Hoofdstuk 6

Privacyaspecten

Door prof.mr J.M.A. Berkvens[126]

In dit hoofdstuk worden de privacyaspecten van uitbesteding door financiële ondernemingen behandeld. In de inleiding wordt de problematiek kort in hoofdlijnen geschetst. Vervolgens worden enkele thema's meer in detail uitgewerkt.

6.1 INLEIDING

6.1.1 Algemeen

Financiële ondernemingen moeten bij hun verwerking van persoonsgegevens voldoen aan de Wet bescherming persoonsgegevens (hierna: Wbp). Zij zijn daarbij niet alleen verantwoordelijk voor hun eigen verwerkingen maar ook voor die van andere partijen die in hun opdracht persoonsgegevens verwerken. De inschakeling van een derde mag er niet toe leiden dat financiële ondernemingen zelf niet meer aan hun verplichtingen kunnen voldoen. Met betrekking tot het onderwerp van uitbesteding zijn de hierna volgende onderdelen van de Wbp van belang

126 Prof. Berkvens is adjunct directeur Juridische zaken bij Rabobank Nederland en emeritus hoogleraar Recht en informatica aan de Radboud Universiteit Nijmegen.

6.1.2
Verantwoordelijke en bewerker

Uitbestedende financiële ondernemingen zijn verantwoordelijke in de zin van de Wbp. Bij uitbesteding zal de inbesteder in het algemeen als bewerker in de zin van de Wbp worden aangemerkt. De grenzen tussen verantwoordelijke en bewerker zijn niet altijd helemaal duidelijk te trekken. Soms komt een bewerker bewust of onbewust in de rol van verantwoordelijke terecht. Verantwoordelijke en bewerker zijn op grond van de Wbp verplicht hun verhouding in een contract vast te leggen. De verantwoordelijke is aansprakelijk voor het handelen van de bewerker.

6.1.3
Beveiliging

Een belangrijke verplichting uit de Wbp is de beveiligingsplicht. Op de financiële onderneming rust de verplichting om persoonsgegevens adequaat te beveiligen. Bij uitbesteding blijft de financiële onderneming verantwoordelijk voor de kwaliteit van de beveiliging bij de inbesteder. De beveiliging moet in orde zijn en het College bescherming persoonsgegevens (Cbp) kan bij uitbesteding een onderzoek instellen naar het niveau van beveiliging bij de derde en zo nodig optreden bij geconstateerde lacunes. Dat geldt bij concrete datalekken maar ook indien er zich (nog) geen incidenten hebben voorgedaan.

6.1.4
Inzage en correctie

De uitbestedende financiële onderneming heeft op grond van de Wbp verplichtingen op het gebied van inzage en correctie. Bij een verzoek om inzage of correctie moet de financiële onderneming daar binnen de wettelijke termijnen aan voldoen. Als de administratie is uitbesteed blijft de verplichting om tijdig te voldoen aan verzoeken om inzage of correctie ongewijzigd op de financiële onderneming rusten. Dat kan bij een *supplier lock-in situatie* (inbesteder werkt niet mee of kan niet meewerken) problemen opleveren.

6.1.5
Datakwaliteit

Een andere in dit kader relevante verplichting uit de Wbp betreft de kwaliteit van de gegevensverwerking. Bij uitbesteding moet de kwaliteit van de

processen van de inbesteder zodanig zijn dat er geen foutieve verwerkingen kunnen plaats vinden. Daarbij kan ook worden gedacht aan het opvolgen van wettelijke bewaartermijnen.

6.1.6
Gegevensexport

Bij de export van gegevens naar landen buiten de EU gelden op grond van de Wbp speciale eisen. Die eisen gelden niet alleen bij verstrekking van gegevens aan een derde (verantwoordelijke naar verantwoordelijke) maar ook bij uitbesteding (verantwoordelijke naar bewerker). De regels gelden tussen de financiële onderneming en de inbesteder maar zijn ook van toepassing als de inbesteder op zijn beurt een subbewerker in een land buiten de EU inschakelt.

6.1.7
Cloud computing of simpele uitbesteding

De Wbp maakt geen onderscheid tussen simpele uitbesteding en cloud computing. Daarom wordt in dit hoofdstuk evenmin dit onderscheid gemaakt. Wel zal duidelijk zijn dat door uitbesteding in de cloud de complexiteit van de governance zal toenemen. Vooral als de cloud zich buiten de landsgrenzen bevindt. Op het onderwerp cloud computing zal nader worden ingegaan in hoofdstuk 8 van deze bundel.

6.2
VERANTWOORDELIJKE EN BEWERKER

6.2.1
Verantwoordelijke of bewerker?

De centrale figuur in de Wbp is de zogenaamde verantwoordelijke. Volgens Wbp art. 1.d is dat:

> 'de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;'

De verantwoordelijke kan bij zijn werkzaamheden gebruikmaken van de diensten van een derde. Die wordt in de Wbp aangeduid als bewerker (in de

Privacyrichtlijn[127]: 'verwerker'). In dit hoofdstuk wordt ook de term 'inbesteder' gehanteerd. Wbp art. 1.e bewerker:

> 'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;'

De begrippen 'verantwoordelijke' en 'bewerker' blijken in de praktijk soms in elkaar over te lopen.[128] Bij het bepalen van de status van de inbesteder zal moeten worden gekeken naar de feitelijke omstandigheden waaronder de werkzaamheden plaatsvinden en naar de aard van de contractuele afspraken. In de meest simpele situatie is sprake van één verantwoordelijke en één bewerker. Maar blijkens de memorie van toelichting zijn ook situaties denkbaar waar sprake is van gedeelde verantwoordelijkheid.[129] De lijn van denken van het Cbp wordt in een advies van het Cbp uit 2002 als volgt weergegeven:

> 'Daarnaast beperkt de bewerker zich tot het verwerken van persoonsgegevens zonder zeggenschap te hebben over het doel van en de middelen voor de verwerking van persoonsgegevens. Zou hij immers deze zeggenschap wel verwerven dan dient hij als verantwoordelijke te worden aangemerkt. Wanneer de bewerker zelf de details van de verwerkingswijze bepaalt, impliceert dat niet dat hij daarmee ook de zeggenschap verkrijgt over de verwerking van persoonsgegevens als zodanig. Het bepalen van de details van de verwerkingswijze door de bewerker zal in de praktijk veelal zijn grondslag vinden in de deskundigheid die de bewerker in huis heeft, de (keuze van de) apparatuur en de software die hij daarbij gebruikt of de mankracht waarover hij beschikt. Resumerend: voor de afbakening van de relatie verantwoordelijke en bewerker zijn het bepalen van de doeleinden van de verwerking en de zeggenschap daarover doorslaggevend. Of en hoeverre de bewerker de details van de verwerkingswijze van persoonsgegevens kan bepalen hangt in grote mate af van hetgeen hierover is bepaald in de overeenkomst die de verantwoordelijke ingevolge artikel 14, tweede lid, WBP heeft afgesloten met de bewerker.'[130]

127 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 *PbEG* 1995 L 281/31.

