Bijlage bij briefnr. 12/10.363/DdN
d.d. 5 maart 2012

Bijlage 1

Algemeen commentaar

1. Geen echte Verordening, risico op divergentie aanwezig
   Een Verordening biedt doorgaans geen interpretatieruimte voor lidstaten en individuele toezichthouders en werkt daarmee harmoniserend: de wet is overal hetzelfde. Dit bevordert de interne markt en kan verschillende nationale regels die de uitrol van Europa-brede bedrijfsprocessen of IT-systemen vaak in de weg zitten uitschakelen.

   Een Richtlijn daarentegen geeft meer interpretatieruimte zowel voor ondernemers als voor toezichthouders van lidstaten. De ruimte voor interpretatie is voor ondernemers zeer belangrijk, geen enkel bedrijfsproces is immers hetzelfde en ondernemers moeten gegevens van klanten kunnen beschermen met maatwerk. Nadeel is echter dat nationale toezichthouders de wet verschillend kunnen interpreteren. Dat kan harmonisatie teniet doen.

   Met deze Verordening probeert de Europese Commissie het beste van de twee te nemen, maar ze slaagt daarin niet goed. Door ruimte voor interpretaties te bieden en tegelijkertijd precieze voorschriften op te schrijven is de Verordening uitvoerig en onduidelijk geworden en blijft het risico van divergentie bestaan.

   Om deze Verordening werkbaar te maken en niet te laten verzanden in 27 verschillende interpretaties, moet harmonisatie strak geregeld worden en dient interpretatieruimte die geboden wordt risicogericht te worden ingevuld. Om te voorkomen dat alsnog per lidstaat verschillende regimes ontstaan moet op cruciale interpretaties door toezichthouders de Europese Commissie uitspraken van toezichthouders toetsen.

2. Verplichtingen moeten risicogericht zijn, anders dreigen hoge kosten
   De Verordening schrijft precies voor bij welke bedrijfsgrootte bepaalde maatregelen zoals het aanstellen van een *Data Protection Officer* verplicht zijn. Het aantal werknemers is echter geen criterium om objectief een verhoogd risico voor persoonsgegevens vast te stellen. VNO-NCW en MKB-Nederland zijn van mening dat bedrijven middelen voor gegevensbescherming niet moeten inzetten omdat ze groot of klein zijn, maar vanuit een risicoafweging.

   Het voorstel heeft onvoldoende oog voor de feitelijke risico's en laat daardoor maatwerk voor beheersing van risico's niet toe. Dit betekent hoge kosten voor maatregelen op plaatsen waar deze gelet op de feitelijke risico's niet nodig zijn. Omgekeerd blijven mogelijk risico's onbeantwoord wanneer het een kleine organisatie betreft. De Verordening moet voorzien zijn van risicobenadering bij het adresseren van problemen en het voorschrijven van oplossingen.

3. Bestaande uitzonderingen voor verwerkingen moeten blijven bestaan
   In de huidige wet worden uitzonderingen gemaakt voor verwerkingen die geen risico vormen voor de persoonlijke levenssfeer van de betrokkenen (zie het Nederlandse Vrijstellingsbesluit). Dit soort generieke ontheffingen heeft zich in de afgelopen jaren goed bewezen, maar komt in de Verordening niet of nauwelijks voor. Bestaande vrijstellingen en andere regelingen zoals zelfreguleringen die door de toezichthouder zijn goedgekeurd dienen mutatis mutandis te worden voortgezet.

4. Specifieke maatregelen moeten alleen gelden voor specifieke sectoren
De Verordening geldt voor alle sectoren, hoe persoonsgegevens ook verwerkt worden. Het *recht om vergeten te worden, dataportabiliteit* en maatregelen voor *profiling*, zijn echter duidelijk geïnspireerd door de online omgeving. Deze verplichtingen gaan straks ook onverkort voor de offline omgeving gelden. Het zou naar het oordeel van VNO-NCW en MKB Nederland logischer zijn om deze problemen te benoemen in aparte regelgeving die zich specifiek richt tot de online omgeving.

5. Stapeling van wetten
Het brede bereik van de Verordening vergroot de kans op samenloop met andere administratieve verplichtingen, met name in gereguleerde sectoren. De bancaire sector, maar ook sectoren als de verzekeringssector en de gezondheidszorg kennen hun eigen regels met betrekking tot dataverwerking. De Verordening moet rekening houden met samenloop en ruimte bieden voor afwijkende verplichtingen in sectorale regelgeving die vaak ook afkomstig is uit Europese wet- en regelgeving.

