Big data, data analytics en privacy: Het creëren van 'shared value'

'With maturity of trust comes greater value'

Monique van Dijken Eeuwijk

SAMENVATTING *'With maturity of trust comes greater value'*. Alleen wanneer er vertrouwen is in de maat-schappij in de wijze waarop data wordt gebruikt door ondernemingen, zo ook door accountantsorganisaties en -kantoren, in wat zij 'beloven' ten aanzien van privacy, is het mogelijk om de potentie van big data en de ontsluiting daarvan door data analytics volledig uit te nutten en waarde te creëren; om '*shared value*' te creëren. Vertrouwen is ook de *key essential* van het accountantsberoep. Nog niet alle vraagstukken met betrekking tot privacy en big data/data analytics zijn beantwoord, zeker niet op de scheidslijn van de wettelijke kaders en de mogelijkheden van de techniek. Batig aan het (bouwen aan) vertrouwen zijn *Privacy Impact Assessments*, toepassing van *Privacy by Design* en het acteren op de verwachtingen van de stakeholders van de onderneming. Transparantie en de overtuiging dat de onderneming '*keeps to its promisses*' is daarbij essentieel.

RELEVANTIE VOOR DE PRAKTIJK Big data en data analytics *are here and here to stay.* In dit verband en om daadwerkelijk *shared value* te bewerkstelligen, is het interessant om te bezien welke aanvullende maatregelen kunnen leiden tot waarborgen om de persoonlijke levenssfeer en persoonsgegevens van individuen te beschermen en tegelijkertijd risico's verbonden aan de privacy van individuen te mitigeren en de kansen die big data en data analytics bieden niet (volledig) teniet te doen.

1 Inleiding

'With maturity of trust comes greater value'. Alleen wanneer er vertrouwen is in de maatschappij in de wijze waarop data wordt gebruikt door ondernemingen, zo ook door accountantsorganisaties en -kantoren, in wat zij 'beloven' ten aanzien van privacy, is het, naar mijn overtuiging, mogelijk om de potentie van big data[1] en de ontsluiting daarvan door data analytics[2] volledig uit te nutten en waarde te creëren; om '*shared value*'[3] te creëren. Vertrouwen staat ook centraal in de kabinetsvisie ePrivacy (Ministerie van Economische Zaken, 2013). Vertrouwen is ook de *key essential* van het accountantsberoep; immers de kerntaak van de accountant is het verschaffen van zekerheid (Klijnsmit, Sodekamp en Wallage, 2003, p. 190). En om vertrouwen te kunnen verschaffen, moet je allereerst zelf vertrouwd worden. Iets waarbij in het voorwoord (Eimers en Van Nieuw Amerongen, 2015) aangehaalde rapport van de accountancysector *'In het Publieke Belang: Maatregelen ter verbetering van de kwaliteit en onafhankelijkheid van de accountantscontrole'* (Werkgroep Toekomst Accountantsberoep, 2015) uitgebreid wordt stilgestaan. Dit rapport demonstreert dat de sector zich terdege bewust is van het feit dat vertrouwen essentieel is en dat vertrouwen de voorwaarde is voor het creëren van *shared value*: *"Do you do what you have promised to your stakeholders?"* Het is deze uitspraak die de essentie weergeeft van waardecreatie, het moderne winstbegrip. Strategie staat van oudsher voor de financiële winst (waarde) die de onderneming creëert voor haar aandeelhouders. Waardecreatie staat voor de waarde die wordt gegenereerd voor alle stakeholders. Waardecreatie veronderstelt dus een direct verband tussen de (uitvoering van de) strategie en (het voldoen aan) de verwachtingen van de stakeholders. Dus waar privacy en het tegelijkertijd volledig uitnutten van de potentie van big data en data analytics innerlijk tegenstrijdig lijken dan wel zo worden gepercipieerd, namelijk het economisch belang vis-a-vis het belang van de bescherming van de persoonlijke levenssfeer, creëren beiden waarde voor de onderneming, voor haar respectievelijke stakeholders, maar alleen dan wanneer het vertrouwen wordt gehonoreerd.

Voor de ontwikkeling van big data en data analytics-toepassingen wordt het belang van vertrouwen alleen maar groter. Bij big data en data analytics leidt de grote schaal waarop gegevens worden verzameld en verwerkt tot nieuwe toepassingen, nieuwe inzichten en nieuwe vormen van impact op ons als individu. Daarom worden controle, transparantie en verantwoordelijkheid van ondernemingen in de kabinetsvisie genoemd als randvoorwaarden voor het verkrijgen en het behouden van het benodigde vertrouwen; de *'required trust'*. Ik kom hier later in deze bijdrage nog op terug.

Een belangrijke vraag die rijst bij big data en data analytics is of de huidige juridische kaders nog aansluiten op de huidige stand en snelheid van ontwikkelingen van de techniek en vervolgens of de risico's verbonden aan big data en data analytics kunnen worden gemitigeerd om een optimale waardecreatie voor alle stakeholders door ondernemingen vanuit big data en data analytics te stimuleren en realiseren. Daar zal ik in dit artikel nader op ingaan. Allereerst bespreek ik welke eigenschappen van big data en data analytics de huidige wettelijke kaders ten aanzien van de bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens op de proef stellen (paragraaf 2). Ik duid het wetgevend kader (paragraaf 3) en correleer dat aan de volgende drie essentiële onderdelen van het big data/data analytics-proces: (i) het verzamelen van gegevens, (ii) het analyseren van gegevens en (iii) het vervolgens toepassen van de uitkomsten van deze analyses (paragraaf 4). Ik sta stil bij de risico's verbonden aan big data en data analytics om daarna in te zoomen op de rol van eigenaarschap en accountability[4] (van transparantie, controle en verantwoordelijkheid) van ondernemingen waar het gaat om het waarborgen van privacy en het bewerkstelligen van de *required trust* (paragraaf 5). Ik rond af met enkele aanbevelingen om de privacy te borgen en tegelijkertijd ondernemingen in staat te stellen de economische waarde van big data te ontsluiten en zo op beide vlakken waarde te creëren voor al hun stakeholders. *'Building trust is creating shared value'* (Porter & Kramer, 2011) (paragraaf 6).