128 Zie bijvoorbeeld de zogenaamde Swift-affaire. J.M.A. Berkvens, 'Europees parlement en terrorisme financiering', *FR* 2010/4.

129 *Kamerstukken II* 1997/1998, 25 892, nr. 3, p. 58 e.v.

130 Advies Cbp z2002-0362 van 14 mei 2002.

Dat naar het oordeel van de Artikel 29 Werkgroep[131] de contractuele afspraak tussen de uitbesteder en de inbesteder niet doorslaggevend hoeft te zijn voor de bepaling van de wettelijke kwalificatie van partijen blijkt uit een advies uit 2010, waarin het volgende wordt opgemerkt:

> 'De relevantie van de feitelijke invloed is ook te zien in de SWIFT-zaak, waarin SWIFT formeel werd beschouwd als gegevensverwerker maar in feite – in ieder geval in zekere mate – fungeerde als de voor de verwerking van gegevens verantwoordelijke. In deze zaak werd duidelijk dat de contractuele aanstelling van een partij als voor de verwerking van gegevens verantwoordelijke of als verwerker weliswaar relevante informatie kan bieden over de wettelijke hoedanigheid van die partij, maar dat een dergelijke contractuele aanstelling toch niet doorslaggevend is voor het vaststellen van de daadwerkelijke hoedanigheid van die partij, die uit concrete omstandigheden moet blijken.'[132]

In hetzelfde advies wordt ook ingegaan op situaties waarin de bewerker gedeeltelijk van kleur kan verschieten en voor een deel als verantwoordelijke kan worden aangemerkt:

> 'Het enkele feit dat iemand bepaalt op welke manier persoonsgegevens worden verwerkt, kan ertoe leiden dat hij wordt aangemerkt als voor de verwerking van de gegevens verantwoordelijk, hoewel deze kwalificatie buiten de werkingssfeer van een contractuele verhouding ontstaat of uitdrukkelijk door een contract wordt uitgesloten. Een duidelijk voorbeeld hiervan was de SWIFT-zaak, waarin deze onderneming het besluit nam om bepaalde persoonsgegevens – die oorspronkelijk namens financiële instellingen voor commerciële doeleinden werden verwerkt – ook beschikbaar te stellen met het oog op de bestrijding van de financiering van terrorisme, zoals verzocht in dagvaardingen van het Amerikaanse ministerie van Financiën.'[133]

131 De Artikel 29 Werkgroep (WP29) is een onafhankelijk adviescollege dat is ingesteld in art. 29 van de Privacyrichtlijn en op grond van art. 30 van de Privacyrichtlijn onder meer tot taak heeft om de Europese Commissie te adviseren in privacy-aangelegenheden. De adviezen van WP29 zijn te vinden op de website van de Europese Commissie http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

132 WP29: Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker', goedgekeurd op 16 februari 2010 (WP 169), p. 11.

133 WP29: Advies 1/2010 over de begrippen 'voor de verwerking verantwoordelijke' en 'verwerker', Goedgekeurd op 16 februari 2010 (WP 169), p. 14.

6.2.2
Het bewerkerscontract

Verantwoordelijke en bewerker zijn op grond van de Wbp verplicht hun verhouding contractueel vast te leggen. Wbp art. 14 leden 2, 4, 5:

> 2. De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.
> 4. Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b.
> 5. Met het oog op het bewaren van het bewijs worden de onderdelen van de overeenkomst of de rechtshandeling die betrekking hebben op de bescherming van persoonsgegevens, alsmede de beveiligingsmaatregelen als bedoeld in artikel 13 schriftelijk of in een andere, gelijkwaardige vorm vastgelegd.

Volgens de memorie van toelichting moeten er afspraken worden vastgelegd die duidelijk betrekking hebben op de gegevensverwerking.[134] Daarmee wordt bedoeld dat een enkele dienstverleningsovereenkomst waarin de dienst wordt beschreven niet voldoende is. De overeenkomst tussen de verantwoordelijke en de bewerker moet naar haar aard betrekking hebben op de gegevensverwerking. De afspraken kunnen natuurlijk wel een apart hoofdstuk vormen van de uitbestedingsovereenkomst.

Vanwege de lock-in problematiek dient de uitbesteder aandacht te besteden aan situaties waarin de inbesteder zijn verplichtingen niet wil of kan nakomen. Het gaat daarbij om verplichtingen met betrekking tot zowel beschikbaarheid, integriteit als exclusiviteit van gegevens. De financiële onderneming kan in de problemen komen als ze aan een inzageverzoek moet voldoen of als een rechter een correctieverzoek toewijst in combinatie met een dwangsom.[135]

134 *Kamerstukken II* 1997/1998, 25 892, nr. 3, p. 99.

135 Soms is ook de curator op jacht naar informatie in de cloud. Rb. 's-Hertogenbosch 20 maart 2012, *LJN* BV9640; Hof 's-Hertogenbosch 26 maart 2013, *LJN* BZ5770. Over lock-in ook: *ECLI:NL:RBAMS*:2010:BL4068 en *ECLI:NL:RBROT*:2012:BW5386.

