Bijlage 2

Specifiek commentaar

HOOFDSTUK I, ALGEMENE BEPALINGEN

Artikel 4

Definities *Betrokkene* en *Persoonsgegeven*
De definities van 'betrokkene' en 'persoonsgegeven' zijn onlosmakelijk aan elkaar gelinkt. Een persoonsgegeven wordt gedefinieerd als 'iedere informatie betreffende een betrokkene'. Iemand is betrokkene zodra te verwachten is dat deze redelijkerwijs met behulp van middelen kan worden geïdentificeerd. Dit gaat te ver. Om de lasten van compliance te beperken is er behoefte aan een definitie die gegevens slechts als persoonsgegevens aanmerkt als die in het licht van de context van de verwerking ook persoonsgegevens zouden moeten zijn.

Definitie van *Verwerking*
Persoonsgegevens zijn in het kader van gebruik door bedrijven informatie, die noodzakelijk is voor organisatiemanagement, klantgerichtheid, goed werkgeverschap, bedrijfsveiligheid, maatschappelijk verkeer en gegevensuitwisseling met de overheid. Aan de definitie van 'verwerking' ontbreekt dat vanuit organisaties de verwerking middel is om een organisatie administratief te voeren, ten behoeve van een dienst.

HOOFDSTUK II, BEGINSELEN

Artikel 6

Gerechtvaardigd ondernemersbelang
Gerechtvaardigd ondernemersbelang (6.1 f) geeft bedrijven de mogelijkheid om persoonsgegevens (onder voorwaarden) ook voor andere doeleinden aan te wenden dan waarvoor zij oorspronkelijk zijn verzameld. Uitgevers kunnen zo bijvoorbeeld een gratis proefexemplaar van een tijdschrift bijvoegen bij een magazine waarop een klant een abonnement heeft. In de huidige Richtlijn bestaat ruimte om gegevens te verwerken ten behoeve van de belangen van derden. Onder voorwaarde van een goede proportionaliteitstoets zou het gerechtvaardigd ondernemersbelang ook in de Verordening moeten gelden voor derde partijen, waaronder dochterondernemingen van de verantwoordelijke.

Artikel 7

Voorwaarden voor toestemming
De verantwoordelijke moet bijhouden of een persoon wel of geen toestemming heeft gegeven om zijn gegevens te verwerken. Dit artikel plaatst een zware last op de schouders van verantwoordelijken. Zeker als de definitie van persoonsgegeven zo breed is, zullen al snel veel en uitvoerige registers moeten worden bijgehouden over wie wel en wie geen toestemming heeft gegeven. Dit leidt tot de paradoxale situatie waarin –om bij te houden dat geen persoonsgegevens mogen worden verwerkt- alsnog persoonsgegevens worden verwerkt. Het is onmogelijk in dit geval het principe dataminimalisatie (niet meer gegevens verwerken dan nodig) te eerbiedigen. De conflicterende eis dient te worden opgelost of geschrapt.

Artikel 8

Verwerking van persoonsgegevens van kinderen
Niet de leeftijd moet leidend zijn voor het mogen verwerken van gegevens van kinderen, maar de legaliteit van het proces *waarvoor* gegevens worden verwerkt. Als een proces legaal is, dan mag de verwerking plaatshebben en vice versa. Daarnaast is het vaststellen van leeftijd via internet moeilijk. Vragen om een creditcard is een mogelijke oplossing (een kind heeft die niet), maar conflicteert met het principe van dataminimalisatie.

Artikel 9

Verwerking van bijzondere categorieën persoonsgegevens
Verwerking van bijzondere categorieën persoonsgegevens mag slechts onder bepaalde voorwaarden. Ten eerste behoeft de tekst aanpassing. Een verwerking van een persoonsgegeven m.b.t. etnische achtergrond is pas risicovol wanneer ook daadwerkelijk bedoeld is de etnische achtergrond te identificeren. Een pasfoto of naam veel weggeven over etnische achtergrond, terwijl deze in een niet-discriminerend proces verwerkt wordt.

Ten tweede worden in veel sectoren bijvoorbeeld strafrechtelijke gegevens verwerkt, in verband met onder meer fraudepreventie. Uitzondering voor gegevensverwerking in het kader van fraudemanagement of een interne risicoafweging bij het verkopen van een product op het gebied van arbeid, bank- of verzekeringssfeer ontbreekt. Het niet mogen verwerken van deze gegevens betekent een groot risico voor bovenstaande sectoren. Hiertoe dient de mogelijkheid te worden geboden, als niet in de Verordening, dan wel nationaal ter voortzetting van bestaande zelfreguleringsprotocollen.