2 Enkele eigenschappen van big data '*challenging*' privacy.

2.1 Proportionaliteit/dataminimalisatie

Op grond van privacywet- en regelgeving moet de verwerking van persoonsgegevens[5] beperkt blijven tot datgene wat minimaal nodig is voor het vooraf bepaalde specifieke doel. Persoonsgegevens mogen bovendien niet langer bewaard worden dan noodzakelijk voor de realisatie van dat doel. Deze beginselen van dataminimalisatie, die al met zoveel woorden in de Privacy Richtlijn (95/46/EG)[6] en de Wet bescherming persoonsgegevens ('Wbp')[7] stonden en nu worden opgenomen in de aanstaande Data Protection Verordening (COM(2012) 11 final)[8] (zie hierna), dwingen ondernemingen verantwoordelijk voor de verwerking van gegevens om kritisch(er) te kijken naar de persoonsgegevens die worden verzameld, verwerkt en bewaard. Minimale gegevensverwerking (dataminimalisatie) is op zichzelf een goed uitgangspunt; wat je als onderneming niet verzamelt kun je ook niet gebruiken, kun je niet verliezen, kun je niet aan derden verstrekken. Door *excessive data* niet vast te leggen wordt bovendien voorkomen dat data die in eerste aanleg anoniem leek, op een later moment alsnog wordt herleid tot een persoon en daarmee onderwerp wordt van wet- en regelgeving terzake de bescherming van persoonsgegevens, en wellicht tevens van wet- en regelgeving terzake de bescherming van de persoonlijke levenssfeer van individuen. Dit *to the extent* dat de nieuw gegenereerde persoonsgegevens (mogelijk) consequenties hebben voor de persoonlijke levenssfeer van het individu. De vraag die hierbij natuurlijk opkomt is of dataminimalisatie realistisch is in een tijdsgewricht waarin data en dataverzamelingen alom aanwezig en beschikbaar zijn. In een tijdsgewricht waarin gegevens steeds lastiger te anonimiseren zijn en de (volledige) verwijdering van gegevens '*the right to be forgotten*' als geformuleerd in de Verordening, praktisch onmogelijk lijkt omdat data wereldwijd worden gedistribueerd, gedeeld en opgeslagen. Dataminimalisatie lijkt dan dus ook te botsen met de realiteit van big data en data analytics.

2.2 Grondslag en doel

De doeleinden waarvoor gegevens worden verzameld moeten ingevolge het bepaalde in de Wbp en de Verordening van tevoren specifiek worden bepaald. Immers alleen dan kan worden vastgesteld of de verwerking van de gegevens te baseren is op één van de limitatief in de Wbp en Verordening opgenomen gronden (rechtmatige grondslag). Inherent aan deze in de wet opgenomen grondslagen is dat de onderneming verplicht is de verzameling van gegevens te beperken tot datgene wat noodzakelijk is voor het desbetreffende doel (zogenaamde proportionaliteit- en subsidiariteitseis). Bij big data en data analytics-toepassingen is echter niet altijd geheel duidelijk (op voorhand) voor welk (nuttig) doel de data kan worden gebruikt. Het risico bestaat aldus dat een te strikte toepassing van het beginsel ertoe kan leiden dat bepaalde toepassingen – die een resultante zijn van ontsluiting van big data door data analytics – met (potentieel) grote waarden voor de onderneming maar zeker ook voor al haar stakeholders, niet meer of minder gemakkelijk mogelijk zijn omdat deze doeleinden pas achteraf duidelijk worden.

2.3 Profielen en transparantie

Gegevensverzamelingen bestaan al lang niet meer uit alleen losse gegevens over individuen. Veel ondernemingen gebruiken profielen. De mogelijkheden voor het opbouwen en gebruiken van profielen nemen door big data en data analytics verder toe. Er kan een steeds specifieker beeld verkregen worden van ons gedrag, onze voorkeuren en interesses en op basis hiervan kan gedrag steeds meer voorspeld en ook beïnvloed worden, het zogenaamde '*nudging*' (Wetenschappelijke Raad voor het Regeringsbeleid, 2014). Deze kennis verschaft ondernemingen belangrijke inzichten waarmee ze de uitvoering van hun strategie kunnen verbeteren, hun impact op al hun stakeholders kunnen vergroten, kortom hoe ze waarde kunnen creëren. Echter het gebruik van profie-

len wordt veelal als heel indringend ervaren. Het samenstellen van een profiel van een individu en het gebruik van dat profiel voor een bepaald doeleinde vereist als hierboven al aangegeven een grondslag, een rechtmatige grondslag. Eén van de voor het samenstellen en het gebruik van profielen relevante grondslagen is het zogenaamde gerechtvaardigde belang van de onderneming.[9] Dit belang van de onderneming moet worden afgewogen tegen het belang van het individu op bescherming van zijn persoonlijke levenssfeer. Hierbij kunnen een rol spelen:

- de hoeveelheid en gevoeligheid van de gegevens die worden verzameld en verwerkt om een profiel te generen;
- de hoeveelheid en diversiteit van bronnen waaruit die gegevens afkomstig zijn (openbaar, semi-openbaar, besloten);
- de gevoeligheid van het profiel;
- de gevolgen voor het individu en de maatregelen die de onderneming heeft genomen om rekening te houden met de belangen van de individuen (zoals het transparant informeren, het wijzen op de hen toekomende rechten, het niet (verder) delen met anderen).

