Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

26 643 Informatie- en communicatietechnologie (ICT)

32 761 Verwerking en bescherming persoonsgegevens

Nr. 537

AAN DE VOORZITTER VAN DE TWEEDE KAMER DER STATEN-GENERAAL

Den Haag, 24 mei 2018

Tijdens de Regeling van Werkzaamheden in uw Kamer op 12 april jl. (Handelingen II 2017/18, nr. 73, item 6) is mij gevraagd om een reactie op het bericht «Verzekeraars sturen surfgedrag naar Facebook, ook van medische pagina's» op NOS.nl.[1] Door leden van uw Kamer is meer in het bijzonder gevraagd om een reactie op de verdienmodellen die de grote socialmediabedrijven en techplatforms ontwikkelen en op wat er in het geval waarop eerder genoemd bericht betrekking heeft, precies is gebeurd, wat er met de gegevens gedaan kan worden en daarbij niet alleen naar zorgverzekeraars te kijken, maar ook naar ziekenhuizen. In deze brief geef ik graag mede namens de Minister voor Medische Zorg en Sport een reactie op een en ander.

Op 30 mei vindt een AO over «Big data en de bescherming van persoonsgegevens» plaats. Met het oog op dat AO geef ik uw Kamer in deze brief ook een overzicht van de stand van zaken bij de uitvoering van de actiepunten uit een brief die voor dat AO is geagendeerd, te weten het kabinetsstandpunt over het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) «Big Data in een vrije en veilige samenleving».[2]

Kort voor het AO zal ik een gesprek hebben met vertegenwoordigers van een aantal bedrijven die zich met Big Data bezighouden, en van VNO/NCW, waarin ik een beter beeld wil krijgen van de maatregelen die bedrijven als gevolg van de Algemene verordening gegevensbescherming hebben getroffen of nog zullen treffen met het oog op de bescherming van persoonsgegevens. Over de uitkomst van dit gesprek zal ik u informeren tijdens het AO. Dat gesprek zal ik ook benutten voor de voorbereiding van de door mij toegezegde visie op de bescherming van de horizontale privacy.[3] Overigens wil ik in die visie ook de voorstellen betrekken uit de initiatiefnota «Onderlinge privacy» die het lid van uw

[1] Nos.nl, 11 april 2018.
[2] Kamerstukken 26 643 en 32 761, nr. 426.
[3] Handelingen II 2017/18, nr. 30, item 4.

kst-26643-537
ISSN 0921 - 7371
's-Gravenhage 2018

Kamer Koopmans onlangs heeft uitgebracht.[4] In verband daarmee zal ik deze visie niet al dit voorjaar uitbrengen, maar pas in het najaar.

Social media en de bescherming van persoonsgegevens

Socialmediabedrijven hebben een groot scala aan producten ontwikkeld waarmee ze in combinatie met door hen verzamelde gegevens geld verdienen. Verschillende van die producten zijn gericht op *microtargeting*. Dit is een proces waarin online gericht wordt geadverteerd op basis van analyses van persoonsgegevens waarmee de interesses van een specifiek individu of van een specifiek publiek worden blootgelegd met het oogmerk hun (koop)gedrag te beïnvloeden. Microtargeting kan worden gebruikt om gepersonaliseerde advertenties te plaatsen op sites van digitale diensten, waaronder social media, die iemand bezoekt. Voor adverteerders heeft dit het voordeel dat advertenties meer effect hebben dan in het geval dat zij ongericht adverteren.

Voor microtargeting worden verschillende tools gebruikt, zoals *cookies*[5], *social plug-ins*[6] en *tracking pixels*[7]. Deze tools leggen het *browsen*, het plaatsen van *likes* en de sociale interactie op internet vast om daarmee profielen van individuele personen of groepen van personen op te bouwen. Op basis van deze profielen kunnen adverteerders dan gericht advertenties plaatsen. Socialmediabedrijven kunnen dergelijke tools op hun eigen platforms plaatsen, maar ook op websites van andere bedrijven en organisaties die geïnteresseerd zijn in het voor hen relevante gedrag van personen die hun site bezoeken.[8]

Daarnaast kennen verschillende social media de functie om met behulp van een persoonlijk account in te loggen op apps van andere bedrijven en organisaties. Deze bedrijven en organisaties kunnen dan, afhankelijk van het contract met de betrokken socialmediabedrijven, toegang krijgen tot (een deel van) de data van de gebruikers van deze social media.[9]