HOOFDSTUK III, RECHTEN VAN DE BETROKKENE

Artikel 13

Rechten met betrekking tot ontvangers
Als persoonsgegevens op verzoek van de betrokkenen worden gewist of veranderd, moet de verantwoordelijke dit melden bij alle andere organisaties met wie deze gegevens heeft uitgewisseld over de betrokkene, tenzij dit onmogelijk is of een te grote moeite vereist. Ook met deze uitzondering kan deze verplichting onevenredig veel geld kosten. Gesuggereerd wordt een mogelijkheid in te voegen voor de verantwoordelijke om een afweging tussen kosten en belangen van de betrokkene te maken.

Artikel 14

Informatieverstrekking aan de betrokkene
Informatieverstrekking aan de betrokkene is goed voor transparantie en het vertrouwen in ondernemingen, maar de eisen om de betrokkene te laten weten welke derde partijen de informatie in opdracht van de verantwoordelijke verwerken, of dat gegevens in een ander land verwerkt worden gaan te ver. Deze leggen een te hoge last met navenante kosten op aan ondernemers, zeker omdat niet gedifferentieerd kan worden naar diverse processen bijvoorbeeld online aankopen, profiling, cameratoezicht, lunchreservering etc. Gesuggereerd wordt een mogelijkheid in te voegen voor de verantwoordelijke om een afweging tussen kosten en belangen van de betrokkene te maken.

Artikel 17

Recht om te worden vergeten en om gegevens te laten wissen
Het is te onduidelijk wat het *recht om vergeten te worden* voor impact gaat hebben op bepaalde sectoren. Zorgvuldige implementatie is gewenst. In alle redelijkheid kan niet gevraagd worden van ISP's of hosters van platforms (zoals online fora) om gegevens of reacties te verwijderen die door derden verder zijn getransporteerd dan de oorspronkelijke bron.

Gesuggereerd wordt een mogelijkheid in te voegen voor de verantwoordelijke om een afweging tussen kosten en belangen van de betrokkene te maken. Ook dient een uitzondering gemaakt te worden voor archiveren van gegevens die bijvoorbeeld gebruikt worden om disputen op te lossen, om fraude te bestrijden of vanuit journalistieke doeleinden worden gebruikt.

Artikel 20

Maatregelen op basis van profilering
Profilering is duidelijk een thema dat in de Verordening is geïntroduceerd met de online omgeving in het achterhoofd. Zoals in de inleiding genoemd zouden sectorspecifieke problemen niet moeten leiden tot algehele toepassing in de Verordening. In de huidige Richtlijn 95/46/EC bestaat al een onderdeel '*geautomatiseerde beslissystemen*'. Een onderscheid tussen geautomatiseerde beslissing en een geautomatiseerde beslissing *in het kader van profiling* zou beter moeten worden gemaakt. Het heeft de voorkeur het kopje 'profilering' te hernoemen naar '*geautomatiseerde beslissystemen*', omdat dit consistent is met de huidige richtlijn en het begrip profiling ook niet gedefinieerd is.

HOOFDSTUK IV, DE VOOR DE VERWERKING VERANTWOORDELIJKE EN DE VERWERKER

Algemeen
De praktijk leert dat – bijvoorbeeld door SaaS en Cloud computing – de processen van verantwoordelijke en bewerker steeds meer door elkaar heen lopen. Dit vraagt om een heldere scheiding van de twee, en om een heldere scheiding van de verantwoordelijkheden. De definitie in de Verordening maakt dit onderscheid juist minder helder. De Verordening dient duidelijker te stellen dat bevoegdheden die aan de verwerker worden toegekend uitsluitend met instemming verantwoordelijke kunnen worden uitgeoefend.

Artikel 24

Gezamenlijk voor de verwerking verantwoordelijken
Het concept van gemeenschappelijke verantwoordelijken is praktisch gezien lastig. Processen moeten minutieus beschreven worden en over elk proces dienen specifieke afspraken gemaakt. Dit zal veel juridisering (en kosten) opleveren.

Artikel 25

Vertegenwoordigers van niet in de Unie gevestigde voor de verwerking verantwoordelijken
Bedrijven die niet in de EU gevestigd zijn moeten een representant in de EU hebben. Juridische implicaties (eventuele boetes) voor het niet voldoen aan de Verordening kunnen direct worden verhaald op deze representant. Door de zwaarte van die consequenties zullen naar verwachting maar weinig bedrijven zich opwerpen om als representant te fungeren.