Door big data en data analytics wordt de impact van profielen op eenieders privacy groter. Ik vermoed dat hierdoor de balans in de afweging van het belang van de onderneming en het belang van het individu steeds vaker zal doorslaan ten faveure van het belang van het individu, waardoor de onderneming zich niet meer op de grondslag van zijn gerechtvaardigd belang kan beroepen. Eén van de andere gronden voor het samenstellen en gebruiken van profielen is de geïnformeerde toestemming van het individu.[10] Een toestemming wordt alleen als zodanig erkend wanneer deze een uitdrukkelijke wilsuiting behelst en de onderneming transparant is over wie zij is; waarvoor zij de gegevens verzamelt; van wie; met wie ze de gegevens deelt et cetera. Deze transparantievereisten worden in de Verordening uitdrukkelijk beschreven en zijn ook reeds in de Privacy Richtlijn en Wbp opgenomen. De Verordening formuleert ze alleen nog scherper. Hierbij doen zich echter twee problemen voor in het kader van big data en data analytics. Enerzijds weet men veelal op voorhand niet waarvoor men de gegevens gebruikt/gebruiken zal. Ten tweede de informatieplicht om zo de beoogde transparantie te bewerkstelligen, blijkt niet effectief, nu onderzoeken uitwijzen dat individuen de zogenaamde Privacy Statements niet (kunnen) lezen (Internet Society, 2012). Met andere woorden; bestaat er nog wel een rechtmatige grondslag voor *profiling*?

3 Big data / data analytics en het wettelijk kader

3.1 Inleiding

Wanneer we spreken over privacy in het kader van big data en data analytics, is het van belang om een onderscheid te maken tussen enerzijds de *bescherming van de persoonlijke levenssfeer* van individuen en anderzijds de *bescherming van persoonsgegevens* van individuen. Beiden raken aan de privacy van ons allen als individu, maar daar waar de bescherming van persoonsgegevens en het daarbij horende wettelijke kader vooral een issue is in de fase van verzamelen en analyseren van big data, raakt juist het toepassen van de analyses van big data aan de persoonlijke levenssfeer van individuen. Voor beiden geldt een *'ander'* juridisch kader.

In de vele bespiegelingen die er in verband met big data en privacy reeds zijn gemaakt, wordt vooral ingezoomd op de bescherming van persoonsgegevens en het feit dat ontwikkelingen in big data ertoe kunnen leiden dat steeds meer gegevens verworden tot persoonsgegevens omdat door het combineren van grote datasets waarin geanonimiseerde gegevens zitten, herleidbaarheid van de gegevens tot een individu toch ontstaat en op dat moment de gegevens zouden gaan kwalificeren als persoonsgegevens. Weinig wordt stilgestaan bij het wettelijk kader ten aanzien van de bescherming van de persoonlijke levenssfeer van individuen. Dit kader kan, althans in mijn visie, mede een contra-balans vormen voor het ongebreidelde gebruik van big data, en kan juist gewetensvol en voorzichtig gebruik van big data en data analytics triggeren. Welke waarborgen maken c.q. kunnen maken dat er door het gebruik van big data en data analytics *shared value* wordt gecreëerd. Dit vermits de onderneming *keeps to its promisses.* In ontwikkelingen als bijvoorbeeld

- *'Privacy by design'*[11],
- de *'Privacy Impact Assessment'*[12],
- het ontwikkelen van het zogenaamde cloud initiatief in Europa zodat data in de Europese Unie blijft gepaard gaande met de Europeesrechtelijke opvatting terzake privacy,
- en in de aanpassing van artikel 13 van de Grondwet (Gw),

ziet men deze waarborgen terug.

De wet- en regelgeving voor de bescherming van persoonsgegevens biedt vooral een kader voor het proces van verwerking van persoonsgegevens en mist daarbij het bredere privacyperspectief en de mogelijke impact van gegevensverwerkingen waar cliënten, consumenten, werknemers door geraakt worden. Dit bredere perspectief kan gevonden worden in voormeld juridisch kader ten aanzien van de bescherming van de persoonlijke levenssfeer en hoe een en ander doorwerkt in bijvoorbeeld arbeidsrechtelijke verhoudingen.

3.2 Wettelijk kader ten opzichte van onderdelen van proces

3.2.1 Bescherming van persoonlijke levenssfeer

De bescherming van de persoonlijke levenssfeer, van persoonsgegevens; van de privacy van het individu, is

in Nederland in diverse wetgeving gedocumenteerd en behelst de zogenaamde informationele privacy.[13] Allereerst is in artikel 10 van de Grondwet ('Gw')[14] 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 Gw 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 Gw[15] in voorbereiding, waarbij het brief- en telefoongeheim wordt uitgebreid naar een brief- en telecommunicatiegeheim.

Op Europees niveau is er het Europees Verdrag tot Bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM).[16] Hierin is het recht op bescherming van het privéleven, waarvan het recht op bescherming van persoonsgegevens deel uitmaakt, als fundamenteel recht vastgelegd. Dat recht op bescherming van het privéleven strekt zich ook uit tot eerbiediging van het privéleven op de werkplek. Deze wetgeving werkt middels de open normen van 'goed werkgeverschap' en 'goed werknemerschap' door in het Nederlandse arbeidsrecht. Het belang dat daaraan wordt toegekend ziet men bijvoorbeeld ook terug in artikel 27 leden k en l van de Wet op de Ondernemingsraden dat de bescherming van de persoonlijke levenssfeer (en die aldus van persoonsgegevens) onderwerpt aan het instemmingsrecht van de Ondernemingsraad.

3.2.2 Bescherming van persoonsgegevens

Het recht op bescherming van persoonsgegevens wordt naast in de Gw en het EVRM 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.[17] Thans is een Verordening[18] op Europees niveau ter bescherming van persoonsgegevens in voorbereiding die de richtlijn 95/46 EG ('Privacy Richtlijn') zal vervangen, welke voorbereidingen reeds in vergevorderd stadium zijn. De zogenaamde Trialoog tussen Parlement, Commissie en Raad heeft reeds aangevangen en *final agreement* is nu voorzien voor eind 2015.[19]

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 geïdentificeerd of identificeerbaar 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 opgesteld waarmee de meldplicht voor datalekken[20] ook buiten de reikwijdte van de Telecommunicatiewet voor o.a. ondernemingen zal gelden. Deze meldplicht wordt opgenomen in de Wbp en treedt in werking op 1 januari 2016. 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, welke meldplicht aldus ook onderdeel vormt van voormelde Verordening. 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 - 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.

