Nederlandse Vereniging van Banken

Leonie van der Spek-Lolkema
Adviseur Juridische zaken & privacy
t + 31 20 55 02 831
m + 31 6 55 72 06 95
e spek@nvb.nl

Ministerie van Veiligheid en Justitie
G.A. van der Steur
Postbus 20301
2500 EH DEN HAAG

Datum 20 januari 2017
Referentie BR2586

Betreft: Internetconsultatie Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)

Geachte heer Van der Steur,

Graag maken wij gebruik van de mogelijkheid te reageren op het consultatiedocument van 9 december 2016 betreffende de 'Regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming)'.

Wij zijn positief over de nadere uitwerking en toelichting op de Algemene Verordening Gegevensverwerking (AVG) in de Memorie van toelichting. Gezien de vele onduidelijkheden die na bestudering van de AVG bestaan, is dit een welkome verduidelijking.

De opbouw van deze reactie is als volgt. In het eerste deel van de bijlage bij dit document zijn enkele belangrijke aandachtspunten uitgewerkt over zowel het wetsvoorstel als de daarbij behorende Memorie van toelichting. In het tweede deel van de bijlage treft u enkele losse punten aan die wat ons betreft aandacht behoeven. Dit betreft kennelijke verschrijvingen of mogelijke inconsistenties.

De Nederlandse Vereniging van Banken (NVB) onderschrijft het belang van het instellen van een privacy toezichthouder die een heldere en stevige positie heeft zowel in Nederland als in het Europese werkveld. Vanuit de banken bestaat behoefte dat de Autoriteit Persoonsgegevens (AP) ook optreedt als gesprekspartner als het om branche brede onderwerpen gaat.

Wij juichen de wijze van implementatie van de Algemene Verordening Gegevensbescherming toe en hopen dat de punten die wij onder uw aandacht brengen hierop aanvulling brengen. Vanzelfsprekend zijn wij tot nadere toelichting bereid.

Met vriendelijke groet,

Eelco Dubbeling
Directeur

Bijlage 1: Deel 1

Minderjarigen (Artikel 5 UAVG en artikel 8 AVG)

In de Memorie van toelichting is een implementatietabel opgenomen. Daarin is aangegeven dat niet is gekozen om de lidstaatoptie die artikel 8 AVG biedt in te vullen. Hiermee blijft de leeftijd waarop een dienst van de informatiemaatschappij kan worden aangeboden door een verwerkingsverantwoordelijke zonder toestemming van de wettelijk vertegenwoordiger 16 jaar. De NVB is van mening dat dit – in de huidige tijd – niet meer goed verdedigbaar is. Het staat te ver weg van wat maatschappelijk gebruikelijk is en zal tot praktische problemen leiden. Op basis van het wetsvoorstel is het voor een minderjarige niet mogelijk om bijvoorbeeld in een app toestemming te geven voor het plaatsen van cookies of om toestemming te geven voor het gebruik van biometrische gegevens voor beveiligingsdoeleinden (bijvoorbeeld voor het gebruik van de vingerafdruk om toegang te krijgen tot een beveiligde bancaire app). De NVB is dan ook voorstander voor een verlaging van deze leeftijd en de ruimte die de AVG biedt in te vullen. Daarbij kan in de onderbouwing wellicht aansluiting worden gezocht bij artikel 1:234 BW waarin is omschreven dat toestemming door de wettelijk vertegenwoordiger verondersteld wordt te zijn gegeven voor handelingen die in het maatschappelijk verkeer gebruikelijk zijn.

Toestemming

Anders dan in de huidige regelgeving, kent de AVG een zelfstandig artikel gewijd aan de eisen die gesteld worden aan het geven van toestemming. Deze eisen werden eerder niet expliciet in de wet benoemd. Niet duidelijk is of een door betrokkene gegeven toestemming voorafgaand aan de inwerkingtreding van de AVG wordt geacht geldig te zijn gegeven in overeenstemming met artikel 7 AVG. Als dit niet het geval is zal dit tot praktische problemen leiden. Er zal dan in tal van situaties opnieuw toestemming moeten worden gevraagd. Dit lijkt niet de bedoeling van de Europese wetgever te zijn. De NVB pleit ervoor dit in de Memorie van toelichting te verduidelijken. De NVB is voor een regeling die er op ziet dat een eerder gegeven toestemming rechtsgeldig blijft, totdat de toestemming wordt ingetrokken.

Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten (artikel 31 UAVG)

Voor dit artikel zien wij een aantal aandachtspunten:

- In de Memorie van toelichting ontbreekt de nadere uitwerking van wat verstaan wordt onder strafrechtelijke veroordelingen en strafbare feiten. Nu deze omschrijving anders is dan de huidige bepaling van artikel 16 Wet bescherming persoonsgegevens (WBP)- waarin gesproken wordt over 'strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag'- stellen wij voor om in de Memorie van toelichting te verduidelijk of het begrip hiermee wijzigt en een toelichting te geven op het begrip. Uit de bewoordingen van de AVG maken wij op dat het begrip 'strafrechtelijke veroordelingen en strafbare feiten' in de AVG strikter is dan het begrip dat nu in de WBP wordt gehanteerd. Zo kwalificeren bijvoorbeeld tuchtrechtelijke veroordelingen volgens het regime van de WBP wel als strafrechtelijke gegevens, maar is dit – naar onze mening - niet het geval op basis van de bewoordingen in de AVG. Wij stellen voor deze striktere interpretatie te verduidelijken in de Memorie van toelichting. Dit draagt bij aan meer rechtszekerheid en transparantie richting betrokkenen.

- In het huidige juridische kader is een strafrechtelijk gegeven een bijzonder persoonsgegeven (artikel 16 WBP), waardoor ook artikel 23 WBP op de verwerking van deze gegevens van toepassing is. Nu persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten zoals beschreven artikel 10 AVG niet onder de definitie van bijzondere persoonsgegevens vallen, zijn ook de uitzonderingen zoals benoemd in artikel 9 AVG niet van toepassing. De uitzonderingen zoals genoemd in artikel 9 AVG komen overeen met de uitzonderingen zoals geformuleerd in het huidige artikel 23 WBP. Naar onze mening zou het – mede vanwege de beleidsneutrale implementatie – in de rede liggen om de uitzonderingen zoals nu genoemd in artikel 23 WBP en opgenomen in artikel 9 AVG ook van toepassing te verklaren op artikel 31 UAVG.
- De verwerking van strafrechtelijke veroordelingen en strafbare feiten ten behoeve van derden niet zijnde andere groepsmaatschappijen van de verwerkingsverantwoordelijke is alleen mogelijk als de AP daartoe eerst toestemming heeft verleend. Dit volgt uit artikel 31 UAVG lid 1, c 3e. Onder het regime van de WBP is de voorwaarde om strafrechtelijke gegevens ten behoeve van een derde te mogen verwerken dat eerst een voorafgaand onderzoek wordt gevolgd (artikel 31 WBP). Hoe verhoudt deze toestemming zich tot het voorafgaand onderzoek? Daarnaast ontstaat de vraag of de door de AP of haar voorganger verrichte en afgeronde voorafgaande onderzoeken met een positieve uitkomst beschouwd mogen worden als een reeds verleende toestemming zoals bedoeld in artikel 31 UAVG. De NVB gaat er vanuit dat dit het geval is. Graag zien wij dit in de Memorie van toelichting bevestigd.
- Artikel 31 lid 4 van het wetsvoorstel bepaalt dat de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen is toegestaan indien dit gebeurt door en ten behoeve van publiekrechtelijke samenwerkingsverbanden van verwerkingsverantwoordelijken of groepen van verwerkingsverantwoordelijken. Bepaalde vormen van criminaliteit zoals bijvoorbeeld vastgoedfraude of terrorismefinanciering nopen om onderzoek te doen naar betere en efficiëntere manieren van criminaliteit- en fraudebestrijding. Het maatschappelijk belang is groot. Ook de overheid stuurt op een nauwere samenwerking tussen publieke en private partijen inzake criminaliteit- en fraudebestrijding. Artikel 10 AVG biedt hiertoe ruimte aan de lokale wetgever. Artikel 31 lid 4 UAVG kan hierin voorzien als het artikel met een enkel woord wordt aangepast: “De verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen is toegestaan indien dit geschiedt mede ten behoeve van publiekrechtelijke samenwerkingsverbanden van …[…].

Verhouding tot andere toezichthouders (artikel 21 UAVG en pagina 32 MvT)

De NVB pleit voor verduidelijking van de taakverdeling van de AP. Zodat het voor banken duidelijk is hoe het toezicht voor de verwerking van persoonsgegevens voor de financiële sector is vormgegeven.

In artikel 21 UAVG wordt de AP de bevoegdheid toegekend om – net als nu weergegeven in artikel 51 WBP – afspraken met andere toezichthouders te maken over de verwerking van persoonsgegevens. Daarnaast is op pagina 32 paragraaf 3.1.1. eerste alinea MvT aangegeven: '*De AP is ook als enige en daarmee leidende, toezichthouder verantwoordelijk voor de uitvoering van de samenwerking tussen toezichthoudende autoriteiten en voor de conformiteitstoetsing (Hoofdstuk VII).*' Er zijn echter ook situaties denkbaar dat AP niet de leidende toezichthouder is, bijvoorbeeld in de situatie waarin niet de AP een onderzoek initieert maar een andere toezichthouder. In Hoofdstuk VII wordt namelijk de samenwerking geregeld tussen de toezichthouders, waarbij het van het onderwerp van het onderzoek, maatregel, etc. afhankelijk is welke toezichthouder verantwoordelijk is voor de uitvoering van de samenwerking.