Artikel 28

Documenten
Documentatie zal zeer lastig zijn, zeker wanneer sprake is van de in artikel 24 genoemde gezamenlijke verantwoordelijkheid. Een veelheid van systemen zal moeten worden geïdentificeerd en de documentatie zal in die systemen moeten worden ingebouwd, zodat deze gemakkelijk elektronisch is te verkrijgen. Dat brengt hoge kosten van systeemaanpassing met zich mee.

Deze verplichting is daarnaast disproportioneel omdat deze zich uitstrekt tot vrijwel alle processen van de organisatie zonder enige mogelijkheid van vrijstelling. Niet alleen zal het in de praktijk vrijwel onmogelijk zijn om alle verwerkingen in het register te beschrijven en de beschrijvingen up-to-date te houden (denk bijvoorbeeld aan onbeduidende verwerkingen als het lijstje met contactgegevens van externe contactpersonen in de computer van iedere medewerker), het is ook niet nodig gelet op de risico's voor de persoonlijke levenssfeer van de betrokkenen. Een vrijstelling van deze verplichting op basis van feitelijke risico's is dan ook dringend gewenst.

Artikel 31 & 32

Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en betrokkene
De melding van een inbreuk in verband met persoonsgegevens dient verder te worden uitgewerkt alvorens in effect te treden. Wát precies een dergelijke inbreuk inhoudt is onduidelijk, maar kan worden beboet met een boete tot 1 miljoen Euro of 2% van de wereldwijde jaaromzet. Zonder meer rechtszekerheid is een dergelijke boete disproportioneel.

De meldplicht datalekken biedt, evenals het Nederlandse voorstel overigens, onvoldoende incentives voor organisaties om effectieve beveiligingsmaatregelen (denk bijvoorbeeld aan encryptie van gegevens) in te voeren teneinde de kans op nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen bij verlies of onrechtmatige verkrijging van gegevens te beperken. Zelfs als versleutelde gegevens worden gelekt, moet er namelijk op grond van de Verordening melding bij de toezichthouder plaatsvinden. Ook dit is disproportioneel en nodigt niet uit tot het nemen van afdoende beschermingsmaatregelen. Het ware dan ook beter om een algemene vrijstelling van de meldingsplicht te creëren ingeval de gegevens zijn versleuteld of anderszins onbegrijpelijk zijn gemaakt. Dus niet alleen voor de melding aan de betrokkene, maar ook voor de melding aan de toezichthouder.

Overigens lopen het Europese en nationale traject voor een meldplicht datalekken vanaf 2013 naar verwachting parallel. Het lijkt kapitaalvernietiging om bedrijven – met de Europese meldplicht in het zicht- te verplichten voor twee jaar aan een andere nationale wet te voldoen.

Artikel 33

Privacyeffectbeoordeling
Het uitvoeren van een Privacyeffectbeoordeling is alleen nodig als er sprake is van "specifieke risico's". Dergelijke risico's vaststellen kan echter alleen door een Privacyeffectbeoordeling. Dit is dus een cirkelredenering.

Voorts is het uitvoeren van een Privacy Impact Assessment nodig als er sprake is van "specifieke risico's". Het tweede lid noemt een aantal gevallen waarin die risico's worden verondersteld aanwezig te zijn. Dit betekent dat het eerste lid een ruimer bereik heeft dan alleen de in het tweede lid genoemde gevallen. In dat geval rijst de vraag wat precies verstaan moet worden onder "specifieke risico's". Bedoeld is wellicht "hoge risico's". Dit zou ook beter zijn, omdat elke verwerking, hoe klein ook, wel "specifieke risico's" kent. Het gaat echter om de vraag of die risico's groot of klein zijn

Artikel 36

Positie van de Data Protectie Officer (functionaris voor gegevensbescherming)
Feitelijk krijgt de Data Protectie Officer (DPO) Europeesrechtelijk de status van toezichthouder. Hij kan als onafhankelijke interne toezichthouder ('expert knowledege') de situatie ter plekke het best inschatten. Verduidelijkt moet worden dat de DPO medewerking aan de nationale toezichthouder verleent door zijn zienswijze met de toezichthouder te delen en dat de toezichthouder rekening heeft te houden met de zienswijze van de DPO;

De Amerikaanse *Federal Sentencing Guidelines* gaan uit van het controlecriterium 'expert advice'. Dit kan afkomstig zijn van een interne DPO, maar ook van een externe deskundige (advocaat, consultant). Het verplicht aanstellen van een DPO is derhalve niet de enige manier om aan het controlecriterium te voldoen. Het Amerikaanse voorschrift geeft ondernemers dus meer vrijheid om te bepalen hoe zij aan dit criterium willen voldoen.