4 Onderdelen van het proces

4.1 Het verzamelen van big data

Bij het verzamelen van gegevens speelt vaak de vraag of het is toegestaan. Als het persoonsgegevens betreft mogen deze dan ingevolge voormeld geschetst kader ten aanzien van de verwerking van persoonsgegevens verzameld worden? En als het cliëntgegevens betreft mogen ze dan indachtig op de onderneming rustende geheimhoudingsplichten, de zogenaamde *'client confidentiality'*, worden verzameld? En indien het antwoord bevestigend luidt welke randvoorwaarden horen daar dan bij? In beginsel kunnen deze vragen vanuit het juridisch kader als hierboven geschetst beantwoord worden. Ingevolge het bepaalde in de Wbp

- moet er een legitieme grondslag voor de verwerking van persoonsgegevens zijn die limitatief in de wet is opgesomd;
- moet de verwerking een specifiek doel hebben;
- gelden informatieverplichtingen richting de betrokken individuen;

- dienen adequate technische en organisatorische maatregelen getroffen te zijn om de persoonsgegevens te beschermen en
- dienen de rechten van de betrokken individuen gehonoreerd te worden.[21]

Voorts moet de onderneming ontslagen zijn van de eventueel op haar rustende *client confidentiality*. Hoewel deze kaders op het eerste gezicht helder lijken te zijn, doen zich juist in de context van big data en data analytics uitdagingen voor; enkele benoemde ik reeds kort in paragraaf 2. Het doel waarvoor gegevens verwerkt worden is veelal vooraf nog niet c.q. nog niet geheel duidelijk. De verbanden tussen gegevens en de uitkomsten van analyses kunnen vernieuwende inzichten opleveren die niet (te) voorzien waren. Dat is tegelijkertijd ook een van de grote beloften van big data en data analytics. Ook informatieverstrekking aan diegene van wie de data verzameld worden kan soms lastig zijn, of het nu om persoonsgegevens of cliëntgegevens gaat. En de organisatorische en technische maatregelen die onrechtmatige verwerking van de gegevens moeten voorkomen, verliezen mogelijkerwijs hun waarde wanneer het delen en combineren van datasets belangrijke drivers worden om de waarde van big data en data analytics te optimaliseren.

4.2 Het analyseren van big data

Het analyseren van big data wordt wel eens vergeleken met het zoeken naar goud; er moet veel worden gezeefd om waardevolle informatie naar boven te krijgen. Wanneer dit zeven goed gebeurt en de juiste data met elkaar wordt verbonden, ontstaat er letterlijk een goudmijn voor ondernemingen. Het gebruik van data analytics in combinatie met steeds snellere computers en dataverbindingen en goedkopere (cloud)rekenkracht maken het steeds eenvoudiger om uit grote hoeveelheden ongestructureerde data patronen te destilleren, op basis daarvan conclusies te trekken en gedragingen en gebeurtenissen te voorspellen. Zo kan Google bijvoorbeeld op basis van miljarden zoekopdrachten griepepidemieën voorspellen[22] en kon de Amerikaanse winkelketen Target gerichte kortingsbonnen toezenden aan vrouwen die zwanger bleken, terwijl de zwangerschap nog onbekend was (Hill, 2012). Binnen de fase van analyseren zijn tal van verwerkingen van data mogelijk, met andere woorden zijn tal van verschillende zeven te hanteren. Het uitgangspunt kan een gericht vastgesteld doel zijn. Een vooraf gesteld doel voor data kan bijvoorbeeld zijn om verkeersstromen in kaart te brengen om uiteindelijk files te kunnen voorspellen en op individueel niveau reisadvies te geven aan individuen. Tomtom doet bijvoorbeeld veel op dit gebied.[23] Echter het toepassen van statistische programma's en algoritmes om verbanden te ontdekken in data om nieuwe inzichten te krijgen ligt ook besloten in big data. Een voorbeeld hiervan zijn de voormelde 'Flutrends' van Google. Ongeacht of het exacte doel vooraf wel of niet duidelijk is, wordt er in de analysefase naar gestreefd om nieuwe verbanden te vinden die vervolgens kunnen worden toegepast; het nieuwe goud.[24]

In de analysefase kunnen ook sets van data worden gecombineerd. Hierdoor kan informatie met elkaar in verband worden gebracht die eerst volledig los van elkaar stond. Met betrekking tot de bescherming van de persoonlijke levenssfeer zijn er in deze fase twee mogelijkheden. Enerzijds kan een en ander mogelijk nadelig uitpakken voor de persoonlijke levenssfeer van individuen. Dit nu de combinatie van data, ook als begonnen wordt met geanonimiseerde gegevens (en men dus in beginsel zich als onderneming geen rekenschap hoeft te geven van het wettelijk kader ten aanzien van de bescherming van persoonsgegevens), kan leiden tot (her)identificatie (Koot, 2012) en *profiling*. Anderzijds is het ook wel voorstelbaar en mogelijk dat de enorme omvang aan datasets en de grote hoeveelheid records die zich in een set bevinden, leiden tot een betere privacybescherming. De mate van anonimiteit neemt immers toe naarmate er meerdere personen in de dataset zitten die een eenzelfde profiel voldoen.

In deze fase van het proces dient ook opgemerkt te worden dat big data en de ontwikkelingen op het gebied van data analytics nadelig (kunnen) uitpakken voor de bescherming van de persoonlijke levenssfeer en voor de bescherming van persoonsgegevens, nu big data en data analytics alleen tot volle wasdom kunnen komen door, als voormeld, de beschikbaarheid en het gebruik van grote (cloud)rekenkracht en *state of the art*-technologie. Er bestaan echter maar een beperkt aantal dominante aanbieders op deze markt, die veelal niet gevestigd zijn in Europa, maar in de Verenigde Staten ('VS') (Van Almelo, 2014). Dit leidt er veelal toe dat (persoons)gegevens Europa verlaten en verwerkt c.q. beschikbaar komen in de VS. Een jurisdictie waarin een andere opvatting terzake de bescherming van persoonsgegevens geldt. Het Amerikaanse recht kent het concept 'persoonsgegeven' zoals wij dat kennen niet. Hoewel privacy in de VS ook een grondrecht is, net als bij ons in Nederland en Europa, wordt dit uitsluitend gerelateerd aan de zogenaamde relationele privacy *'The right to be let alone'*. Informationele privacy – zeggenschap over wat men weet over jezelf – en dan met name de invulling die de zeggenschap over persoonsgegevens bij de betrokkene, het individu, zelf legt, is een Europeesrechtelijk concept. Daarnaast kent de VS een volledig ander zogenaamd '*discovery and litigation*'-regime dat maakt dat gegevens veel eenvoudiger voor derden toegankelijk en openbaar worden, nog daargelaten dat de Amerikaanse overheid, zo hebben recente schandalen[25] gedemonstreerd, met regelmaat inbreekt op de privacy... niet alleen van haar ingezetenen maar van eenieder.