Het sluiten van contracten met grote inbesteders is geen sinecure. De Europese Commissie is bezig met een onderzoek naar een mogelijke handreiking voor het opstellen van veilige en billijke contractvoorwaarden.[136] Ook zijn cloud service-providers, verenigd in de Select Industry Group, bezig met een onderzoek naar de mogelijkheid van een Europese gedragscode als bedoeld in art. 27 lid 3 van de Privacyrichtlijn.[137] Daarnaast is sprake van overleg tussen individuele leveranciers en de Artikel 29 Werkgroep.[138]

6.2.3 Aansprakelijkheid

De verantwoordelijke is aansprakelijk voor het handelen van de bewerker. Dat volgt uit art. 49 Wbp. Het betreft een lex specialis ten opzichte van art. 6:162 BW. De toelichting op de Wbp meldt daarover het volgende:

> 'Vanzelfsprekend is alleen aansprakelijk de verantwoordelijke voor de verwerking met betrekking waartoe in strijd is gehandeld met de wettelijke voorschriften. De bepaling impliceert voorts dat ook indien er een bewerker is die gegevens verwerkt ten behoeve van een verantwoordelijke, ook steeds die verantwoordelijke daarvoor aansprakelijk is. De verwerking blijft immers altijd onder de verantwoordelijkheid van de verantwoordelijke plaatsvinden. Dit laat onverlet dat hij mogelijk een regresrecht heeft op de bewerker. Daarnaast is de bewerker ook zelfstandig aansprakelijk voor zijn aandeel in de schade.'[139]

Wbp art. 49:

> 1. Indien iemand schade lijdt doordat ten opzichte van hem in strijd wordt gehandeld met de bij of krachtens deze wet gegeven voorschriften zijn de volgende leden van toepassing, onverminderd de aanspraken op grond van andere wettelijke regels.
> 2. Voor nadeel dat niet in vermogensschade bestaat, heeft de benadeelde recht op een naar billijkheid vast te stellen schadevergoeding.

136 *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the regions, 'Unlashing the Potential of Cloud Computing in Europe'*, Com(2012)529 final van 27-9-2012. Zie onder meer de aanbevelingen op p. 12-13. Voor een reactie op dit stuk van het ministerie van Buitenlandse Zaken: *Kamerstukken II* 2012/2013, 22 112, nr. 1500.

137 Zie https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct.

138 Brief Ref. Ares(2014)1033670 - 02/04/2014 van WP29 aan Microsoft van 2 april 2014 [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf].

139 *Kamerstukken II* 1997/1998, 25 892, nr. 3, p.176.

3. De verantwoordelijke is aansprakelijk voor de schade of het nadeel, voortvloeiende uit het niet-nakomen van de in het eerste lid bedoelde voorschriften. De bewerker is aansprakelijk voor die schade of dat nadeel, voor zover ontstaan door zijn werkzaamheid.
4. De verantwoordelijke of de bewerker kan geheel of gedeeltelijk worden ontheven van deze aansprakelijkheid, indien hij bewijst dat de schade hem niet kan worden toegerekend.'

6.2.4
Subbewerker

Als de inbesteder een subbewerker inschakelt, blijft de oorspronkelijke uitbesteder (de financiële onderneming) verantwoordelijk. Dat volgt eveneens uit de memorie van toelichting:

> 'Uit de verantwoordelijkheid van de opdrachtgever – die in de zin van de wet geldt als verantwoordelijke voor de gegevensverwerking – vloeit voort dat hij uitdrukkelijk heeft ingestemd met het subbewerkersschap. Indien de opdrachtgever daarvoor in zijn overeenkomst met de bewerker uitdrukkelijk ruimte heeft gegeven, kan de bewerker – met behoud van zijn volle aansprakelijkheid voor de naleving van zijn contract met de verantwoordelijke – delen van de verwerking uitbesteden aan «subbewerkers». De bewerker dient dan wel contractueel verzekerd te hebben dat de subbewerker zich eveneens richt naar de instructies van de verantwoordelijke, tot geheimhouding verplicht is en de nodige beveiligingsmaatregelen ten opzichte van de gegevensverwerking neemt. De verantwoordelijke dient hiervan wel op de hoogte te worden gesteld opdat deze in staat is toe te zien op de naleving van zijn afspraken met de bewerker (artikel 14).'[140]

6.3
BEVEILIGING

6.3.1
Algemeen

Een belangrijke verplichting van de verantwoordelijke is de beveiliging van (de verwerking van) persoonsgegevens. De verplichting tot beveiliging wordt geformuleerd in art. 13 Wbp:

140 *Kamerstukken II* 1997/1998, 25 892, nr. 3, p. 63.

> 'De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.'

De verplichting van de verantwoordelijke tot beveiliging houdt niet op bij uitbesteding van een beveiliging van de persoonsgegevens. Die verantwoordelijkheid volgt de hele keten van eventuele verdere uitbestedingen aan sub verwerking. Uit art. 14 Wbp volgt dat de opdrachtgever bij uitbesteding verantwoordelijk blijft voor de -bewerkers. Wbp art. 14, leden 1 en 3:

> 1. Indien de verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, draagt hij zorg dat deze voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke ziet toe op de naleving van die maatregelen.
> 3. De verantwoordelijke draagt zorg dat de bewerker
> a. de persoonsgegevens verwerkt in overeenstemming met artikel 12, eerste lid en
> b. de verplichtingen nakomt die op de verantwoordelijke rusten ingevolge artikel 13.'

Het Cbp heeft in 2013 richtsnoeren uitgegeven voor de beveiliging van persoonsgegevens. In hoofdstuk 4 van die richtsnoeren wordt nader ingegaan op beveiligingsaspecten bij de inschakeling van een bewerker.[141] Bij uitbesteding kan de inbesteder zelf niet goed bepalen welk niveau van beveiliging moet worden aangehouden. De financiële onderneming zal eerst zelf een analyse moeten maken van het uit te besteden proces en van de aard van de gegevens. Daarbij kan worden gedacht aan een risicoanalyse. In die risicoanalyse wordt aandacht besteed aan de gevoeligheid van de gegevens en de impact die inbreuken op de beveiliging kunnen hebben voor financiele onderneming en betrokken individuen waarvan de gegevens worden verwerkt. De risicoanalyse dient er rekening mee te houden dat buitenlandse autoriteiten toegang kunnen eisen tot persoonsgegevens die zich binnen hun territorium bevinden of die vanuit hun territorium kunnen worden be-

141 *Cbp richtsnoeren beveiliging persoonsgegevens*, Cbp: Den Haag, februari 2013.

naderd.[142] De risicoanalyse moet er bovendien rekening mee houden, dat de inbesteder mogelijk geen mededelingen mag doen aan de uitbestedende financiële onderneming (*gag order*). Landenrisico's zijn overigens een specifiek aandachtspunt. Men moet in de risicoanalyse ook aandacht besteden aan de algemene veiligheidscondities. Denk aan de integriteit en beschikbaarheid van de telecommunicatie- infrastructuur en de praktische mogelijkheden voor screening van medewerkers bij de inbesteder.