Een product dat hier tot slot wordt genoemd, is het uploaden van klantenlijsten naar socialmediabedrijven om deze lijsten te combineren met data die deze bedrijven hebben. Het bedrijf dat haar klantenbestand uploadt, kan dat bestand eerst *hashen* (vorm van pseudonimiseren), voordat het naar het socialmediabedrijf wordt gestuurd. In dat geval worden de persoonsgegevens uit het bestand gecodeerd. Vervolgens wordt het gecodeerde bestand gekoppeld aan een bestand van het socialmediabedrijf met de gehashte identificaties van de gebruikers van de social media van dat bedrijf. Op basis van deze koppeling is het mogelijk om gepersonaliseerde advertenties toe te zenden.[10]

Hoeveel geld socialmediabedrijven op deze wijze verdienen, verschilt uiteraard per bedrijf. Als we kijken naar wat Facebook ieder kwartaal per

---

[4] Kamerstuk 34 926, nrs. 1–2.
[5] Tekstbestand op een website waarmee bezoekers van de site kunnen worden gevolgd.
[6] Zichtbaar op een website geplaatste icoon die een koppeling tot stand brengt tussen het bezoek aan de site en het desbetreffende social medium.
[7] Op een website aangebrachte onzichtbare voorziening waarmee het bezoek aan de site kan worden gevolgd.
[8] https://dataprotection.ie/documents/PandAPrefs.pdf.
[9] https://www.trouw.nl/samenleving/de-tentakels-van-facebook-reiken-veel-verder-dan-zijzelf-weten~a91a83ff/.
[10] https://www.nrc.nl/nieuws/2016/03/01/zo-verdient-facebook-geld-aan-gebruikers-1592441-a715864. https://nl-nl.facebook.com/business/help/112061095610075.

Europese gebruiker verdient, komt dit uit op een bedrag van gemiddeld 8,01 dollar, gemeten naar het eerste kwartaal van 2018.[11]

In het geval waarop het bericht «Verzekeraars sturen surfgedrag naar Facebook, ook van medische pagina's» betrekking heeft, ging het om het gebruik van *tracking pixels*. Bedrijven kunnen op hun website een onzichtbare pixel-plug-in installeren om te laten meten wat mensen op hun websites doen. In dit geval ging het om een *plug-in* van Facebook. Dat bedrijf kan met deze plug-in het surfgedrag van mensen die de desbetreffende sites bezoeken, koppelen aan het Facebook-account, als die persoon is ingelogd. Wie niet is ingelogd of geen Facebook-account heeft, kan ook worden gevolgd, al weet Facebook dan niet exact om wie het gaat.[12] In beide gevallen kan Facebook gepersonaliseerde advertenties laten zien op de Facebookpagina's van de betrokken mensen of op geselecteerde sites van andere bedrijven of organisaties.

Uit het aangehaalde bericht blijkt dat van de onderzochte zorgverzekeraars er achttien tracking-pixels gebruikten. Daarvan gebruikten er elf de pixel-plug-in op een pagina waarop medische informatie wordt getoond. Ook het Diakonessenziekenhuis in Utrecht bleek een pixel-plug-in te gebruiken. Of andere ziekenhuizen een dergelijke plug-in gebruiken, is niet bekend. Voor zover ik weet hebben de meeste zorgverzekeraars en het Diakonessenziekenhuis in Utrecht het gebruik van de Facebook-pixel-plug-in inmiddels gestopt. Van belang is vooral dat, voor zover mij bekend, geen enkele zorgverzekeraar nog gebruik maakt van de pixel-plug-ins op pagina's waarop medische informatie staat. Bij navraag bij de Nederlandse Vereniging van Ziekenhuizen (NVZ) bleek dat zij dit onderwerp al specifiek onder de aandacht van de security officers van haar leden heeft gebracht. Overigens blijken ook andere bedrijven en organisaties, zoals winkels, media en politieke partijen, tracking-pixels te gebruiken.[13] Zo'n vijftien tot twintig procent van de websites zou hiervan gebruik maken.[14]

Het gebruik van genoemde tools gaat gepaard met de verwerking van persoonsgegevens. Het gebruik daarvan behoeft overigens op zich niet onrechtmatig te zijn. Wil de daarmee gepaard gaande verwerking van persoonsgegevens rechtmatig zijn, dan dient de verwerkingsverantwoordelijke daarvoor een grondslag te hebben als bedoeld artikel 8 van de Wet bescherming persoonsgegevens (Wbp) en vanaf 25 mei a.s. artikel 6 van de Algemene verordening gegevensbescherming (AVG). In dit geval lijkt toestemming van degene wiens surfgedrag wordt gemonitord, als grondslag het meest voor de hand te liggen (zie artikel 6, eerste lid, onder a, AVG).