4.3 Het toepassen van de uitkomsten van data analytics

Wanneer uitkomsten van data analytics worden toegepast kan eigenlijk pas duidelijk worden wat de daadwerkelijke impact van de gegevensverwerking is op individuen of groepen. Een belangrijk deel van de *required trust* om zo daadwerkelijk '*shared value*' te creëren, hangt daarom samen met de toepassing, de gevolgen daarvan en de perceptie van de maatschappij over de toepassing.[26] Daarnaast is het daarom ook juist dat bij de toepassing van de uitkomsten van data analytics het juridisch kader ten aanzien van de bescherming van de persoonlijke levenssfeer, als hierboven geschetst in ogenschouw dient te worden genomen. En dat juist in de fase van het verzamelen en het analyseren van persoons- en cliëntgegevens, het juridisch kader ten aanzien van de bescherming van persoonsgegevens en *client confidentiality* relevant is. En wanneer men dan focust op de bescherming van de persoonlijke levenssfeer van het individu, dan dient men zich rekenschap te geven van het feit dat de uitkomsten van data analytics een gemiddelde vertegenwoordigen en veelal beïnvloed (kunnen) zijn door de zoekopdrachten die zijn uitgevoerd in de database. Daarmee zijn de uitkomsten niet altijd van toepassing op alle personen die aan het profiel voldoen en ook niet objectief. Waar de schijn ontstaat dat door raadpleging van een grote hoeveelheid aan data, bias wordt uitgesloten en zekerheid en objectiviteit wordt bewerkstelligd, is dat niet een gegeven: "*In reality, working with Big Data is still subjective, and what it quantifies does not necessarily have a closer claim on the objective truth*" (Boyd & Crawford, 2012, p. 667). Deze subjectiviteit is, naast het door de onderneming niet naleven van alle juridische kaders en het zich onvoldoende rekenschap geven van de perceptie in de maatschappij, kortom van de verwachtingen van haar stakeholders, meteen één van de belangrijkste risico's van big data en data analytics, en ook meteen één van de belangrijkste risico's voor het niet realiseren van de *required trust*.

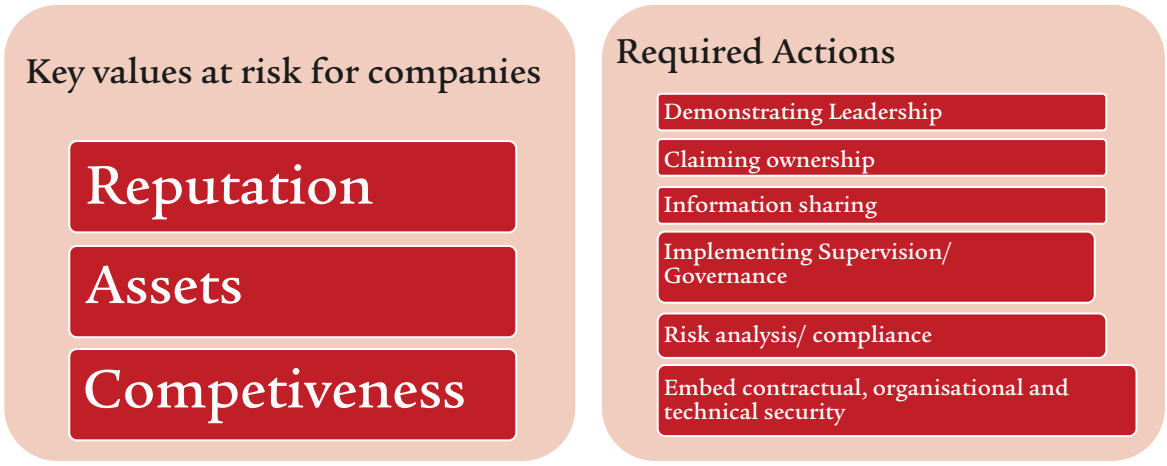
5 Establishing and safeguarding the *required trust*; amending the risks

De (toepassing van de) huidige wettelijke kaders, zoals hierboven geschetst, sluiten dus onvoldoende aan bij het fenomeen big data; de ontsluiting daarvan door gebruikmaking van data analytics en de toepassing van de uiteindelijke analyses. Maar niet alleen non-compliance met het wettelijk kader is een risico van big data en data analytics.

Zoals bovenstaande laat zien neemt het risico op non-compliance met wet- en regelgeving terzake privacy toe. Maar zijn dat de enige risico's wanneer men als onderneming *shared value* wil creëren? Ondernemingen die big data en data analytics maximaal willen uitnutten, c.q. zich realiseren dat men daar eigenlijk niet voor kan opteren, zullen alle risico's zoveel mogelijk willen mitigeren: "*The use of big data will become a key basis of competition and growth for individual firms. (...) From the standpoint of competitiveness and the potential capture of value, all companies need to take big data seriously*" (Manyika et al., 2011, p. 6). Om, in mijn visie, dat effectief te kunnen doen, merk ik op dat de risico's grofweg in drie categorieën uiteenvallen (zie figuur 1).