De uitbesteder is verplicht in de uitbestedingsovereenkomst aandacht te besteden aan het onderwerp beveiliging. Dat blijft niet beperkt tot het specificeren van het beveiligingsniveau en het verplichten van de inbesteder om een overeengekomen niveau van beveiliging aan te houden. Hij mag niet alleen afgaan op de contractuele beloften van de inbesteder maar heeft ook een zekere vergewisplicht.[143] Die vergewisplicht kan tot uitdrukking komen in een *right to audit* of de mogelijkheid om een onafhankelijke derde een verklaring te laten afleggen over de kwaliteit van de beveiliging en de afwezigheid van veiligheidsincidenten. Dat is overigens niet zo eenvoudig als het op het eerste gezicht lijkt. Er zijn diverse standaards voor verklaringen in omloop zoals de inmiddels verouderde SAS 70 type II-verklaring en de ISAE 3402-verklaring.[144] Deze verklaringen betreffen echter meer de continuïteit van de onderneming en in mindere mate of niet de kwaliteit van de geboden beveiliging. Een ander aandachtspunt is het feit dat de verklaringen achteraf worden opgesteld en dus altijd achter de feiten aanlopen. Nieuwe standaards bieden mogelijk soelaas. Bijvoorbeeld de SOC I t/m III.[145] Iedere verklaring moet in ieder geval worden gecheckt op reikwijdte, looptijd, verversing, soorten processen, controle over subbewerkers.[146]

142 Zie J.V.J. van Hoboken, A.M. Arnbak, N.A.N.M. van Eijk, m.m.v. N. Kruijssen, *Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act*, Instituut voor Informatierecht (UVA), Amsterdam: september 2012, p. 36. Deze publicatie wordt uitvoerig geciteerd door de staatssecretaris van het ministerie van Veiligheid en Justitie bij het beantwoorden van Kamervragen over de buitenlandrisico's van cloud computing. Ingezonden vragen van de leden Gesthuizen en Van Bommel aan de ministers van Veiligheid en Justitie en van Buitenlandse zaken over de toegang van de V.S. tot data in de cloud (15 oktober 2012, nr. 2012Z17456) en ingezonden vragen van het lid Oosenbrug aan de minister van Veiligheid en Justitie over Amerikaanse toegang tot cloudgegevens (15 oktober 2012, nr. 2012Z17457) (Beantwoord op 8 november 2012.)

143 Vergelijk dictum in zaak C-119/12, Arrest van het Hof (Derde kamer) van 22 november 2012 '*Elektronische communicatie – Richtlijn 2002/58/EG – Artikel 6, leden 2 en 5 – Verwerking van persoonsgegevens – Verkeersgegevens nodig voor opmaken en innen van facturen – Inning van vorderingen door derde vennootschap – Personen handelend onder gezag van aanbieders van openbare communicatienetwerken en elektronischecommunicatiediensten*'.

144 Vergelijk de Norea-richtlijn 3402. Te vinden via http://www.norea.nl/Norea/Actueel/Nieuws/

145 Tommy W. Singleton, 'Understanding the new SOC reports', *ISACA Journal*, volume 2/2011.

146 Zie par. 4.2 van 'Opinion 05/2012 on cloud computing', adopted July 1st 2012 by the Article 29 Data Protection Working Party (WP 196).

De bewerkersovereenkomst dient ten slotte aandacht te besteden aan de afhandeling van veiligheidsincidenten. Zie ook hierna onder 'Datalekken'.

6.3.2 Datalekken

Bijzondere aandachtspunten bij uitbesteding zijn veiligheidsincidenten. Op grond van art. 12 Bpr dient een financiële onderneming incidenten al te melden bij DNB.[147] Als er sprake is van een incident bij een inbesteder zal de uitbestedende financiële onderneming medewerking moeten hebben van de inbesteder bij het behandelen van het incident. Naast deze bestaande Wft-meldplicht is ook sprake van het voornemen van de Nederlandse wetgever om een nieuwe meldplicht (*security breach notification*) te introduceren naar aanleiding van de Diginotar-affaire.[148] Ook financiële ondernemingen zullen daarmee te maken krijgen.[149] Overigens wordt ook gewerkt aan een aparte meldplicht voor datalekken waarbij persoonsgegevens zijn betrokken. Die zal in de Wbp worden opgenomen.[150] Financiële ondernemingen worden voor een deel uitgezonderd van de verplichtingen uit de meldplicht. Deze uitzondering bleef in de nota van wijziging van april 2014 in stand.[151] In de Ontwerp-verordening gegevensbescherming van de Europese Commissie zal de meldplicht worden aangescherpt en krijgen ook bewerkers een eigen meldplicht.[152]

147 Voor de definitie van 'incident' zie art. 1 Bpr.

148 *Kamerstukken II* 2011/12, 26 643, nr. 202 (motie-Hennis-Plasschaert). Zie de uitwerking in de brief van de Nationaal coördinator Terrorismebestrijding en Veiligheid (2512000075/nctv/2012) van 6 juli 2012 aan de Tweede Kamer (voor de financiële sector specifiek p. 11 en p. 23-25). Zie ook het consultatiedocument van VGJ 'Wet melding inbreuken elektronische informatiesystemen' van 22/7/2013.

149 F. van der Jagt, 'Iets te melden', *NJB* 2012/1415.

150 *Kamerstukken II* 2012/2013, 33 662, nr. 1.

151 *Kamerstukken II* 2012/2013, 33 662, nr. 7.