De Europese Commissie wil met deze regels een voorbeeld stellen voor de rest van de wereld. De regels van deze Verordening moeten daarom ook in het buitenland gelden, zo wil de Commissie. Dit is echter niet haalbaar waardoor bedrijven die internationaal (in landen buiten de EU) zaken doen, worden verplicht te voldoen aan conflicterende regels. Dit brengt ondernemingen in een onmogelijke positie. De strijd wie de beste standaard voor gegevensbescherming neerzet, moet in de politiek gevoerd worden en niet over de rug van ondernemers.

6. De meldplicht datalekken mag niet leiden tot disproportionele administratieve lasten
VNO-NCW en MKB-Nederland wijzen er op dat het Europese voorstel voor een meldplicht datalekken leidt tot disproportionele administratieve lasten. Anders dan het Nederlandse wetsvoorstel datalekken (dit jaar in de Kamer) dat al forse investeringen vergt, vereist het Europese voorstel bovendien dat alle datalekken bij de toezichthouder worden gemeld. Ook datalekken die geen aanmerkelijke kans op nadelige gevolgen voor de betrokkene meebrengen.

Niet alleen stijgt hierdoor de hoeveelheid meldingen tot disproportionele hoogtes, het vergt ook veel arbeid en kosten om aan die verplichting te voldoen. De inzet van deze middelen onder bedreiging van de torenhoge boete voor niet-melden dreigt dan ten koste te gaan van het nemen van preventieve maatregelen, hetgeen juist een afname van de bescherming zou betekenen. Dit treft zowel het mkb als grote organisaties.

7. Kosten
De plicht om voorafgaand aan een verwerking dit te melden bij de toezichthouder wordt afgeschaft. De besparing hierdoor aan administratieve lasten wordt door de Europese Commissie geschat op 2,3 miljard euro per jaar voor de hele Unie.

Echter, als compenserende maatregel stelt de Europese Commissie een aantal verplichte beheersmaatregelen voor die ondernemingen en instellingen moeten invoeren in hun organisatie. Deze maatregelen betreffen:

- het verplicht bijhouden van een register met verwerkingen;
- het verplicht aanstellen van een *Data Protection Officer* (DPO);
- het verplicht uitvoeren van Privacy Impact Assessments.

In het voorstel mist een berekening van de nalevingkosten met betrekking tot de nieuwe maatregelen die waarschijnlijk hoog uitvallen. Zeker als de meldplicht datalekken mee wordt genomen in de berekening. De lastenverlichting van 2,3 miljard is dus een eenzijdig beeld.

Voordat een goed beeld van de reële kosten en baten bestaat, is niet te bepalen of de verplichtingen proportioneel zijn ten opzichte van de gewenste resultaten.

8. Technische tekst verhindert adoptie, mkb zal kennis moeten inkopen
   De voorgestelde tekst van de Verordening is zeer technisch en specialistisch van aard. Hierdoor is hij lastig te lezen voor bijvoorbeeld mkb'ers. Nu al is het wetteljik regime voor gegevensbescherming voor het mkb vaak onbegrijpelijk, waardoor goede toepassing lastig is. Implementatie zal ondernemers op kosten jagen omdat deze kennis zal moeten inkopen.

9. Verantwoordelijkheden voor privacy liggen door de gehele keten
   Niet alleen ondernemers hebben een verantwoordelijkheid. 'Vrienden worden' op een sociaal netwerk betekent dat de twee betrokkenen gegevens delen, hetgeen ook van hen verantwoordelijk gedrag vraagt. Burgers zouden zich bewuster moeten zijn van de risico's om persoonsgegevens van zichzelf en van anderen toe te vertrouwen aan het publieke domein. Dit vergt een inspanning aan de zijde van de overheid (o.a. publieksvoorlichting, Digibewust-lessen in het onderwijs).

   Daarnaast kan worden nagedacht over het beleggen van verantwoordelijkheden bij individuen die zich met de verwerking van persoonsgegevens bezighouden. Zo zou bijvoorbeeld de aansprakelijkheid van een bedrijf kunnen worden beperkt als er sprake is van opzet of bewuste roekeloosheid aan de kant van de werknemers. Dit zou de toezichthouder mee moeten nemen in haar sancties.

10. Vertaling
    Bij de vertaling van de Verordening, dienen wettelijke rolaanduidingen niet te worden vertaald, dit leidt tot ruis en daarmee divergentie. De vertaling van *Data Controller* en *Processor* leveren misverstanden op. De Nederlandse vertalingen Verantwoordelijke en Bewerker roepen andere associaties op. De Verordening gaat uit van regie door het verantwoordelijke bedrijf. *Data Controller* sluit daarbij goed aan. Een Processor *verwerkt* in plaats van bewerkt.