In dat verband is van belang dat de AVG nieuwe, strengere eisen aan toestemming als grond voor verwerking van persoonsgegevens stelt dan de Wbp. Het gaat om onder meer de volgende eisen:

- De toestemming moet actief worden gegeven. Dat betekent dat stilzwijgen of inactiviteit niet geldt als toestemming. Ook reeds vooraf aangekruiste vakjes gelden niet als toestemming.

---

[11] https://s21.q4cdn.com/399680738/files/doc_financials/2018/Q1/Q1-2018-Earnings-Presentation-(1).pdf.

[12] https://nos.nl/artikel/2226902-verzekeraars-sturen-surfgedrag-naar-facebook-ook-van-medische-pagina-s.html.

[13] https://nos.nl/artikel/2226957-aantal-zorgsites-stopt-met-tracking-pixel-van-facebook.html. NRC Next 13 april 2018, p. 8.

[14] https://www.trouw.nl/home/facebook-weet-ook-veel-over-niet-gebruikers~a3ad118a/.

- De vraag om toestemming moet specifiek betrekking hebben op de gegevensverwerking en mag niet worden verstopt in de kleine lettertjes van een document over andere aangelegenheden.

Als burgers menen dat hun persoonsgegevens onrechtmatig worden verwerkt, kunnen zij een klacht bij de AP indienen. De AP is vanaf 25 mei 2018 verplicht om elke klacht in behandeling te nemen. Indien de AP oordeelt dat er sprake is geweest van onrechtmatige verwerking van iemands persoonsgegevens, dan kan zij hoge boetes opleggen (oplopend tot 20 miljoen euro of 4% van de totale wereldwijde jaaromzet). Dat een bedrijf zijn hoofdvestiging in bijvoorbeeld de Verenigde Staten heeft, doet hieraan niet af. De AVG is niet alleen van toepassing op bedrijven die binnen de EU zijn gevestigd, maar ook op bedrijven die buiten de EU zijn gevestigd, namelijk bij het verwerken van persoonsgegevens in verband met het aanbieden van diensten of goederen aan burgers in de EU.

Het oordeel of in het onderhavige geval al dan niet sprake is van onrechtmatige verwerking van persoonsgegevens is aan de AP. Zij is volledig onafhankelijk en bepaalt als gevolg daarvan bij het uitoefenen van toezicht zelf haar prioriteiten. Als een partij het niet eens is met het oordeel van de AP, kan zij desgewenst naar de rechter stappen. Overigens heeft een woordvoerder van de AP al laten weten dat de verwerking van persoonsgegevens in het geval waarop het bericht betrekking heeft, niet in orde lijkt. «Voor elke verwerking van gegevens moet je een fatsoenlijke grondslag hebben en die lijkt er niet te zijn» aldus deze woordvoerder. Of de AP op dit punt actief gaat handhaven, blijft in het midden.[15]

Los van de juridische merites van dit geval meen ik dat bedrijven goed moeten nadenken of zij voor marketingdoeleinden pixel-plug-ins willen gebruiken en hoe zij dat doen. Dat geldt zeker in het geval dat dergelijke plug-ins worden geplaatst op pagina's van een website van een zorgaanbieder waarop de vergoedingen voor de behandeling van bepaalde medische kwalen of anderszins medische informatie staan. Het surfen naar dergelijke pagina's zou immers iets kunnen zeggen over de gezondheid van betrokkenen en daarmee gevoelige informatie opleveren. Het doet mij om die reden deugd dat de zorgverzekeraars die gebruik maakten van de pixel-plug-ins op medische pagina's deze hebben verwijderd. Voor zover mij bekend hebben de meeste zorgverzekeraars – naast pixel-plug-ins op pagina's waar medische informatie staat – tevens pixel-plug-ins op algemene pagina's (tijdelijk) verwijderd. Alle bedrijven die gebruik maken van pixel-plug-ins op webpagina's met medische informatie wil ik oproepen hier nog eens kritisch naar te kijken.