152 Art. 31(2) of Proposal COM(2012)11 Final for a regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

6.4

UITBESTEDING VANUIT NEDERLAND NAAR HET BUITENLAND

6.4.1
Toepasselijk recht algemeen

Bij uitbesteding buiten Nederland blijft Nederlands recht van toepassing op de verwerking van de gegevens. Dat vloeit voort uit art. 4 van de Privacyrichtlijn en het daarvan afgeleide art. 4 lid 1 Wbp.

Wbp art. 4:

> '1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland.
> 2. Deze wet is van toepassing op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens.
> 3. Het is een verantwoordelijke als bedoeld in het tweede lid, verboden persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt overeenkomstig de bepalingen van deze wet. Voor de toepassing van deze wet en de daarop berustende bepalingen, wordt hij aangemerkt als de verantwoordelijke.'

6.4.2
Toepasselijk recht bij uitbesteding binnen de EU

Bij uitbesteding binnen de EU bestaat er een kleine uitzondering op deze hoofdregel. In navolging van art. 17 lid 3 van de Privacyrichtlijn bepaalt art. 14 lid 4 Wbp dat de buitenlandse bewerker gebonden is aan zijn nationale voorschriften op het gebied van beveiliging. Let op: art. 4 lid 2 Wbp verwijst anders dan art. 76 lid 2 Wbp *niet* naar de landen van de EER (Noorwegen, Liechtenstein en IJsland).

RL art. 17 lid 3:

> 'De uitvoering van verwerkingen door een verwerker moet worden geregeld in een overeenkomst of een rechtsakte die de verwerker bindt jegens de voor de verwerker verantwoordelijke en waarin met name wordt bepaald dat
> – de verwerker slechts handelt in opdracht van de voor de verwerking verantwoordelijke,
> – de in lid 1 bedoelde verplichtingen, zoals gedefinieerd door de wetgeving van de Lid-Staat waarin de verwerker is gevestigd, eveneens op deze persoon rusten.'

Wbp art. 14 lid 4:

> 'Is de bewerker gevestigd in een ander land van de Europese Unie, dan draagt de verantwoordelijke zorg dat de bewerker het recht van dat andere land nakomt, in afwijking van het derde lid, onder b'

6.4.3 Toeppasselijk recht bij uitbesteding buiten de EU

Als de bewerker is gevestigd buiten de EU, blijft de Wbp volledig van toepassing op de verwerking. Dat volgt eveneens uit art. 4 lid 1 Wbp. In dat geval geldt de uitzondering voor wettelijke regels betreffende beveiliging niet meer.

6.4.4 Toepasselijk recht bij uitbesteding vanuit buitenland naar Nederland

Binnen financiële concerns kan het voorkomen dat een buitenlands concernonderdeel de verwerking van gegevens uitbesteedt aan een Nederlands concernonderdeel. In dat geval moet het buitenlandse concernonderdeel op grond van art. 4 lid 3 Wbp een partij in Nederland aanwijzen als zijn vertegenwoordiger (verantwoordelijke). Een daarop aansluitend probleem is dat het retourverkeer moet voldoen aan de eisen voor grensoverschrijdend persoonsgegevensverkeer buiten de EU (zie hierna).[153]

153 Dat kan betekenen dat de door de bewerker aangewezen verantwoordelijke een model-contract (controller to controller) moet afsluiten met de opdrachtgever. Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, *PbEG* 2004, L 385/74 .

6.4.5
Doorgifte van persoonsgegevens buiten de EU

Uitbesteding gaat gepaard met verstrekking van persoonsgegevens (doorgifte) door de uitbesteder aan de inbesteder. Wanneer sprake is van uitbesteding van een verwerking binnen Europa is geen sprake van aanvullende eisen aan die doorgifte. Dat wordt anders als de inbesteder gevestigd is in een land buiten de EU. Op grond van art. 76 lid 1 Wbp is doorgifte buiten de EU alleen toegestaan als het ontvangende land beschikt over een voldoende niveau van bescherming van de persoonlijke levenssfeer (*adequacy*). De regels voor doorgifte vormen een aanvulling op de verplichtingen van de voor de verwerking van persoonsgegevens Nederlandse verantwoordelijke in Nederland.

Wbp art. 76 lid 1:

> 'Persoonsgegevens die aan een verwerking worden onderworpen of die bestemd zijn om na hun doorgifte te worden verwerkt, worden slechts naar een land buiten de Europese Unie doorgegeven indien, onverminderd de naleving van de wet, dat land een passend beschermingsniveau waarborgt.'

6.4.6
Adequacy decision

Op grond van art. 76 lid 2 Wbp geldt voor de EER (Noorwegen, Liechtenstein en IJsland) een adequacy-veronderstelling. Dat betekent dat een uitbesteding naar een EER-land wordt behandeld als een uitbesteding binnen de EU. Wbp art. 76 lid 2:

> 'In afwijking van het eerste lid kunnen persoonsgegevens die aan een verwerking worden onderworpen of die zijn bestemd om na hun doorgifte te worden verwerkt naar een land buiten de Europese Unie worden doorgegeven, indien dat land partij is bij de op 2 mei 1992 te Oporto tot stand gekomen Overeenkomst betreffende de Europese Economische Ruimte (Trb. 1992, 132), tenzij uit een besluit van de Commissie van de Europese Gemeenschappen of de Raad van de Europese Unie voortvloeit dat deze doorgifte is beperkt of verboden.'

De Europese Commissie kan bovendien bepalen dat individuele landen beschikken over een voldoende niveau van privacybescherming. Dat vloeit voort uit art. 25 lid 6 van de Privacyrichtlijn:

> 'De Commissie kan volgens de procedure van artikel 31, lid 2, constateren dat een derde land, op grond van zijn nationale wetgeving of zijn internationale verbintenissen, die het met name na de in lid 5 bedoelde onderhandelingen is aangegaan, waarborgen voor een passend beschermingsniveau in de zin van lid 2 biedt met het oog op de bescherming van de persoonlijke levenssfeer en de fundamentele vrijheden en rechten van personen. De Lid-Staten nemen de nodige maatregelen om zich naar het besluit van de Commissie te voegen.'

