepaalde diensten, of voor het kunnen kopen van producten. De teksten van de voorwaarden zijn veelal lang, complex en gezien het juridische jargon niet voldoende te begrijpen voor een gemiddelde eindgebruiker.

Een vinkje bij de privacyvoorwaarden ontslaat een organisatie er niet van de privacy van hun klanten te respecteren en hiertoe helder te communiceren over waarom en hoe organisaties en derde partijen met persoonsgegevens en persoonlijke data van hun klanten omgaan. Het moet voor het bedrijfsleven onderdeel zijn van het maatschappelijk verantwoord ondernemen om de internetgebruiker van makkelijk toegankelijke informatie te voorzien over het privacybeleid van een bedrijf. Daarin moet duidelijk worden aangegeven door wie, met welk doel, en wat er met de persoonlijke gegevens van de internetgebruiker gebeurt.

---

[2] Ernst&Young, Groeien door Veiligheid (2011).
[3] Eurobarometer 359 juni 2011

1.2. Randvoorwaarden voor meer vertrouwen

Het kabinet hecht sterk aan een doeltreffende bescherming van persoonsgegevens en de persoonlijke levenssfeer, waarbij van belang is dat de invulling van de bescherming gebruikersvriendelijk is en praktisch uitvoerbaar voor het bedrijfsleven en innovatie niet onnodig wordt belemmerd. Belangrijk is dat de eindgebruiker meer controle krijgt over zijn gegevens[4]. Hiervoor zijn de volgende randvoorwaarden noodzakelijk:

- **Controle** van de eindgebruikers over gebruik van hun persoonsgegevens. Zij moeten nadrukkelijk toestemming voor gebruik persoonsgegevens kunnen geven; eindgebruikers moeten het recht krijgen om vergeten te worden en de mogelijkheid hebben hun data te verplaatsen en mee te nemen naar bijvoorbeeld een andere aanbieder of platform (dataportabiliteit).
- **Transparantie** over de verzameling en verwerking van gegevens: de eindgebruiker moet volledig en duidelijk over de verwerking geïnformeerd worden, zodat hij ook een duidelijke keuze heeft en weet wat er met zijn gegevens gebeurt.
- **Verantwoordelijkheid bedrijven:** bedrijven zijn reeds bij de inrichting van hun diensten verantwoordelijk voor correcte verwerking van persoonsgegevens en moeten te allen tijde zorg dragen voor een goede beveiliging van persoonsgegevens.

Om de randvoorwaarden voor meer vertrouwen te scheppen, zal het kabinet een aantal acties ondernemen via de sporen wetgeving, versterking van het toezicht en intensivering van de dialoog met het bedrijfsleven, en vergroting van het bewustzijn van eindgebruikers en marktpartijen op het gebied van e-privacy.

Een eerste stap hierbij is dat gebruikers en online-bedrijven kritisch zijn op het geven van persoonsgegevens respectievelijk verzamelen van gegevens die niet nodig zijn voor het verdienmodel en zich beperken tot die gegevens die nodig zijn om de dienst af te kunnen nemen respectievelijk aan te kunnen bieden, met andere woorden dataminimalisering. Dat zal de risico's voor de privacy ook beperken.
Een aantal van de randvoorwaarden is al ingevuld in de Wet bescherming persoonsgegevens (Wbp). Uitgangspunt daarbij is dat verwerking van (gevoelige) persoonsgegevens veilig, transparant en uitsluitend op basis van een in de wet bepaalde grond voor verwerking plaatsvindt. Binnen dit wettelijk kader is het mogelijk persoonsgegevens te verwerken en kunnen online-diensten volop worden ontwikkeld en geïnnoveerd.

Online privacy heeft een sterke internationale dimensie. Internationaal geldende regels voor privacy zijn dan ook van het grootste belang voor zowel burgers als het bedrijfsleven. Daarom hecht het kabinet sterk aan de totstandkoming van een Europese Verordening over privacy en afspraken met landen buiten de EU. Op 25 januari 2012 heeft de Europese Commissie een voorstel gepresenteerd voor een Verordening die de huidige Privacyrichtlijn uit 1995 moet vervangen. Daarin wordt een aantal maatregelen voorgesteld ter verbetering van de positie van eindgebruikers. Het gaat daarbij onder meer om onderwerpen als transparantie, toestemming voor gebruik van persoonsgegevens, betere bescherming van minderjarigen op het internet, het recht om vergeten te worden en dataportabiliteit. Belangrijk element van het voorstel voor de Verordening is ook het scheppen van een eenduidig en gelijk speelveld voor de bedrijven door gelijke wetgeving in alle 27 lidstaten. Bedrijven zullen in alle lidstaten hetzelfde niveau van bescherming van privacy moeten bieden. Het kabinet ondersteunt de hoofdlijnen van dit voorstel.

---

[4] Booz&Co, Digital Confidence. Securing the Next Wave of Digital Growth (2008).