Naar aanleiding van de gebeurtenissen rond Cambridge Analytica en Facebook zal een werkgroep van de samenwerkende Europese privacytoezichthouders gaan bekijken hoe social media-platformen aan hun gegevens komen en hoe ze voorkomen dat anderen daar onrechtmatig toegang toe hebben. De AP wil een actieve rol spelen in deze werkgroep. De werkgroep zal in Europees verband ook een langetermijnstrategie ontwikkelen voor het gebruik van persoonsgegevens door social media. Zij zal niet alleen naar social media kijken, maar ook naar andere partijen als datahandelaren en app-ontwikkelaars.[16] Ik verwacht dat het rapport van de werkgroep onder meer betekenis zal hebben voor het gebruik van plug-ins door socialmediabedrijven. Mede om deze reden kijk ik met

---

[15] https://nos.nl/artikel/2227026-zorgverzekeraars-overtraden-waarschijnlijk-de-wet-met-trackers.html.

[16] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=621779. https://autoriteitpersoonsgegevens.nl/nl/nieuws/europese-privacytoezichthouders-trekken-samen-op-aanpak-social-media.

belangstelling uit naar de langetermijnstrategie die deze werkgroep zal opleveren.

Big Data en de bescherming van persoonsgegevens

In zijn brief van 11 november 2016 heeft het vorige kabinet naar aanleiding van het WRR-rapport «Big Data in een vrije en veilige samenleving» de volgende kernboodschap opgenomen:
«Big Data biedt veel kansen om de veiligheid te bevorderen. Om deze kansen te benutten dient er voldoende ruimte te zijn om de toegevoegde waarde van Big Data verder te verkennen. Big Data laat ook risico's zien. Daarom zal het experimenteren en benutten van Big Data gepaard moeten gaan met voldoende waarborgen waarin bescherming van de privacy en persoonsgegevens, het verbod van discriminatie, transparantie en de betrouwbaarheid van zowel data als analysemethoden centraal staan. Zo kan worden bereikt dat er voldoende vertrouwen bij de burgers ontstaat in de wijze waarop de overheid de mogelijkheden van Big Data in het veiligheidsdomein benut.»

Ik meen dat deze kernboodschap niets aan betekenis heeft ingeboet. Ik onderschrijf daarbij de beleidsuitgangspunten die in de kabinetsbrief van 2016 zijn opgenomen. Daarbij denk ik in het bijzonder aan het uitgangspunt dat de te analyseren data *up to date* zijn, datasets een zo gering mogelijke *bias* bevatten en te gebruiken algoritmen en methoden deugdelijk zijn.

Het kabinetsstandpunt bevat ook een aantal actiepunten. Een overzicht van de stand van zaken bij de uitvoering daarvan en de verdere planning is opgenomen in een bijlage bij deze brief. Een aantal van de producten die uit deze actiepunten voortvloeien, zullen toegankelijk worden gemaakt door plaatsing in een zgn. Big Data Toolbox op rijksoverheid.nl. In deze Toolbox, die nog in ontwikkeling is, zullen verder onder meer de volgende producten worden opgenomen: een Factsheet Big Data[17], een overzicht van tien uitgangspunten voor experimenteren met Big Data[18], een modelverwerkersovereenkomst, een aanvulling op het Model GEB Rijkdienst (PIA) met privacy-aandachtspunten voor Big Data verwerkingen, alsmede een set richtlijnen om toezichthouders en rechters inzicht te kunnen verschaffen in gebruikte algoritmen. Deze producten zijn ontwikkeld om de kwaliteit van Big Data toepassingen bij de rijksoverheid te bevorderen. Het gebruik van de instrumenten uit deze Toolbox kan aldus bijdragen aan een verantwoorde toepassing van Big Data door de rijksoverheid, die van essentieel belang is voor het vertrouwen dat burgers in dergelijke toepassingen dienen te hebben.

De Minister voor Rechtsbescherming,
S. Dekker

[17] Al toegankelijk via: https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/documenten/publicaties/2018/04/20/big-data-factsheet.
[18] Al toegankelijk via: https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/documenten/publicaties/2018/04/20/handreiking-open-data-in-10-stappen.