Dergelijke adequacy-beschikkingen zijn inmiddels voor diverse landen afgegeven. Het gaat om de volgende landen[154]:

AD Andorra
AR Argentina
CA Canada
CH Switzerland
FO Faeroe Islands
GG Guernsey
IL State of Israel
IM Isle of Man
JE Jersey
UY Eastern Republic of Uruguay
NZ New Zealand

Ten aanzien van de Verenigde Staten geldt een afwijkend regime: het niveau van privacybescherming binnen de Verenigde Staten wordt niet als voldoende beschouwd. Daarom heeft de Europese Commissie geen beschikking afgegeven dat er sprake is van 'adequacy' in de Verenigde Staten. In een op art. 25 lid 6 van de Privacyrichtlijn gebaseerde beschikking van de Europese Commissie is gekozen voor een systeem van gecontroleerde zelf-certificatie waar ondernemingen zich kunnen aanmelden bij het zogenaamde Safe Harbor-programma.[155] Zij dienen dan te voldoen aan de eisen die in de Safe Harbor-beschikking staan vermeld. Ondernemingen die deelnemen aan het Safe Harbor-programma, zeggen de Safe Harbor-spelregels te accepteren en onderwerpen zich aan het toezicht door de Federal Trade Commission of het ministerie van Vervoer van de Verenigde Staten.[156] Daarbij zij volledigheidshalve opgemerkt dat financiële ondernemingen in de VS als regel niet onder

154 http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-1
155 Beschikking 2000/520/EG van 26 juli 2000, *PbEG* 2000 L215/7.
156 Art. 2 lid 2 sub b juncto bijlage VII bij de Safe Harbor beschikking.

een Safe Harbor-regime zullen vallen, omdat ze niet vallen onder het toezicht van de Federal Trade Commission of het ministerie van Vervoer. Europese financiële ondernemingen kunnen natuurlijk wel werkzaamheden uitbesteden aan een niet-bancaire Amerikaanse opdrachtnemer die wel kan voldoen aan de randvoorwaarde van het toezicht. Die vallen dan meestal onder het toezicht van de FTC. De Amerikaanse overheid onderhoudt een website waarop kan worden nagegaan of ondernemingen deelnemen aan het Safe Harbor-programma.[157] Per onderneming wordt aangegeven wanneer de geldigheid van de melding verstrijkt. Tevens wordt aangegeven voor welke activiteiten het certificaat geldt. Als een onderneming bijvoorbeeld gecertificeerd is voor klantregistratiesystemen, is de certificatie niet geldig bij uitbesteding van een personeelsadministratie. Tussen de VS en de Europese Commissie wordt thans onderhandeld over herziening van de afspraken.[158]

Art.76 lid 3 Wbp bepaalt dat doorgifte naar een land met een onvoldoende niveau van bescherming van de persoonlijke levenssfeer toch is toegestaan als zich speciale omstandigheden voordoen zoals bijvoorbeeld uitwisseling binnen een sector waar wél sprake is van voldoende aanvullende bescherming. De verantwoordelijke kan deze beslissing nemen.[159] Voor zover mij bekend wordt van deze mogelijkheid niet of nauwelijks gebruikgemaakt. Naast art. 76 Wbp definieert art. 77 Wbp een aantal *uitzonderingen* waarbij doorgifte toch is toegestaan (zie hierna).

6.4.7
Uitzonderingen

In navolging van art. 26 van de Privacyrichtlijn bepaalt art. 77 Wbp dat in een aantal gevallen ook doorgifte van persoonsgegevens naar een *non adequate country* is toegestaan. Het gaat om de volgende gevallen:

Wbp art. 77 lid 1 sub a t/m f:

> 'In afwijking van artikel 76 kan een doorgifte of een categorie van doorgiften van persoonsgegevens naar een derde land dat geen waarborgen biedt voor een passend beschermingsniveau, plaatsvinden indien:

157 http://safeharbor.export.gov/list.aspx.

158 http://europa.eu/rapid/press-release_IP-13-1166_en.htm. Zie ook: COM(2013) 847 Communication from the Commission to the European parliPament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU.

159 *Kamerstukken II* 1999/2000 , 27 043, nr. 1, Toepassing van art. 25 en 26 van Richtlijn 95/46/EG (gegevensverkeer tussen de EU en derde landen).

a. de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft gegeven;
b. de doorgifte noodzakelijk is voor de uitvoering van een overeenkomst tussen de betrokkene en de verantwoordelijke, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
c. de doorgifte noodzakelijk is voor de sluiting of uitvoering van een in het belang van de betrokkene tussen de verantwoordelijke en een derde gesloten of te sluiten overeenkomst;
d. de doorgifte noodzakelijk is vanwege een zwaarwegend algemeen belang, of voor de vaststelling, de uitvoering of de verdediging in rechte van enig recht;
e. de doorgifte noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene, of
f. de doorgifte geschiedt vanuit een register dat bij wettelijk voorschrift is ingesteld en dat door een ieder dan wel door iedere persoon die zich op een gerechtvaardigd belang kan beroepen, kan worden geraadpleegd, voor zover in het betrokken geval is voldaan aan de wettelijke voorwaarden voor raadpleging;'

Het komt in de praktijk niet vaak voor dat een beroep op deze uitzonderingen wordt gedaan. In adviezen van de Artikel 29 Werkgroep wordt aangegeven dat deze uitzonderingen restrictief moeten worden toegepast.[160] Art. 77 lid 1 sub c Wbp zou overigens wel een rol kunnen spelen bij de inschakeling van partijen bij de afwikkeling van het betalingsverkeer.