1.3. Innovaties en e-privacy

Actuele ontwikkelingen en de randvoorwaarden

In deze paragraaf worden enkele innovaties en actuele ontwikkelingen uitgelicht die nu spelen. Bij alle ontwikkelingen zal het kabinet steeds toezien dat deze passen binnen de geformuleerde randvoorwaarden die worden gesteld aan privacy te weten: controle van de eindgebruikers over gebruik van hun persoonsgegevens, transparantie over de verzameling en verwerking van gegevens en verantwoordelijkheid van bedrijven. Daarbij zullen de toezichthouders moeten controleren dat de ontwikkelingen voldoen aan de Wet bescherming persoonsgegevens, de Telecommunicatiewet en in de toekomst aan de Verordening. Er zal ook steeds moeten worden beoordeeld of bestaande wetgeving nog adequaat is en mogelijkheden van zelfregulering zullen moeten worden benut.

Cookies

Op dit moment geldt op basis van de zogenoemde cookiebepaling voor het plaatsen en lezen van een cookie de eis dat daarvoor toestemming moet zijn verleend door de internetgebruiker nadat deze afdoende over de cookie is geïnformeerd.

Deze regel geldt voor alle cookies, behalve functioneel noodzakelijke cookies, ook al gaat het om cookies die geen inbreuk maken op de privacy. Er wordt een wetsvoorstel voorbereid om hier verandering in te brengen.

Het voorstel tot wijziging van de cookie-bepaling in de Telecommunicatiewet wordt momenteel geconsulteerd. Voorop staat dat geen afbreuk wordt gedaan aan het doel van de cookiebepaling, bescherming van de persoonlijke levenssfeer van de internetgebruiker. De eindgebruiker op internet moet, duidelijk en in begrijpelijke taal, informatie over het gebruik van cookies krijgen en vooraf om toestemming worden gevraagd voor het gebruik van de cookies. Alleen voor die cookies die geen of geringe gevolgen hebben voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker, is geen voorafgaande toestemming nodig.

Met de voorgestelde wijziging wordt voorkomen dat de cookiebepaling zijn doel voorbij schiet, terwijl het doel van de cookiebepaling, bescherming van de privacy, overeind blijft. Internetgebruikers worden beter in staat gesteld om hun privacy te beschermen als zij alleen in gevallen waarin dit hun persoonlijke levenssfeer raakt, om toestemming worden gevraagd. Als ook toestemming wordt gevraagd voor cookies die de privacy niet schenden, verliest het verzoek om toestemming aan betekenis.

De voorgestelde wijziging past in de geformuleerde randvoorwaarden van controle en transparantie voor internetgebruikers en eigen verantwoordelijkheid van bedrijven, met oog voor de gebruikersvriendelijkheid en praktische uitvoerbaarheid voor het bedrijfsleven.

Big Data: verzamelen van persoonsgegevens

Marktpartijen verzamelen op allerlei manieren persoonsgegevens. Het benutten van almaar groeiende datasets door bedrijven, wordt ook wel het principe van *Big Data* genoemd; het analyseren van grote hoeveelheden gegevens in hun samenhang. Het verzamelen en gebruiken van big data is een belangrijke ontwikkeling. Het gaat daarbij om allerlei toepassingen: machine to machine (voorbeeld: besturing slimme dijken en

wegen), maar ook op grote schaal verzamelen van persoons- en privacygevoelige gegevens.

Door middel van profiling krijgen marktpartijen beter inzicht in hun doelgroep en kan deze doelgroep online gerichter worden benaderd. Profiling gebeurt onder meer door het surfgedrag van eindgebruikers in kaart te brengen. Om dit te doen worden bijvoorbeeld cookies op de computer van de eindgebruiker geïnstalleerd, wordt de standaard HTML 5 gebruikt,of wordt device fingerprinting[5] ingezet.

Ook kan het zoekgedrag bestudeerd worden via de informatie die een zoekmachine, zoals Google, heeft, via het achterlaten van gegevens door de gebruiker zelf (op social media zoals Facebook) en door bij te houden wat iemand online koopt en door de informatie afkomstig van klantenkaarten van «gewone» winkels. Op dit moment wordt ook geëxperimenteerd met o.a. de zogenaamde *«persuasion profiles»* oftewel «overtuigingsprofielen». Deze profielen bevatten informatie over het soort argumenten waarvoor specifieke eindgebruikers het meest gevoelig zijn.

Het gebruik van al dit soort profielen heeft invloed op de werking van bijvoorbeeld zoekmachines, per gebruiker. Het Rathenau-instituut heeft in de studie «Voorgeprogrammeerd» [6] gekeken naar de manier waarop de op het internet geleverde selecties, of zoekopdrachten het leven bepalen van eindgebruikers. Hierbij wordt aangegeven dat voorprogrammeren de keuzemogelijkheden voor eindgebruikers zowel verruimt als beperkt. Dat er voorgeprogrammeerde keuzes worden gemaakt op basis van bijvoorbeeld profielen kan als positief worden ervaren. Zo vinden veel mensen gepersonifieerde aanbiedingen die bij hun levensstijl passen heel handig. Het kan er voor zorgen dat de consument van beperkte informatie wordt voorzien, wat in sommige gevallen ook de bedoeling is. De kans bestaat echter ook dat de online omgeving strikt wordt afgestemd op een profiel, waardoor de consument online wordt beperkt. De rest van de online wereld wordt als het ware buiten beeld gelaten zonder dat de gebruiker dat weet. De plaatsing in bepaalde categorieën kan zelfs leiden tot ongelijke behandeling: het is mogelijk dat de eindgebruiker keuzes op internet worden onthouden, of dat sprake is van (prijs)discriminatie op het internet.