Bijlage

Overzicht stand van zaken en planning uitvoering Kabinetsstandpunt over WRR-rapport «Big Data in een vrije en veilige samenleving»

Actiepunten	Stand van zaken	Planning
1. Heldere wettelijke basis. Het kabinet zal bezien of de wettelijke basis voor het uitvoeren en gebruiken van data-analyses versterking behoeft, met inbegrip van de waarborgen die daarbij gehanteerd dienen te worden.	Een werkgroep bereidt voor: 1. een generieke bepaling in de Uitvoeringswet AVG over geautomatiseerde verwerking van persoonsgegevens op basis van profilering; 2. een aanwijzing voor de regelgeving met eisen aan profilering in sectorale wetten.	Gereed: tweede helft 2018.
2. Inzicht in algoritmen. Het kabinet zal onderzoeken hoe voor toezicht en rechterlijke toetsing voldoende inzicht kan worden gegeven in gebruikte algoritmen en analysemethoden, met name voor situaties waarin besluitvorming op basis van een Big Data analyse rechtsgevolgen of anderszins een aanmerkelijke impact op burgers heeft.	Een werkgroep heeft een concept-circulaire «Inzicht in algoritmen» opgesteld, die na vaststelling in een *Big Data Toolbox* op rijksoverheid.nl zal worden opgenomen.	Gereed: eerste helft 2018. Circulaire zal daarna periodiek worden aangepast aan technologische ontwikkelingen.
3. Inzicht in algoritmen. Het kabinet zal onderzoeken of het mogelijk is dat bij ICT-overheidsaanbestedingen kan worden vereist dat de meedingende aanbieders algoritmen die worden ingebouwd in de software, voldoende inzichtelijk maken voor in elk geval de toezichthouder en voor de rechter.	De Interdepartementale Commissie Bedrijfsjuridisch Advies ziet in de aanbestedingspraktijk geen aanleiding om de ARBIT uit te breiden met een bepaling over inzicht in algoritmen, omdat de behoefte daaraan op dit moment te beperkt is om opneming in algemene voorwaarden te rechtvaardigen. Overigens staat het de aanbestedende dienst vrij eisen te stellen aan het inzicht dat door opdrachtnemer wordt geboden in de gehanteerde algoritmen voor zover dat inzicht noodzakelijk is om daarop gebaseerde besluitvorming voldoende inzichtelijk te maken voor de toezichthouder en de rechter.	Al gereed.
4. Aanpassing toetsmodel PIA. Als een PIA dient plaats te vinden, ligt het voor de hand daarin ook een verantwoording van de gemaakte keuzes inzake data en methode van analyse op te nemen. Bij de komende aanpassing van het huidige toetsmodel PIA Rijksdienst zal worden bezien op welke wijze deze elementen van Big Data verwerkingen een plaats kunnen krijgen in het toetsmodel.	In september 2017 is een Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA) vastgesteld die in de toelichting op de punten 8 en 17 specifieke elementen met betrekking tot Big Data bevat.	Al gereed.
5. Implementatiewet Richtlijn. De AVG schrijft voor dat, indien nodig, de verwerkingsverantwoordelijke toetst of de verwerking overeenkomstig de PIA wordt uitgevoerd. Een hiermee vergelijkbare bepaling ontbreekt in de Richtlijn. Bij de implementatie van de Richtlijn zal worden bezien of een dergelijke bepaling niettemin in de implementatiewetgeving dient te worden opgenomen.	Bepaling is opgenomen in artikel 4c, derde lid, Wpg en artikel 7b, derde lid, Wjsg, zoals voorgesteld in het wetsvoorstel tot wijziging van de Wpg en Wjsg ter implementatie van de Richtlijn gegevensbescherming opsporing en vervolging.	Al gereed.
6. Rechtspraak. Het kabinet zal de Raad voor de rechtspraak verzoeken zich te oriënteren op de kennis die nodig zal zijn om rechtszaken te kunnen behandelen waarbij Big Data analyses een rol spelen.	In een mail aan de Raad voor de rechtspraak is hier aandacht voor gevraagd.	Al gereed.
7. Autoriteit Persoonsgegevens. VenJ en de Autoriteit Persoonsgegevens zijn een traject gestart waarin een onafhankelijk adviesbureau de consequenties in kaart brengt van de versteviging van bevoegdheden en middelen van de Autoriteit door de AVG voor de capaciteit en het budget van dit college.	Met het oog op de komst van de AVG wordt het budget van de AP met 7 mln euro vermeerderd tot 15 mln euro.	Al gereed.
8. Transparantie. Om voor meer transparantie rond Big Data analyses door overheidsdiensten te zorgen, zal het kabinet stimuleren dat deze diensten op hun websites informatie opnemen over het doel van analyses die zij uitvoeren, en de databestanden die daarvoor worden gebruikt.	Een werkgroep bereidt richtlijnen voor publiekvoorlichting over Big Data analyses door de overheid voor, die in de *Big Data Toolbox* (zie 2) zullen worden opgenomen.	Gereed: derde kwartaal 2018.