In dit verband en om daadwerkelijk *shared value* te bewerkstelligen, is het dan ook interessant om te bezien welke aanvullende maatregelen kunnen leiden tot waarborgen om alsnog de persoonlijke levenssfeer en persoonsgegevens van individuen te beschermen en tegelijkertijd voormelde risico's te mitigeren en de kansen die big data en data analytics bieden niet (volledig) teniet te doen. In mijn visie, en zo blijkt ook uit de Kabinetsvisie maar ook uit de Verordening waarin het begrip 'Accountability' wordt geïntroduceerd en waaraan daarin nadere invulling wordt gegeven, bestaan die maatregelen op het gebied van accountability en eigenaarschap omdat transparantie[27], controle[28] en (het ne-

Figuur 1 Risico's en vereiste actie



men van) verantwoordelijkheid[29] hierin samenkomen. Voorbeelden van acties die in dat verband genomen moeten worden, heb ik in figuur 1 al geduid.

6 Waarborgen voor privacy en realiseren van waardecreatie

6.1 Eigenaarschap/accountability

Bij eigenaarschap speelt enerzijds dat de onderneming die over de data beschikt, mogelijk een databankenrecht, auteursrecht of bepaalde licenties heeft. De rechthebbende heeft dus bepaalde aanspraken, maar ook bijbehorende verantwoordelijkheden. Eigenaarschap of zeggenschap gaat over de rechten en verantwoordelijkheden die organisaties en individuen hebben ten aanzien van bepaalde datasets en het combineren ervan. Duidelijkheid over eigenaarschap, welke duidelijkheid thans veelal nog ontbreekt, verschaft inzicht in welke partijen geautoriseerd zijn om (persoons)gegevens te verwerken en daarop aanspreekbaar zijn. Accountability sluit aan op de verantwoordelijkheid voor de onderneming, zoals genoemd in de Kabinetsvisie ePrivacy en de Verordening, en is een belangrijk aspect om te verantwoorden hoe met data omgegaan wordt. Bij accountability wordt vooral gekeken naar de wijze van verantwoorden van activiteiten, het verzamelen en gebruiken van gegevens en waarom een partij dat doet.[30] *Privacy Impact Assessments* alsmede het vereiste van *Privacy by Design* zijn hier een mooi voorbeeld van. De transparantie wordt hiermee gediend en op deze wijze wordt de positie van het individu versterkt. Daarnaast zal handhaving, indachtig ook het nieuwe zware boeteregime als geformuleerd in de Verordening (oplopende tot 5% van de wereldwijde omzet van de onderneming), ook daadwerkelijk effectief kunnen zijn nu daadwerkelijk inzicht in de activiteiten van een onderneming terzake de bescherming van privacy door toezichthouders kan worden verkregen. En indien non-compliance wordt vastgesteld, kan handhaving (mede) worden bewerkstelligd door sanctionering.

6.2 Privacy Impact Assessment en Privacy by Design

Ondernemingen zouden bij de ontwikkeling van hun dienstverlening, hun producten, hun bedrijfsvoering en de inrichting van hun organisatie een *Privacy Impact Assessment* moeten doen. Tevens kan het potentieel van big data daadwerkelijk aangewend worden als tijdens de ontwerpfase van nieuwe producten, diensten, van hun dienstverlening en bedrijfsvoering consequent gebruik wordt gemaakt van *Privacy by Design*. Het gaat er daarbij in essentie om dat ondernemingen in de ontwikkelingsfase een goede bescherming van de (persoons)gegevens en de persoonlijke levenssfeer van hun stakeholders opnemen. Organisaties moeten vervolgens hun stakeholders duidelijk maken hoe zij hun processen inrichten, en welke waarborgen en beschermingingebouwd worden. Daarmee kunnen bedrijven invulling geven aan transparantie en de eigen verantwoordelijkheid die zij hebben voor de bescherming van de privacy van hun stakeholders. In het nieuwe privacypakket van de Europese Commissie wordt *Privacy by Design31* genoemd als een belangrijke ontwikkeling die gesteund moet worden.

6.3 Cloud computing: internationale afspraken, bewustwording en keuze voor gebruikers

Zoals in de Digitale Agenda.nl van de overheid is aangegeven, ziet het kabinet cloud computing als een belangrijke ontwikkeling om efficiënter en flexibeler te werken. En is cloud computing een voorwaarde voor het kunnen uitnutten van het potentieel van big data en data analytics. Omdat cloud computing een grensoverschrijdend onderwerp is en bovenal in de relatie tot de VS een eigen dynamiek kent, zijn afspraken en aanpak vooral in Europees verband essentieel. Het Europese Cloud Initiatief is daar een mooi voorbeeld van. Aangezien er geen barrières bestaan die grensoverschrijdende cloud-diensten tegenhouden en de bescherming van de privacy niet in alle landen buiten de Europese Unie van een gelijkwaardig niveau is, als in Nederland c.q. binnen Europa, is de internationale dialoog van cruciaal belang om ook buiten de Europese Unie de privacy te beschermen.

6.4 Versterken bewustwording en positie van het individu.

Privacy is een groot goed. Uit onderzoek (Kaspersky, 2015) blijkt dat burgers het ook belangrijk vinden. Tegelijkertijd hebben weinig Nederlanders besef van en grip op wat er met hun privégegevens gebeurt. Het is hoog tijd burgers niet alleen verantwoordelijk te stellen voor hun privacy, maar ze ook de middelen te geven om die verantwoordelijkheid te kunnen nemen. Transparantie en communicatie is hierbij key. Er is een heel dubbel beeld. Enerzijds heeft de burger geen grip op wat er allemaal met zijn of haar gegevens gebeurt. Anderzijds is de burger wel steeds bewuster dat privacy belangrijk is. Het leeft in de maatschappij. Het gebrek aan grip valt volgens Eva de Leede, deelneemster aan de Nationale DenkTank 2014[32], mede te verklaren door onvermijdbaarheid: *"Je moet je gegevens ook wel afgeven als je bepaalde diensten wilt gebruiken"*. Daarbij worden lange en lastig te doorgronden gebruiksvoorwaarden of reglementen voorgeschoteld die individuen 'blind' accepteren. *"Je bent 72 werkdagen per jaar kwijt om alle disclaimers te lezen die je normaal accepteert"*. Zij pleit voor een *labeling* (Siljee en De Leede, 2015) met duidelijke iconen die de inhoud behapbaar maakt voor het individu. Daarbij moeten de daadwerkelijke voorwaarden en reglementen natuurlijk ook nog gewoon te zien zijn. Dit zou een werkelijke bijdrage aan de versterking en bewustwording van het individu behelzen. Het zou de gewenste transparantie mede helpen bewerkstelli-

gen en tegelijkertijd toestemming tot een rechtmatige grondslag voor de verwerking van big data en data analytics mogelijk maken.