Ook voor de samenwerking die tussen diverse partijen mogelijk is, vraagt de NVB aandacht. Banken worden regelmatig – los van de AP – benaderd door andere toezichthouders, zoals AFM die zich vanuit hun toezichthoudende taak vanuit de Wft ook bezig houden met de privacy van de klant en gegevensverwerking. ACM houdt toezicht op de cookieregelgeving en het gebruik van locatiegegevens. Hierdoor is niet altijd duidelijk wat de verhoudingen tussen de toezichthouders zijn en of er afspraken zijn en/of gezamenlijk toezicht is. Dit betekent niet alleen een toename van rechtsonzekerheid, maar mogelijk ook van administratieve lasten.

Geautomatiseerde individuele besluitvorming (artikel 38 UAVG)

Dit artikel regelt kortgezegd dat het verbod op geautomatiseerde individuele besluitvorming zoals opgenomen in artikel 22 van de AVG niet geldt als dit noodzakelijk is om te voldoen aan een wettelijke verplichting. Dit is een welkome en zelfs noodzakelijke uitzondering, waar de NVB dan ook achter staat. Op pagina 43 van het wetsvoorstel wordt uitleg gegeven over wat wordt bedoeld met "wettelijke verplichting". Dit ziet op artikel 6 lid 1 AVG. Het gaat niet alleen om een wetsregel in formele zin: "Denkbaar is ook dat verwerking van persoonsgegevens een basis vindt in een ruimer geformuleerde zorgplicht". De NVB neemt aan dat deze uitleg met betrekking tot de wettelijke verplichting ook geldt in het geval van artikel 38 UAVG. De NVB zou dit graag verduidelijkt willen zien in de Memorie van toelichting bij artikel 38 UAVG (pagina's 84 en 85). De Memorie van toelichting geeft nu slechts voorbeelden uit de publieke sector om meer duiding te geven aan deze uitzondering. Suggestie van de NVB is om hier dan ook één of meerdere voorbeelden uit de private sector te noemen. Denk hierbij bijvoorbeeld aan de wettelijke zorgplicht die banken op diverse onderwerpen hebben te hanteren. Ook hier is, net als in het voorbeeld uit de publieke sector, geen specifieke wettelijke grondslag voor de geautomatiseerde individuele besluitvorming, maar slechts een algemene. Een ander voorbeeld is artikel 114 Besluit Gedragstoezicht financiële ondernemingen Wft, waarin het volgende is opgenomen: ***'Alvorens met een consument een overeenkomst inzake krediet aan te gaan waarvan het totale kredietbedrag meer dan € 250 bedraagt, raadpleegt een aanbieder van krediet de bij het stelsel van kredietregistratie waaraan hij deelneemt geregistreerde gegevens over reeds aan de consument verleende kredieten.'*** Hierin staat weliswaar niet letterlijk dat dit met behulp van geautomatiseerde individuele besluitvorming dient plaats te vinden, maar in de praktijk zal dit vanwege de zeer geringe beoordelingsruimte de facto veelal wel gebeuren. Een ander voorbeeld is het automatisch besluit om een transactie op te schorten of te stoppen als de bancaire systemen detecteren dat een pinpas in twee verschillende landen tegelijk wordt gebruikt (wegens fraude) of het gebruik van profielen en besluiten om cyberaanvallen op de bancaire systemen te bestrijden. Graag zou de NVB zien dat hieraan aandacht wordt besteed in de Memorie van toelichting.

Direct marketing op basis van gerechtvaardigd belang (MvT p. 48)