Big Data als strategie voor bedrijven is volop in ontwikkeling vooral bij de grote bedrijven. Tegelijkertijd zijn de gevolgen voor de privacy van gebruikers van online aangeboden diensten en producten op voorhand nog niet duidelijk, maar kunnen wel ingrijpend zijn. Niet alle risico's die productie en het gebruik van bijvoorbeeld online profiling met zich meebrengen zijn in beeld. Het is dan ook een ontwikkeling die zal worden gevolgd door het kabinet om er voor te zorgen dat de verzameling en verwerking van big data plaats vindt binnen de randvoorwaarden die het kabinet heeft gesteld, waaronder de Wet bescherming persoonsgegevens en artikel 11.7a van de Telecommunicatiewet (de cookiebepaling).

Sociale media en de positie van minderjarigen

Het gebruik van sociale media is de afgelopen jaren enorm toegenomen. Deze platforms zijn erg populair. De gebruikers van sociale media ervaren namelijk veel voordelen van het feit dat ze (continu) online zichtbaar zijn

---

[5] Device fingerprinting is een technologie waarmee een profiel van een eindgebruiker wordt samengesteld op basis van instellingen van een mobiele telefoon, laptop of tablet. Daarbij kan worden gekeken naar de ingestelde tijdzone, lettertypes en plug-ins.

[6] «Voorgeprogrammeerd», Rathenau-instituut (februari 2012)

en zonder tussenkomst van massamedia interactief met elkaar kunnen communiceren.
Juist omdat sociale media ruimte bieden aan het breed uitdragen van persoonlijke informatie, vindt zowel het kabinet als de Europese Commissie het van groot belang dat hierbij speciale aandacht is voor het gebruik van online diensten door minderjarigen. Minderjarigen zijn nog niet in staat om privacyrisico's te beoordelen en te overzien wat hier de consequenties van zijn op lange termijn. Ook de Tweede Kamer heeft aandacht gevraagd voor de veiligheid van minderjarigen op internet (moties van het lid Recourt c.s. (Kamerstuk 32 761, nrs. 10 en 11). Het kabinet deelt de bezorgdheid van de Kamer met betrekking tot de veiligheid van minderjarigen op internet. Gelet op de veelal internationaal opererende aanbieders van sociale media is dit een onderwerp dat qua wetgeving en flankerend beleid in toenemende mate in een Europese context moet worden bezien en waar een belangrijke verantwoordelijkheid voor het bedrijfsleven ligt.

Cloud computing en e-privacy: informatiebeveiliging

In het rapport «Fundament op orde»[7] dat in opdracht van het toenmalige ministerie van EL&I is opgesteld, worden de kansen en bedreigingen van cloud computing op een rij gezet en wordt de relatie gelegd met privacy-aspecten. Cloud computing biedt vele mogelijkheden, maar vereist tegelijkertijd een goede borging van de privacy. Uitgangspunt voor Nederland, verwoord in de Digitale Implementatie Agenda, is dat de eindgebruiker een gerechtvaardigd vertrouwen moet ervaren bij het internetgebruik.
In dit verband is de EU cloud strategie[8] die op 27 september 2012 is gepubliceerd van belang. In deze strategie wordt ingezet op de economische kansen van cloud computing en de nodige activiteiten om door dataprotectie en standaardisering in internationaal verband privacy-aspecten beter te borgen. Daarnaast heeft het Cbp in 2012 een zienswijze over cloud computing uitgebracht.

Aangezien er geen barrières bestaan die grensoverschrijdende clouddiensten tegenhouden, is internationale dialoog van cruciaal belang om ook buiten de EU de privacy te beschermen.

Enkele dominante partijen

Categorisering van eindgebruikers, mogelijke risico's voor informatiebeveiliging bij cloud computing en het gebruik van sociale media door jongeren kunnen allemaal leiden tot privacy risico's. Deze risico's worden mogelijk versterkt door de beperkte concurrentie tussen dienstaanbieders[9].

De meeste internetgebruikers in Europa en een groot deel van de gebruikers in de VS maken gebruik van Google als zoekmachine. Bij de sociale media lijkt op dit moment Facebook de markt te overheersen. Gezien de posities van genoemde bedrijven leent zich dit nadrukkelijk voor mogelijke aanpak hiervan op internationaal niveau. In dit kader doet de Europese Commissie al onderzoek, op het terrein van mededinging, naar mogelijk misbruik door Google van zijn economische machtspositie door eigen diensten te bevoordelen bij de zoekresultaten van zijn eigen zoekmachine. Dit is echter gericht op de economische machtspositie die deze bedrijven innemen. Bedrijven hebben een eigen verantwoorde-

[7] «Fundament op orde» (maart 2012), VKA/Van Doorne en Rand.
[8] «Unleashing the potential of cloud computing in Europe» (september 2012).
[9] «Voorgeprogrammeerd», Rathenau-instituut (februari 2012).

lijkheid en dienen bij het aanbieden van diensten de privacyregels in acht te nemen. Gezien de positie van genoemde bedrijven, leent ook hier het Europees niveau zich het beste om deze privacyregels vast te stellen.