Oorspronkelijk bepaalde de Wbp dat doorgifte, ook indien geen uitzondering van toepassing was, tot de mogelijkheden behoorde mits de exporteur over een vergunning van de minister van Justitie zou beschikken. Een dergelijke vergunning kon worden aangevraagd bij het Cbp en werd dan (automatisch) verleend door de minister van Justitie op voorwaarde dat de exporteur gebruikmaakte van door de Europese Commissie goedgekeurde modelcontracten. Voor de praktijk belangrijk is de recente wetswijziging (nieuwe art. 77 lid 1 sub g Wbp), die de vergunningplicht afschafte en het direct mogelijk maakte om op basis van goedgekeurde modelcontracten gegevens door te

160 WP12; DG XV D/5025/98; *Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, werkdocument Doorgifte van persoonsgegevens naar derde landen: toepassing van de artikelen 25 en 26 van de EU-Richtlijn betreffende gegevensbescherming*, goedgekeurd door de groep op 24 juli 1998; zie ook *Kamerstukken II* 1997/1998, 25 892, nr. 3, p. 195.

geven.[161] De Europese Commissie heeft enkele modelcontracten goedgekeurd. Bij uitbesteding gaat het om een modelcontract dat in 2010 is goedgekeurd. Het bevat een overzicht van de rechten en plichten van de uitbesteder en de inbesteder alsmede een sjabloon voor het beschrijven van de operationele details.[162]

Wbp art. 77 lid 1 sub g:

> 'In afwijking van artikel 76 kan een doorgifte of een categorie van doorgiften van persoonsgegevens naar een derde land dat geen waarborgen biedt voor een passend beschermingsniveau, plaatsvinden indien:
> g. gebruik wordt gemaakt van een modelcontract als bedoeld in artikel 26, vierde lid, van richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie 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 (PbEG L 281).'

In de praktijk betekent dit voor Nederland dat als de financiële onderneming en de inbesteder geen gebruik kunnen of willen maken van de modelcontracten, een exportvergunning moet worden aangevraagd. De aanvraag van een dergelijke vergunning kan worden gebaseerd op een alternatief contract dat voldoende waarborgen biedt.

Wbp art. 77 lid 2:

> 'In afwijking van het eerste lid, kan Onze Minister, gehoord het College, een vergunning geven voor een doorgifte of een categorie doorgiften van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt. Aan de vergunning worden de nadere voorschriften verbonden die nodig zijn om de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen, alsmede de uitoefening van de daarmee verband houdende rechten te waarborgen.'

Een andere mogelijk is dat de financiële onderneming en de inbesteder deel uitmaken van hetzelfde concern en dat concern beschikt over goedgekeurde

161 Wet van 26 januari 2012 tot wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen, Stb. 2012, nr. 33.

162 Beschikking 2010/87/EU van 5 februari 2010, *PbEU* 2010 L 39/5.

Binding Corporate Rules (BCR). In Nederland beschikken bijvoorbeeld de grootbanken over goedgekeurde BCR.[163] Dat betekent dat doorgifte naar buitenlandse vestigingen, ook in het kader van uitbesteding, op basis van de BCR kan plaats vinden.

6.4.8
Subcontracting door inbesteder

Bij outsourcing kan de inbesteder ook gebruikmaken van de diensten van externe partijen. Indien sprake is van een dergelijke uitbestedingsketen, blijft de uitbestedende financiële onderneming verantwoordelijk voor de gehele keten. In de praktijk zal dat er op neerkomen, dat in het contract tussen uitbesteder en inbesteder over de naleving van de Wbp nadere afspraken worden opgenomen over de inschakeling van derden door de inbesteder. De meest eenvoudige afspraak is dat de inbesteder geen derden mag inschakelen. Daarbij is het verstandig af te spreken dat onder een dergelijk inschakelen van derden door de inbesteder niet alleen de uitbesteding van werkzaamheden door inbesteder wordt verstaan, maar ook het inschakelen van externe partijen in het kader van onderhoud op de systemen van inbesteder. Immers, ook in het kader van onderhoud kan een derde partij toegang krijgen tot uitbestede productieomgevingen waar persoonsgegevens in aanwezig kunnen zijn. Indien partijen overeenkomen dat de inbesteder toch derden mag inschakelen, kan worden afgesproken dat de financiële onderneming vooraf wordt ingelicht en toestemming dient te verlenen. Een dergelijke toestemming kan aan voorwaarden worden onderworpen. Een voor de hand liggende voorwaarde is dat de inbesteder bepaalde voorwaarden die voor hem gelden, doorgeeft aan de derde partij. Een variant is dat de derde de overeenkomst tussen de uitbestedende financiële onderneming en de inbesteder mede ondertekent.

6.4.9
Subcontracting bij Safe Harbor en Modelcontracten

Indien de financiële onderneming contracteert met een Amerikaanse inbesteder die een Safe Harbor-certificatie bezit, kan volgens de Safe Harbor-beschikking de inbesteder gebruikmaken van de diensten van derden.

163 http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm.

Bijlage I bij Safe Harbor beschikking:

> "VERDERE DOORGIFTE': Wanneer een organisatie informatie bekendmaakt aan een derde, moet zij het kennisgevings- en het keuzebeginsel toepassen. Wanneer zij informatie wil doorgeven aan een derde die als haar vertegenwoordiger optreedt, zoals in de eindnoot wordt beschreven, mag dit indien zij zich er eerst van vergewist dat deze derde de Veiligehavenbeginselen onderschrijft, dan wel of de richtlijn of een andere vaststelling van gepastheid op hem van toepassing is, of indien zij een schriftelijke overeenkomst met deze derde aangaat waarin zij eist dat deze derde ten minste dezelfde bescherming van de persoonlijke levenssfeer biedt als de desbetreffende Veiligehavenbeginselen bieden. Indien de organisatie aan deze eisen voldoet, zal zij niet aansprakelijk worden gehouden (tenzij door de organisatie anders wordt overeengekomen) indien een derde partij waaraan de informatie is doorgegeven, deze verwerkt op een manier die strijdig is met eventuele restricties of verklaringen, tenzij de organisatie wist of had moeten weten dat de derde partij de informatie op een dergelijke manier zou verwerken, maar geen redelijke maatregelen heeft genomen om deze verwerking te voorkomen of stop te zetten.'