HOOFDSTUK V, DOORGIFTE VAN PERSOONSGEGEVENS NAAR DERDE LANDEN OF INTERNATIONALE ORGANISATIES

Artikel 42

Doorgiften op basis van passende garanties
De modelcontracten dienen te worden aangepast aan de nieuwe regels voordat de Verordening in werking treedt. Daarbij dienen bepaalde onderdelen die toepassing van cloudoplossingen in de weg staan te worden geschrapt.

HOOFDSTUK VI, ONAFHANKELIJKE TOEZICHTHOUDENDE AUTORITEITEN

Proportionaliteit en rechtszekerheid
Onderzoek door een toezichthouder heeft grote impact op een bedrijf en vergt veel tijd en energie. Daarom is een maximum tijdsduur van onderzoek gewenst.

Non-discriminatie
De toezichthouder dient in haar toezicht af te gaan op daadwerkelijke schendingen van de Verordening en dient een bedrijf na onderzoek weer te behandelen als een bedrijf met een schone lei.

HOOFDSTUK VII, SAMENWERKING EN CONFORMITEIT

Artikel 66

Taken van het Europees Comité voor gegevensbescherming
De hoeveelheid ruimte voor extra eisen is aanzienlijk (o.m. delegatiebepalingen). Positief is dat deze bepalingen via politieke weg tot stand komen en belanghebbenden dus hun belang kunnen inbrengen. Toch zijn de officieel betrokken instituties eenzijdig: de Europese Data Protectie Board (alle 27 toezichthouders) en een 'Comité Mixe', hebben adviesfuncties. Een groep die vanuit het bedrijfsleven de belangen meeneemt is niet aanwezig. Hiervoor dient opening te zijn.

HOOFDSTUK VIII, BEROEP, AANSPRAKELIJKHEID EN SANCTIES

--

HOOFDSTUK IX, BEPALINGEN IN VERBAND MET SPECIFIEKE SITUATIES OP HET GEBIED VAN GEGEVENSVERWERKING

Artikel 80

Verwerking van persoonsgegevens en vrijheid van meningsuiting
Hier worden uitzonderingen gemaakt voor verwerking van persoonsgegevens in situaties waar de vrijheid van meningsuiting boven gegevensbescherming gaat. Voor de journalistieke vrijheid is dit artikel van groot belang. Het recht om vergeten te worden (artikel 17) dient ook bij archieven voor journalistieke doeleinden niet te gelden.

Artikel 81

Verwerking van persoonsgegevens over gezondheid
Het stuk over gegevens over gezondheid is te beperkt en sluit verwerking door voor de handliggende ondernemingen als opticiens en scholen uit, maar beperkt ook bijvoorbeeld ondernemers in sportwaren of manicure. Dit schaadt het maatschappelijk leven. Suggestie wordt gedaan niet meer uitzonderingen te introduceren, maar het artikel te verwijderen. Met het verwijderen van dit artikel dient wel onder artikel 9 een opening te worden geboden inzake het verwerken van gegevens over gezondheid.

Artikel 81 **c**
Het verwerken van gegevens over gezondheid is dus cruciaal voor meerdere sectoren. Mocht artikel 81 niet in zijn geheel worden geschrapt en artikel 9 een bredere basis bieden voor verwerking van deze gegevens dan dient de bepaling in artikel 81 c worden uitgebreid.

Artikel 82

Verwerking in het kader van de arbeidsverhouding
Lidstaten wordt toegestaan specifieke regels m.b.t. verwerkingen in de arbeidsverhouding te stellen. Dit zal niet bijdragen aan een homogene en consistente toepassing van het gegevensbeschermingsrecht in de EU. Voor zover er behoefte is aan een dergelijke bepaling, dient deze beperkt te worden tot de verwerking ten behoeve van de arbeidsrelatie als zodanig (arbeidsovereenkomst, controle op werknemer). De verwerking van gegevens betreffende betrokkenen die ook werknemer zijn voor algemene beheersdoeleinden dient uniform te blijven.

--