2. Wetgeving

Bij wet is een aantal zaken geregeld om er voor te zorgen dat gegevens goed worden beveiligd. Op Europees niveau is er het Europees Verdrag tot Bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM)[10]. Hierin is het recht op bescherming van het privéleven, waarvan het recht op bescherming van persoonsgegevens deel uitmaakt, als fundamenteel recht vastgelegd. Het recht op bescherming van persoonsgegevens wordt op gelijkwaardige wijze beschermd door artikel 8 van het Handvest voor de Grondrechten van de Europese Unie.

Op het niveau van de Raad van Europa is al in 1981 het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag nr. 108) vastgesteld. Dit verdrag wordt momenteel gemoderniseerd. Op EU-niveau zijn relevante privacykaders vastgesteld in een tweetal richtlijnen op het gebied van privacy[11].

Om persoonsgegevens en de persoonlijke levenssfeer te beschermen, is in Nederland diverse wetgeving van kracht. In artikel 10 van de Grondwet is het recht op bescherming van de persoonlijke levenssfeer gegarandeerd, en wordt de wetgever een opdracht gegeven regels vast te stellen met betrekking tot de bescherming van persoonsgegevens. In artikel 13 van de Grondwet is het brief-, telefoon en telegraafgeheim vastgelegd. Dit kader blijkt onvoldoende duidelijk nu veel communicatie via elektronische kanalen plaatsvindt. Er is dan ook een wijziging van artikel 13 van de Grondwet in voorbereiding, waarbij het brief- en telefoongeheim wordt uitgebreid naar een brief- en telecommunicatiegeheim.

Naast de Grondwet is in dit kader de Wet bescherming persoonsgegevens Wbp) van toepassing. Deze wet bepaalt dat persoonsgegevens (ofwel: gegevens die herleidbaar zijn tot een individu) alleen onder bepaalde voorwaarden mogen worden verwerkt of opgeslagen. Het College bescherming persoonsgegevens (Cbp) heeft als taak toe te zien op het zorgvuldig en veilig gebruik van persoonsgegevens.

De Staatssecretaris van Veiligheid en Justitie heeft, samen met de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken, een wetsvoorstel in voorbereiding waarmee de meldplicht voor datalekken ook buiten de reikwijdte van de Telecommunicatiewet voor bedrijven, organisaties en instellingen zal gelden. Deze meldplicht zal worden opgenomen in de Wbp. Het opnemen van een brede meldplicht in algemene bepalingen sluit aan bij het voornemen van de Europese Commissie een meldplicht voor datalekken in de Europese wetgeving te regelen.

In de Telecommunicatiewet zijn in hoofdstuk 11 (Bescherming van persoonsgegevens en de persoonlijke levenssfeer) bepalingen opgenomen voor de aanbieders van openbare elektronische netwerken en diensten met betrekking tot verkeersgegevens. Verkeersgegevens zijn gegevens die de aanbieder nodig heeft voor het transport, de facturering of voor verbetering van de service. Deze gegevens mag de aanbieder niet langer ongeanonimiseerd bewaren dan nodig voor de facturering of

[10] EVRM, artikel 8.
[11] Richtlijn 95/46/EG en richtlijn 2002/58/EG.

– mits de abonnee daarvoor toestemming heeft gegeven – voor marktonderzoek. Daarnaast zijn in dit hoofdstuk bepalingen opgenomen inzake de zorgplicht voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers en het vertrouwelijke karakter van de communicatie en bepalingen inzake o.a. locatiegegevens, spam, telemarketing, de cookies en de meldplicht bij datalekken voor de telecomsector.

3. Acties

Om de randvoorwaarden voor meer vertrouwen te scheppen, zal het kabinet een aantal acties op gang brengen. Deze acties zijn kaderstellend via wetgeving, zijn gericht op versterking van het toezicht en de dialoog met het bedrijfsleven en de effectiviteit van de handhaving van de geschapen kaders. Tot slot moet het bewustzijn worden vergroot van eindgebruikers en marktpartijen op het gebied van e-privacy.

3.1. Wetgeving

Nieuwe wetgeving is voorzien in een voorstel voor de EU-Verordening over het gebruik van persoonsgegevens, ook online. Daarover wordt nu onderhandeld in Brussel. Deze Verordening heeft straks rechtstreekse werking in de lidstaten.