Actiepunten	Stand van zaken	Planning
9. Implementatiewet Richtlijn. In artikel 14, tweede lid, onder g, AVG, is vastgelegd dat betrokkenen recht hebben op informatie over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene. Een equivalent van genoemde bepaling uit de AVG ontbreekt in de Richtlijn. In het kader van de implementatie daarvan zal worden bezien of een bepaling als deze niet ook voor geautomatiseerde besluitvorming op grond van strafrechtelijke gegevens zou moeten gaan gelden.	Bepaling is opgenomen in artikel 24b, tweede lid, onder e, Wpg en artikel 17b, derde lid, onder e, Wjsg, zoals voorgesteld in het wetsvoorstel tot wijziging van de Wpg en Wjsg ter implementatie van de Richtlijn gegevensbescherming opsporing en vervolging.	Al gereed.
10. Rechterlijke toetsing. Het kabinet zal onderzoeken of uitbreiding van de mogelijkheden voor burgers en belangenorganisaties om zich voor een toetsing van Big Data toepassingen tot de rechter te wenden mogelijk en wenselijk is.	Het onderzoek is door het WODC uitbesteed aan de Universiteit Tilburg.	Gereed: tweede helft 2018.
11. Bevorderen van experimenten. Het kabinet zal binnen de kaders van de huidige en toekomstige wetgeving inzake gegevensbescherming experimenten met Big Data in het veiligheidsdomein starten c.q. voortzetten. Bij deze experimenten zullen de geformuleerde beleidsuitgangspunten leidend zijn en, zo nodig, verder worden uitgewerkt.	Er worden aan de hand van toetsingskaders, ontleend aan de beleidsuitgangspunten, experimenten uitgevoerd in het kader van: 1. het Living Lab Big Data JenV, 2. de City Deal Zicht op ondermijning.	Uitgevoerd: 1/1/2019. Daarna mogelijk doorstart in structurele zin.
12. Implementatie bij rijksoverheid. Om tot voldoende inbedding van de door het kabinet geformuleerde beleidsuitgangspunten binnen de rijksoverheid te komen zal het kabinet ervoor zorgen dat deze worden toegelicht en besproken in in ieder geval het CIO-beraad van het Rijk. De verschillende departementen zullen, via hun CIO's of andere bestaande structuren, er vervolgens voor zorgen dat deze uitgangspunten binnen hun domein in voldoende mate worden verankerd en, voor zover nodig, verder worden uitgewerkt in samenhang met het reguliere beleid, de uitvoering en de handhaving.	De beleidsuitgangspunten zijn besproken in het CIO-beraad Rijk van 3 mei 2017. Dit heeft tot oprichting van de interdepartementale kennisgroep Big Data geleid, die de departementen ondersteunt bij de toepassing van de beleidsuitgangspunten.	Kennisgroep voert periodiek overleg.
13. Implementatie bij andere overheden. Het kabinet zal in overleg met de VNG en het IPO treden om gezamenlijk te bezien in hoeverre de hiervóór geformuleerde beleidsuitgangspunten ook binnen de andere overheden kunnen worden ingebed.	Met uitvoering van dit actiepunt wordt gewacht totdat de uitvoering van de overige actiepunten, m.n. de actiepunten 2 en 8, is voltooid.	Nader te bepalen.
14. Dialoog. Het kabinet zal de dialoog met organisaties die het privacybelang behartigen, over de wijze waarop de overheid de kansen van Big Data wil benutten en over de normen en principes die zij daarbij hanteert, voortzetten en verder versterken.	De dialoog vindt plaats in het kader van minisymposia over Big Data. Symposia zijn gehouden op 29 juni en 7 december 2017 over transparantie, respectievelijk experimenten.	Het eerstvolgende symposium vindt plaats op 7 juni 2018 over datakwaliteit.