Als de uitbestedende financiële onderneming gebruikmaakt van het door de Europese Commissie goedgekeurde modelcontract voor uitbesteding is art. 11 uit dat model van belang:

Modelcontract Art. 11 Subverwerking

> '1. De gegevensimporteur besteedt de verwerkingsactiviteiten die hij overeenkomstig de bepalingen namens de gegevensexporteur uitvoert, niet uit zonder de voorafgaande schriftelijke toestemming van de gegevensexporteur. Indien de gegevensimporteur met toestemming van de gegevensexporteur zijn verplichtingen uit hoofde van de bepalingen uitbesteedt, dient hij met de subverwerker een schriftelijk contract te sluiten waarbij aan de subverwerker dezelfde verplichtingen worden opgelegd als die waaraan de gegevensimporteur uit hoofde van de bepalingen moet voldoen . Indien de subverwerker niet voldoet aan zijn verplichtingen tot gegevensbescherming uit hoofde van dat schriftelijke contract, blijft de gegevensimporteur jegens de gegevensexporteur volledig aansprakelijk voor de uitvoering van de verplichtingen van de subverwerker uit hoofde van dat contract.
> 2. In het tevoren tussen de gegevensimporteur en de subverwerker te sluiten schriftelijke contract dient tevens een derdenbeding te zijn opgenomen zoals vervat in bepaling 3, dat voorziet in gevallen dat de betrokkene

geen vordering tot schadevergoeding als bedoeld in bepaling 6, lid 1, kan instellen tegen de gegevensexporteur of de gegevensimporteur omdat deze feitelijk zijn verdwenen, hebben opgehouden rechtens te bestaan of insolvent zijn geworden, en er geen rechtsopvolger is die contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur heeft overgenomen. Deze aansprakelijkheid van de subverwerker jegens derden blijft beperkt tot de verwerkingswerkzaamheden die deze zelf heeft uitgevoerd krachtens de bepalingen.

3. Op de in lid 1 bedoelde bepalingen betreffende de gegevensbeschermingsaspecten van de subverwerking uit hoofde van het in lid 1 bedoelde contract is het recht van de lidstaat van vestiging van de gegevensexporteur van toepassing, te weten
4. De gegevensexporteur houdt een lijst bij van subverwerkingscontracten die krachtens de bepalingen zijn gesloten en door de gegevensimporteur overeenkomstig bepaling 5, onder j), zijn aangemeld, en werkt deze ten minste eenmaal per jaar bij. Deze lijst wordt ter beschikking gesteld van de toezichthoudende autoriteit voor gegevensbescherming die op de gegevensexporteur toezicht houdt.'

Daarnaast kan nog worden gewezen op een initiatief van de Artikel 29 Werkgroep om ook *Binding Corporate rules* voor bewerkers toe te laten.[164] Dat zou betekenen dat de inbesteder binnen zijn organisatie een *adequate level of protection* biedt en dat tevens *subcontracting* binnen de groep waar de inbesteder toe behoort zonder belemmeringen kan plaatsvinden.[165] Ten slotte is er ook nog een onderzoek gepubliceerd, eveneens van de Artikel 29 Werkgroep, naar modelbepalingen voor de uitbesteding door een bewerker naar een subbewerker.[166]

164 Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (WP 195). Explanatory Document on the Processor Binding Corporate Rules, adopted on 19 April 2013 by the Article 29 Data Protection Working Party, (WP 204).

165 Zie persbericht WP29 van 21-12-2012: '*The European data protection authorities, assembled in the Article 29 Working Party (WP29), have at their 88th plenary meeting decided to launch Binding Corporate Rules (BCR) for processors from 1 January 2013. BCR for processors are internal codes of conduct regarding data privacy and security, to ensure that transfers of personal data outside the European Union by a processor, who acts on behalf of his clients and under their instructions, will take place in accordance with the EU rules on data protection.*'

166 WP29: *Working document 01/2014 on Draft Ad hoc contractual clauses 'EU data processor to non-EU sub-processor'*, Adopted on 21 March 2014 (WP214).

6.5 CONCLUSIE

Het domein 'privacy, uitbesteding en financiële ondernemingen' blijft fors in beweging. Financiële ondernemingen dienen de ontwikkelingen nauwgezet te blijven volgen. Verplichtingen worden aangescherpt en sancties op nietnaleving worden verzwaard. De focus van het gegevensbeschermingsrecht komt steeds meer te liggen op accountability. De verantwoordelijkheden van ondernemingen worden meer in detail beschreven. Ook financiële ondernemingen moeten bij uitbesteding kunnen aantonen dat zij hun verantwoordelijkheid hebben genomen.

6.6 LITERATUUR

J.M.A. Berkvens, 'Clou(d)(t)sourcing binnen de financiële sector', *FR* 2012/12, p. 444 e.v.

CBP: Zienswijze inzake de toepassing van de Wet bescherming persoonsgegevens bij een overeenkomst met betrekking tot cloud computing diensten van een Amerikaanse leverancier, mededeling Cbp van 10 september 2012. Bron: http://www.cbpweb.nl/downloads_med/med_20120910-zienswijze-toepassing-wbp-SURFmarket-cloud-computing.pdf

T.E,M. Hooghiemstra en S. Nouwt, S., *SDU Commentaar Wet bescherming persoonsgegevens*, Den Haag: SDU 2e druk 2011.

N.P.H. Kruijsen, 'E-mail in de cloud: privacy in de prullenbak?'
Over de onevenwichtige situatie tussen enerzijds strafrechtelijke gegevensvordering door Amerikaanse opsporingsdiensten uit e-mails en anderzijds grondrechtelijke privacybescherming in de cloud', *P&I* 2013/1, p. e.v.

C. Kuner, '*The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law'*,Privacy & Security Law Report, 11 PVLR 06, 02/06/2012.

C. Kuner, *Transborder Data Flow Regulation in Data Protection and Privacy Law*, (diss.Tilburg UVT) 2012.

L. Moerel, *Binding corporate rules* (diss.Tilburg UVT), Amsterdam: 2011.

L. Viergever, 'Privacy in de clouds', *Tijdschrift voor Internetrecht*, 2010/3.

M.B. Voulon, 'Catch 22, Amerikaanse vorderingen tot het verstrekken van gegevens versus het verbod op doorgifte aan derde landen', *P&I* 2012/5, p. 214 e.v.

H.H. de Vries en N. Wisman, 'Doorgifte van persoonsgegevens onder de nieuwe Verordening', *P&I* 2012/3, p. 110 e.v.

WP29: *Opinion 05/2012 on cloud computing*, adopted July 1st 2012 by the Article 29 Data Protection Working Party (WP 196).

WP29: *Working document 01/2014 on Draft Ad hoc contractual clauses 'EU data processor to non-EU sub-processor'* Adopted on 21 March 2014 (WP214).