De Tweede Kamer wordt in kwartaalrapportages op de hoogte gehouden van het verloop van de onderhandelingen (Kamerstuk 32 761, nrs. 34, 44 en 46). In het voorstel voor deze Verordening wordt een aantal maatregelen voorgesteld ter verbetering van de positie van de eindgebruiker:

- **het recht om vergeten te worden:** dit houdt in dat verantwoordelijken (bedrijven), onder bepaalde voorwaarden, op verzoek van betrokkenen onmiddellijk actie dienen te ondernemen om alle persoonsgegevens van betrokkenen te verwijderen. Tevens dienen verantwoordelijken ervoor te zorgen dat derde partijen aan wie zij de gegevens hebben verstrekt, de gegevens ook verwijderen;
- **recht op dataportabiliteit:** betrokkenen moeten een kopie van hun opgeslagen persoonsgegevens kunnen krijgen om deze gegevens over te kunnen dragen aan een ander bedrijf;
- **geen profiling zonder toestemming:** betrokkenen hebben het recht om hun toestemming te onthouden aan profilingactiviteiten;
- **zwaardere informatieplicht:** op duidelijke, eenvoudig toegankelijke en begrijpelijke wijze informeren van consumenten over de verwerking van persoonsgegevens; inclusief de periode van opslag van de persoonsgegevens.

Daarnaast wordt juridische zekerheid aan bedrijven en organisaties voor het privacyregime in de hele EU gegeven, waarmee in alle lidstaten van de EU een gelijk speelveld ontstaat. De eerder genoemde EU-Verordening voorziet ook in meer- en hogere sancties. Boetes kunnen in het huidige voorstel oplopen tot twee procent van de wereldwijde omzet van een bedrijf dat zich niet aan de regels houdt. Nederland steunt in hoofdlijnen het voorstel en werkt binnen het Europese verband aan een spoedige vaststelling van de Verordening. De voorgestelde Verordening geeft invulling aan de eerder genoemde randvoorwaarden. De behandeling van het voorstel van de EU-Verordening is in volle gang bij de Raad en het Europees Parlement. De uiteindelijke en meer specifieke invulling van de bovenvoorgestelde maatregelen is uiteraard afhankelijk van het resultaat van deze onderhandelingen.

Naast Europese wetgeving speelt ook de wetgeving in de Verenigde Staten een belangrijke rol ten aanzien privacy en de behandeling en verwerking van persoonsgegevens. Bedrijven opereren namelijk veelal op mondiale schaal. Deze wetgeving verschilt van de EU wetgeving. Het kabinet wil dan ook een dialoog tussen de EU en de VS om wetgeving op elkaar af te stemmen actief ondersteunen ten behoeve van de bescherming van persoonsgegevens en de persoonlijke levenssfeer. Daarnaast zal ook een dialoog nodig zijn met andere landen in de wereld die een belangrijke rol spelen op het gebied van gegevensverwerking.

3.2. Toezicht & handhaving: uitbreiding boetebevoegdheid en voorlichting bedrijfsleven

Effectieve handhaving van de regels ten aanzien van privacy is uiteraard van groot belang. Het College bescherming persoonsgegevens (Cbp) houdt toezicht op de Wet bescherming persoonsgegevens (Wbp) en ACM houdt toezicht op de Telecommunicatiewet. De Kamer heeft eerder haar zorgen geuit of het Cbp voldoende is uitgerust voor een effectieve handhaving, tegen de achtergrond van het toenemend belang van bescherming van persoonsgegevens en persoonsgevoelige data en de voorgestelde EU-verordening algemene gegevensbescherming

In het voorstel voor de EU-Verordening zijn sancties opgenomen die aanzienlijk verder reiken dan de sancties die nu zijn voorzien in de Wbp. Het kabinet ondersteunt de in het voorstel opgenomen sancties. In het regeerakkoord van het kabinet-Rutte II van 29 oktober 2012 is opgenomen dat het Cbp meer bevoegdheden krijgt om bestuurlijke boetes op te leggen ter handhaving van de regels in de Wbp. De uitbreiding van de boetebevoegdheden zal worden opgenomen in het in paragraaf 3 vermelde wetsvoorstel tot wijziging van de Wbp in verband met de invoering van de meldplicht datalekken.

De effectiviteit van toezicht kan ook nog op een andere wijze worden bevorderd. Diverse gesprekken met het bedrijfsleven en ook de onderzoeksresultaten van de TNO-studie wijzen erop dat het bedrijfsleven in Nederland tijdens de ontwikkeling van een nieuw product of bedrijfsproces waarbij mogelijk de bescherming van persoonsgegevens in het geding is, behoefte heeft aan de mogelijkheid van overleg met het Cbp over de verenigbaarheid van dat product of bedrijfsproces met de eisen die worden gesteld of gesteld gaan worden aan bescherming van persoonsgegevens. Hoewel het Cbp zich in samenspraak met achtereenvolgende kabinetten in toenemende mate heeft gericht op de handhaving van de Wbp, is het ook gewenst dat het Cbp voorlichting en een mogelijkheid van een dialoog vooraf geeft over de verenigbaarheid van een bepaald product of bedrijfsproces met de bestaande privacywetgeving.