7 Ter afsluiting

Big data en data analytics zijn hier en *here to stay*. Daarbij valt op, en zo heb ik ook getracht in deze bijdrage aan te geven, dat nog niet alle vraagstukken zijn beantwoord, zeker niet op de scheidslijn van de wettelijke kaders en de mogelijkheden van de techniek. Op het gebied van de bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens kleven er risico's aan het gebruik van big data en data analytics. Tegelijkertijd bestaan en ook weer *down sides* aan het niet (kunnen) benutten van big data en data analytics. Om daadwerkelijk *shared value* te creëren voor en door de onderneming voor al haar stakeholders, zal als voormeld de *required trust* moeten worden bewerkstelligd. In mijn visie, kan *required trust* bovenal gerealiseerd worden door het doen uitvoeren van zogenoemde *Privacy Impact Assessments* en door toepassing van *Privacy by Design*; het vroegtijdig in het ontwerp van big data en data analytics-toepassingen meenemen van de privacyvereisten en de verwachtingen van de stakeholders van de onderneming. Deze zien niet alleen op de bescherming van hun gegevens, maar bovenal op de bescherming van hun persoonlijke levenssfeer en de zeggenschap die zij daarover hebben. Transparantie over wat, waarvoor er door wie met hun gegevens gebeurt en de overtuiging dat de onderneming *'keeps to its promisses'* is daarbij essentieel...*With maturity of trust comes greater value.* ■

Mr. drs Monique G.M. van Dijken Eeuwijk, advocaat bij NautaDutilh; voorzitter van het Benelux Sector Team Professional Services Firms en lid van het Privacy en E-commerce team.

Noten

1 Volgens onderzoeks- en adviesbureau Gartner gaat het bij Big Data om drie factoren: de hoeveelheid data, de snelheid waarmee data binnenkomt en opgevraagd kan worden en de diversiteit van data.

2 Data Analytics: het op een gestructureerde wijze verzamelen van digitale gegevens en deze met behulp van analyse omzetten in relevante informatie.

3 Shared value: het genereren van economische waarde op een dusdanige wijze dat naast het genereren van winst tegelijkertijd waarde wordt gecreëerd voor de maatschappij, met andere woorden waarde wordt gecreëerd niet alleen voor de shareholder maar voor alle stakeholders van een onderneming. Dit door ook recht te doen aan de verwachtingen en behoeften van deze stakeholders.

4 Het principe van accountability behelst dat verantwoordelijken een proactieve houding aannemen bij het uitvoeren van hun dataprotectieplichten. Zij moeten maatregelen nemen om te garanderen dat de materiële verplichtingen worden nageleefd in de praktijk. Dataprotectie zou een onderdeel moeten worden van de gedeelde waarden van een organisatie en ingebed in alle bedrijfsprocessen. Op verzoek dient dit ook aantoonbaar te worden gemaakt; Opinie 3/2010 van de 'Artikel 29 Werkgroep' met betrekking tot het principe van accountability, de dato 10 Juli 2013; WP 173.

5 Verwerking van persoonsgegevens: alle handelingen die een organisatie kan uitvoeren met persoonsgegevens, van verzamelen tot en met vernietigen.
Persoonsgegeven: Een gegeven wordt als persoonsgegeven aangemerkt indien en voor zover de onderneming, of iemand anders, in staat is om daarmee zonder onevenredige inspanning, de identiteit van een individueel natuurlijk persoon vast te stellen of te achterhalen.

6 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl.

7 Artikel 6 lid 1 onder c Privacy Richtlijn jo artikel 10 en 11 Wbp.

8 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:NL:PDF

9 Artikel 8 sub f Wbp.

10 Artikel 8 sub a Wbp.

11 "Privacy by design" gaat uit van het principe dat er in een vroeg stadium van de ontwikkeling van de gegevensverwerking nagedacht wordt over een goed gebruik van persoonsgegevens, de noodzaak om deze gegevens te gebruiken en te beschermen. Door bij de ontwikkeling van systemen de bescherming van persoonsgegevens en van privacy in te bouwen, is de kans op succes het grootst. Opinie 8/2014 van de Artikel 29 Werkgroep met betrekking tot recente ontwikkelingen op het gebied van Internet of Things: WP 223 de dato 16 september 2014.

12 Privacy Impact Assessment: deze beoordeling heeft tot doel om de risico's van een bepaalde verwerking van persoonsgegevens voor de betrokkenen in kaart te brengen en om waar nodig maatregelen te nemen. Opinie 04/2013 van de Artikel 29 Werkgroep met betrekking tot Data Protection Impact Assessment Template for Smart Grid and Smart Metering System; WP 205 de dato 22 april 2013.

13 Informationele Privacy: zeggenschap van het individu over wat men weet over jezelf.

14 Artikel 10 Gw:
1.Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2.De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3.De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

15 TK 2013/14, 33 989 Brief- en telecommunicatiegeheim.

16 Artikel 8 EVRM. *Recht op eerbiediging van privé-, familie- en gezinsleven.*
1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

17 Richtlijn 95/46/EG en richtlijn 2002/58/EG.

18 (COM(2012) 11 final).

19 European Commission (2015). Press release: http://ec.europa.eu/justice/newsroom/data-protection/news/150615_en.htm.

20 Besluit 2015/281. Geraadpleegd op https://www.eerstekamer.nl/behandeling/20150710/publicatie_inwerkingtreding/document3/f=/vjvgcs561qzg.pdf.

21 Artt. 8, 11,12, 13.14, 33, 34 Wbp.

22 Http://www.google.org/flutrends/about/how.html.

23 Zie: https://www.tomtom.com/en_gb/drive/maps-services/.

24 De privacy impact van Big Data, Considerati 2013, p. 6.

25 Bijvoorbeeld het afluisteren van Angela Merkel, de Snowdon-affaire, de zogenaamde Swift Casus (http://www.recht.nl/vakliteratuur/ie/artikel/173070/de-swift-casus/).