Het Cbp draagt tot nu toe met de volgende instrumenten bij aan verheldering van de Wbp:

1) Het Cbp geeft opinies uit samen met de andere Europese toezichthouders verenigd in de zogenaamde «artikel 29 Werkgroep», waarin uitleg wordt gegeven aan de normen uit de Europese richtlijn (zoals de opinie over mobiele app's in 2013);
2) het Cbp publiceert op verzoek van organisaties of bedrijven zienswijzen ten aanzien van maatschappelijke en technologische ontwikkelingen, indien deze ontwikkelingen leiden tot nieuwe rechtsvragen (bijvoorbeeld eenzienswijze over cloud computing in 2012); daarbij is het uiteraard wel de bedoeling dat het bedrijfsleven zelf het nodige vooronderzoek verricht. Het Cbp hanteert hierbij de voorwaarde dat het moet gaan om toepassingen die voor meer dan één bedrijf van

belang zijn en/of een grote maatschappelijk impact hebben. Ook deze zienswijzen worden op de website gepubliceerd;
3) Het Cbp geeft ook op eigen initiatief uitleg over hoe het de open normen uit de Wbp interpreteert in richtsnoeren. Voorbeelden hiervan zijn de richtsnoeren over identificatie en verificatie van persoonsgegevens in de private sector (2012) en de richtsnoeren beveiliging van persoonsgegevens (2013);
4) Het Cbp toetst op verzoek, voordat een organisatie (of een aantal organisaties samen) een eigen gedragscode uitbrengt een concept-gedragscode. Organisaties weten op die manier of hun gedragscode een juiste uitwerking is van de regels uit de Wbp.

Vermeldenswaard is ook de in te voeren verbetering van de websites van het Cbp (zoals: www.cbpweb.nl en www.mijnprivacy.nl). Toegankelijkheid en duidelijkheid van de beschikbare informatie zullen daarbij aandacht krijgen, waardoor een betere voorlichting en informatieverstrekking aan organisaties, bedrijven en gebruikers van online diensten, zal worden bereikt.

Het Cbp stelt bij de toepassing van bovengenoemde instrumenten als onafhankelijk college zijn eigen prioriteiten. Het kabinet is verheugd dat het Cbp sinds enige tijd weer regelmatig overleg voert met diverse maatschappelijke groeperingen. Dit overleg verdient voortzetting, gezien de behoefte daaraan vanuit het bedrijfsleven. Bij de communicatie naar het bedrijfsleven in den brede, dus ook met MKB, kunnen koepelorganisaties en ook het ECP (Electronic Commerce Platform) een nuttige rol vervullen.

Het kabinet acht het zinvol dat het bedrijfsleven en het Cbp met elkaar in overleg treden over het benutten van de mogelijkheden voor een dialoog en een optimale inzet van de instrumenten die de Wbp biedt in het kader van voorlichting en verheldering van de Wbp. Het spreekt voor zich dat deze activiteiten de rol van het Cbp waar het gaat om de handhaving onverlet laten. Een dergelijke benadering zal de effectiviteit van het toezicht kunnen vergroten.

3.3. Bewustwording en kwetsbare doelgroepen op sociale media

De huidige Wbp bevat in artikel 5 een leeftijdsgrens van 16 jaar voor het gebruik van persoonsgegevens van minderjarigen. De door de Europese Commissie voorgestelde Verordening bevat een leeftijdsgrens van 13 jaar voor het vereiste van ouderlijke toestemming bij de verwerking van persoonsgegevens, bij het aanbod van diensten van de informatiemaatschappij. De door de Europese Commissie voorgestelde leeftijdsgrens van 13 jaar sluit aan bij Amerikaanse wetgeving en de daarop gebaseerde gebruikersovereenkomsten van Amerikaanse aanbieders van sociale media, zoals Facebook. Dit betekent dat bij het aanmaken van een profiel van sociale media, de jeugdige eerst toestemming moet hebben van zijn wettelijke vertegenwoordiger (ouder/voogd).

Het Cbp heeft richtsnoeren gepubliceerd over de publicatie van persoonsgegevens op internet, waarin onder andere wordt ingegaan op de zorgplicht die aanbieders van sociale media hebben jegens kinderen. Kinderen dienen bij aanmelding te verklaren dat zij toestemming hebben van hun ouders om een profiel aan te maken. Bij enige twijfel aan de gegeven toestemming dient de verantwoordelijke nadere maatregelen te treffen om de toegang tot het profiel te blokkeren, totdat de verantwoordelijke zich heeft vergewist dat ouders daadwerkelijke hebben ingestemd met het maken van een profiel. De aanbieder dient verder als standaardin-

stelling te hanteren dat alleen zelfgekozen vrienden toegang hebben tot het profiel van de deelnemer[12].

Ook heeft de Europese Commissie een «Europese Strategie voor een beter internet voor kinderen»[13] voorgesteld, waarover de staatssecretaris van Buitenlandse Zaken uw Kamer bij brief van 8 juni 2012 (Kamerstuk 22 112, nr. 1425) berichtte. De Commissie beschrijft een palet aan maatregelen, waaronder filters en andere middelen voor ouderlijk toezicht op internetgebruik van kinderen en leeftijdsgebonden privacyinstellingen voor sociale media. Doel van het voorstel is dat kinderen in alle lidstaten veilig internet kunnen gebruiken en dat kindvriendelijke online producten en diensten zich op de interne markt gemakkelijker kunnen ontwikkelen. De Commissie bepleit een gecoördineerde aanpak binnen de EU, waarbij de Commissie, de lidstaten en het bedrijfsleven samenwerken.

Het kabinet ondersteunt de initiatieven van de Europese Commissie om te komen tot een gecoördineerde aanpak in de EU voor een veilig gebruik van internet door kinderen. De betrokken departementen zullen in samenwerking de uitvoering van de mededeling ter hand nemen. Hierbij gaat het om het vergroten van kennis over het gebruik van persoonsgevoelige data op social media. Dit past in de Europese Strategie voor een beter internet voor kinderen.

Op de website www.digibewust.nl worden verder verschillende brochures aangeboden die informatie bieden over specifieke onderwerpen met betrekking tot de veiligheid van kinderen op internet. Er is de website meldknop.nl, een initiatief van Digibewust en het Meldpunt Kinderporno waarbij minderjarigen informatie, hulp en advies wordt geboden wanneer zij iets vervelends meemaken op internet. Daarnaast zal in vervolg op de mededeling «Europese Strategie voor een beter internet voor kinderen» van de Europese Commissie de voorgestelde EU-verordening voorzien in privacy by default voor minderjarigen. Dat betekent aan de leeftijd aangepaste privacyinstellingen voor minderjarigen.

Voorts is het van belang dat de eindgebruiker zich bewust is wat er met zijn gegevens kan gebeuren en aan welke eisen een aanbieder van producten en/of diensten dient te voldoen. De bewustwording van de consument moet hand in hand gaan met transparantie van de kant van het bedrijfsleven dat op het internet opereert.

- Voor de bewustwording van de eindgebruiker zal het kabinet de succesvolle aanpak die het programma Digivaardig&Digiveilig de afgelopen jaren heeft gevolgd, intensiveren.

In het programma Digiveilig is gericht aandacht voor het MKB. Daarnaast is VNO-NCW/MKB-Nederland bezig een handzame tool voor het bedrijfsleven te ontwikkelen, die zich richt op bewustwording: de privacy-quickscan. Ondernemers kunnen online een aantal vragen invullen over hun situatie en krijgen direct advies over de risico's van hun verwerking van persoonsgegevens. Dat is een uitstekend initiatief.

- De privacy-quickscan wordt onder ondernemers verspreid via de programma's die er lopen bij het Agentschap NL en door opname ervan bij de informatievoorziening van de overheid naar bedrijven via «Antwoord voor Bedrijven».

---

[12] Vgl. beantwoording kamervragen van de leden Hilkens, Oosenbrug en Ypma door de Staatssecretaris van Veiligheid en Jusititie van 17 april 2013, Aanhangsel Handelingen II, 2012–2013, 1985.

[13] COM(2012) 196 final (Brussel, 2.5.2012)

3.4. Stimulering privacy impact assessment en privacy by design

Bedrijven zouden bij de ontwikkeling van hun producten en de inrichting van hun organisatie een privacy impact assessment moeten doen. Daarnaast dringt het kabinet er bij de organisaties op aan dat tijdens de ontwerpfase van nieuwe producten en diensten consequent gebruik gemaakt van privacy by design. Het gaat er daarbij in essentie om dat bedrijven in de ontwikkelingsfase van een product of dienst een goede bescherming van de persoonsgegevens van hun klanten opnemen. Organisaties moeten vervolgens hun klanten duidelijk maken hoe zij hun processen inrichten, en welke waarborgen en bescherming ingebouwd worden. Daarmee kunnen bedrijven invulling geven aan transparantie en de eigen verantwoordelijkheid die zij hebben voor de bescherming van de privacy van hun klanten.

In het nieuwe privacypakket van de Europese Commissie wordt privacy by design genoemd als een belangrijke ontwikkeling die gesteund moet worden. Uit het rapport «Stimulerende en remmende factoren van Privacy by Design in Nederland» dat TNO heeft uitgevoerd in opdracht van het toenmalige ministerie van EL&I[14], blijkt dat er voor bedrijven nog een aantal drempels is om privacy by design te omarmen.

- Het kabinet zal samen met het bedrijfsleven de best practices op het gebied van privacy impact assessment en privacy by design in kaart brengen, met ondersteuning van TNO en het PI lab. Het is vervolgens aan de organisaties van het bedrijfsleven om de *best practices* breed ingang te laten vinden bij de bedrijven.
- Reeds bestaande platforms zoals het Platform Internet Veiligheid zullen worden benut voor de uitwisseling van *best practices* op het gebied van privacy impact assessment en het ontwikkelen van een modelbenadering van privacy by design voor het bedrijfsleven. Dat kan uiteindelijk resulteren in door organisaties op te stellen gedragscodes die voor een reactie kunnen worden voorgelegd aan het Cbp. Op deze manier worden bedrijven en organisaties zich meer bewust van hun verantwoordelijkheid.
- De Rijksoverheid zal, als inkoper van relevante producten en diensten, de mogelijkheden benutten om het gebruik van privacy impact assessment en privacy by design door de leverancier op te nemen als eis bij aanbestedingstrajecten. Op die manier kan worden bevorderd dat privacyaspecten van de producten en diensten die de overheid zelf koopt vanaf de ontwerpfase worden meegenomen en kan een stimulans worden gegeven aan het bedrijfsleven om in deze ontwikkeling te investeren.