26 Voorbeeld hiervan is de ING casus: zie http://www.nu.nl/economie/3722010/ing-houdt-privacygevoelige-proef-met-klantgegevens.html.

27 Transparantie: 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.

28 Controle: 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).

29 Verantwoordelijkheid: Ondernemingen 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.

30 Zie noot 4.

31 Acht key elementen van Privacy by Design: (i) Procatief i.p.v. reactief, (ii) Preventief i.p.v. herstellend, (iii) Privacy als Standaard, (iv) Privacy geïntegreerd in het ontwerp, (v) Volledige functionaliteit, (vi) Veiligheid van begin tot eind, (vii) Zichtbaarheid en Transparantie, (viii) Laat gebruiker centraal staan.

32 http://www.nationale-denktank.nl/.

Literatuur

- Almelo, L. van (2014). 'Houd gegevens binnen de EU'. Juridische aspecten van big data. *Accountant, 4*(3, maart), 18-20. Geraadpleegd op https://www.accountant.nl/magazines/accountant-maart-2014/houd-gegevens-binnen-de-eu/.
- Article 29 Data Protection Working Party (2014). Opinion 8/2014 on the on Recent Developments on the Internet of Things. Geraadpleegd op http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.
- Article 29 Data Protection Working Party (2013). Opinion 4/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force. Adopted on 22 April 2013. Geraadpleegd op http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf.
- Article 29 Data Protection Working Party (2010). Opinion 3/2010 on the principle of accountability. Adopted on 13 July 2010. Geraadpleegd op http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.
- Besluit 2015/281. Besluit van 1 juli 2015 tot vaststelling van het tijdstip van inwerkingtreding van de Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp) (Stb. 2015, 230). Geraadpleegd op https://www.rijksoverheid.nl/documenten/publicaties/2015/07/10/staatsblad-281-besluit-inwerkingstredingsbesluit-meldplicht-datalekken-en-uitbreiding-bestuurlijke-boetebevoegdheid-cbp.
- Boyd, D., & Crawford, K. (2012). Critical questions for Big Data; Provocations for a cultural, technological and scholarly phenomenon. *Information, Communication & Society, 15*(5), 662-679.
- Eimers, P.W.A., & Nieuw Amerongen, C.M. van (2015). Ontwikkelingen in de toepassing van data-analyse voor de accountantscontrole. Niets nieuws onder de zon? *Maandblad voor Accountancy en Bedrijfseconomie, 89*(10), dit themanummer.
- Europese Commissie (2002). Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie). Publicatieblad nr. L 201 van 31 juli 2002. Geraadpleegd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:nl:PDF.
- Europese Commissie (1995). Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. Publicatieblad Nr. L 281 van 23/11/1995. Geraadpleegd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl:HTML.
- Europese Commissie (2012). Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming). Geraadpleegd op http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:NL:PDF.
- Europese Commissie (2012). Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van

natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming). COM(2012) 11 final. Geraadpleegd op http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_nl.pdf.
- European Commission (2015). Press release. Commission proposal on new data protection rules to boost EU Digital Single Market supported by Justice Ministers. Press release 15-06-2015. Geraadpleegd op http://ec.europa.eu/justice/newsroom/data-protection/news/150615_en.htm.
- Hill, K. (2012). How Target figured out a teen girl was pregnant before her farther did. Forbes Magazine, 16 februari 2012. Geraadpleegd op http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.
- Internet Society (2012). Global Internet User Survey. Internet Society. Geraadpleegd op http://bit.ly/TFHWsd.
- Kaspersky (2015). Right marktonderzoek. Rapportage onderzoek on line privacy. Geraadpleegd op http://newsroom.kaspersky.eu/fileadmin/user_upload/nl/Downloads/PDFs/Kaspersky_Lab_Onderzoek_Online_privacy.pdf.
- Klijnsmit, P., Sodekamp, M., & Wallage, P. (2003l). Bedrijfsrisico's van de accountant en het Audit Risk Model. *Maandblad voor Accountancy en Bedrijfseconomie, 77*(5), 190-195.
- Koot, M.R. (2012). Measuring and predicting anonymity. Dissertatie Universiteit van Amsterdam. Geraadpleegd op http://dare.uva.nl/document/2/107610.
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A.H. (2011). *Big data: the next frontier for innovation, competition and productivity*. McKinsey Global Institute. Geraadpleegd op http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.
- Ministerie van Economische Zaken (2013). Brief Kabinetsvisie op e-privacy: op weg naar gerechtvaardigd vertrouwen, 24 mei. Geraadpleegd op https://www.rijksoverheid.nl/documenten/kamerstukken/2013/05/24/kamerbrief-met-kabinetsvisie-op-e-privacy.
- Porter, M.E., & Kramer, M.R. (2011). Creating shared value. *Harvard Business Review, 89*(1/2), 62-77.
- Siljee, J., & Leede, E. de (2015). Privacypictogrammen: Privacy en transparantie als unique selling points. Privacy & Practice 01-02/2015.
- Werkgroep Toekomst Accountantsberoep (2014). *In het publiek belang – maatregelen ter verbetering van de kwaliteit en onafhankelijkheid van de accountantscontrole*. Nederlandse Beroepsorganisatie voor Accountants (NBA). Geraadpleegd op https://www.nba.nl/Documents/Nieuws/2014/pdfs/In%20het%20publiek%20belang%20rapport%20WG%20Toekomst%20Acc%2025sep14.pdf.
- Wet 2015/230/Wbp. Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp). Geraadpleegd op https://www.rijksoverheid.nl/documenten/publicaties/2015/07/10/staatsblad-230-wijziging-van-de-wet-bescherming-persoonsgegevens.
- Wetenschappelijke Raad voor het Regeringsbeleid (2014). Met kennis van gedrag beleid maken. Amsterdam University Press: Amsterdam. Geraadpleegd op http://www.wrr.nl/fileadmin/nl/publicaties/PDF-Rapporten/92_Met_kennis_van_gedrag_beleid_maken.pdf.