3.5. Cloud computing: internationale afspraken, bewustwording en keuze voor gebruikers

Zoals in de Digitale Agenda.nl is aangegeven, ziet het kabinet cloud computing als een belangrijke ontwikkeling om efficiënter en flexibeler te werken. Zo kunnen ondernemers en organisaties snel over nieuwe ICT-diensten beschikken zonder hoge investeringskosten. In de praktijk blijkt dat zowel bedrijven als eindgebruikers nog vele risico's op zich zien afkomen. Voor cloud computing loopt een publiekprivaat programma «Productiviteit en Cloud Computing» als onderdeel van de Digitale Agenda.nl. In dit tweejarig programma is gekozen om – in relatie tot privacy- transparantie en bewustwording te verbeteren, zodat (bewust) gebruik van cloud computing toeneemt. Dit zal samen met betrokkenen, met name gericht op het MKB, worden uitgewerkt. Omdat cloud

[14] «Stimulerende en remmende factoren van Privacy by Design in Nederland» TNO (mei 2012). Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

computing een grensoverschrijdend onderwerp is, zijn afspraken en aanpak vooral in EU verband essentieel.
- In relatie tot privacy wordt samen met de branche voor het MKB een website gemaakt over cloud computing, waarmee ondernemers onder meer bewust worden gemaakt van de privacyrisico's, en van de kansen die deze technologie biedt.

Aangezien er geen barrières bestaan die grensoverschrijdende cloud-diensten tegenhouden, is de internationale dialoog van cruciaal belang om ook buiten de EU de privacy te beschermen. In reactie op de EU-strategie is aangeven dat nog meer zou kunnen worden ingegaan op de vraag of de voorgestelde EU-Verordening instrumenten bevat die toereikend zijn voor bescherming van persoonsgegevens in een cloud-omgeving.

4. Monitoring

Het kabinet zal dit jaar in kaart brengen hoe het nu is gesteld met het vertrouwen in de bescherming van de persoonsgegevens en het vertrouwen in online-diensten. Daarbij zal zoveel mogelijk worden aangesloten bij de reeds bestaande monitors. Over twee à drie jaar zal worden gemeten wat het effect is geweest van de hierboven genoemde acties.
De digitale markt is een dynamische markt met veel innovaties, waarbij op voorhand niet is aan te geven welke gevolgen ontwikkelingen zullen hebben voor de privacy en welke consequenties daar aan moeten worden verbonden. Daarom zal het kabinet de ontwikkelingen op deze markt nauwgezet blijven volgen en overleg met de sector houden om, mocht dat nodig zijn, bij te kunnen sturen om ervoor te zorgen dat persoonsgegevens adequaat zijn beschermd binnen de randvoorwaarden die zijn geformuleerd.

5. Tot slot

In Nederland worden steeds meer innovatieve online diensten ontwikkeld. Eindgebruikers maken daarvan dankbaar gebruik, en stellen voor het gebruik hun persoonsgegevens ter beschikking. Deze persoonsgegevens vertegenwoordigen een aanzienlijke financiële waarde voor online dienstenaanbieders. Helaas worden persoonsgegevens niet altijd optimaal beschermd, en ontstaat er zorg over de bescherming van persoonsgegevens en het vertrouwen van de gebruikers in online-diensten. Het kabinet gaat een gerechtvaardig digitaal vertrouwen bevorderen en daarmee een impuls geven aan economische groei.

Bescherming van persoonsgegevens online is een internationale aangelegenheid. Om effectief te zijn, zullen veel regels internationaal moeten werken. Het kabinet zal zich dan ook sterk maken voor internationale wetgeving op het gebied van privacy. Aanvullend daarop wil het kabinet ook maatregelen treffen die bijdragen aan een goede bescherming van de consument waarbij ook volop ruimte blijft voor innovatie. Er is daarbij nadrukkelijk ook een rol voor het bedrijfsleven weggelegd. Het kabinet wil dan ook samen met het bedrijfsleven komen tot de invulling van maatregelen. In de brief is aangegeven wat het kabinet op korte termijn zal gaan doen.

Daarbij kan het niet blijven. Zoals gezegd staan de ontwikkelingen niet stil. Dat zal betekenen dat de komende jaren goed zal worden gevolgd of de wetgeving en de overige maatregelen nog de gewenste online privacybescherming bieden aan de consument en voldoende ruimte bieden voor innovatie.

Daarnaast geldt onverkort dat het betrokken bedrijfsleven en de burgers ook een eigen verantwoordelijkheid dragen voor een zorgvuldige omgang met persoonsgegevens.

De Minister van Economische Zaken,
H.G.J. Kamp