In de Memorie van toelichting (pagina 48, derde alinea) is opgenomen: 'Verdere verwerking voor zuiver commerciële doelstellingen zoals het gericht kunnen aanbieden van reclame, ... kan alleen met uitdrukkelijke toestemming van de betrokkene.'
Deze alinea strookt niet met de structuur van het privacyrecht en meer specifiek de Verordening waar in overweging 47 ons inziens terecht is opgenomen dat marketing is toegestaan op basis van het gerechtvaardigd belang, zie de laatste zin: 'De verwerking van persoonsgegevens ten behoeve van direct marketing kan worden beschouwd als uitgevoerd met het oog op een gerechtvaardigd belang'. In een dergelijk geval heeft de verwerkingsverantwoordelijke de verplichting om vast te stellen of de betreffende marketing verenigbaar is. En geldt voor de betrokkene een recht van bezwaar: 'tegen de verwerking van hem betreffende persoonsgegevens voor dergelijke marketing' (artikel 21 lid 2 AVG). De NVB stelt voor om deze alinea te vervangen door een alinea die recht doet aan bovenstaande uitleg zoals bijvoorbeeld: '*Verdere verwerking voor zuiver commerciële doelstellingen zoals het gericht aanbieden van reclame kan plaatsvinden op basis van het gerechtvaardigd belang. In dat geval heeft de verwerkingsverantwoordelijke de verplichting om een belangenafweging te maken en daarmee vast te stellen of de betreffende marketing gerechtvaardigd is.* '

Biometrische gegevens (artikel 26 UAVG)

De NVB juicht het ten zeerste toe dat de wetgever de mogelijkheid heeft benut om in bepaalde gevallen gebruik te maken van haar recht om een nationale uitzondering te maken op het verbod om biometrische gegevens te verwerken. Tegelijkertijd roept de redactie van artikel 26 de nodige vragen op waar de MvT slechts ten dele antwoord op geeft. Zo besteedt de wetgever op pagina 80 MvT ons inziens terecht aandacht aan het feit dat biometrische systemen sterk in opkomst zijn en dat deze ontwikkelingen in zowel de publieke als de private sector doorgang moeten kunnen vinden. Zo niet, zou Nederland zich hiermee in de vingers snijden als innovatieve economie. De MvT beperkt zich vervolgens tot een opmerking met betrekking tot de werkgever - werknemer relatie. De NVB zou graag één of meerdere voorbeelden uit de klant - aanbieder relatie opgenomen zien waarbij de uitzondering op het verbod om biometrische gegevens te verwerken van toepassing is. Het volgende voorbeeld kan ter inspiratie dienen: het beveiligen van bankkluizen. Banken krijgen wel eens klachten van klanten omdat er zaken uit de door hen gehuurde bankkluis ontvreemd zouden zijn. Sommige banken overwegen de optie om de ruimte waar deze kluizen zich bevinden te beveiligen met behulp van biometrie, vingerafdruk in dit geval. De klant sluit een overeenkomst met de bank over het gebruik van de kluis en de toegang daartoe. Ons inziens zou het gebruik van biometrie onderdeel uitmaken van deze overeenkomst en daarom op grond van artikel 26 UAVG moeten zijn toegestaan. Graag zien wij dit of een vergelijkbaar voorbeeld opgenomen in de MvT ter verduidelijking van artikel 26.
Op pagina 49 Memorie van toelichting staat naar onze mening ten onrechte gelaatsherkenning als biometrisch gegeven vermeld. Naar wij begrijpen is gelaatsherkenning een proces en gelaatskenmerken zijn de biometrische gegevens.

Verder vragen wij ons af in hoeverre bij een foto die eenmaal is opgeslagen, nadat deze is verwerkt, sprake is van een biometrisch gegeven. De tekst die daarover gaat op p. 49 in de MvT is overgenomen uit overweging (51) van de AVG maar deze verschaft op dit punt geen duidelijkheid.

Toepassingsgebied

Op pagina 72 t/m 74 MvT bij artikel 3 Toepassingsgebied. Bij de implementatie van artikel 3 AVG heeft de Nederlandse wetgever voor de volgende uitleg gekozen: indien sprake is van een verwerkingsverantwoordelijke die gevestigd is binnen de Unie maar in een andere lidstaat dan Nederland en de verwerking (Betrokkene) vindt plaats in Nederland, is het nationaal recht van die andere lidstaat van toepassing. Terwijl in de situatie dat de verwerkingsverantwoordelijke buiten de Unie is gevestigd, Nederlands recht van toepassing is op een verwerking die in Nederland plaatsvindt. Zie tabel p. 74 3e en 5e regel. Dit betekent dat een betrokkene in Nederland die bijvoorbeeld gebruik maakt van online dienstverlening te maken kan krijgen met twee verschillende rechtstelsels afhankelijk van de vestigingsplaats van de verwerkingsverantwoordelijke. Het is de vraag of deze uitleg strookt met de AVG nu met deze uitleg de transparantie en rechtszekerheid voor betrokkene niet voorop wordt gesteld.
Zie ook de MvT, p. 73 laatste zin: De hoofdregel in deze is dat de toezichthoudende autoriteit competentie heeft op het grondgebied van haar lidstaat.
Zie in dit kader ook overweging (122): Elke toezichthoudende autoriteit dient op het grondgebied van haar lidstaat bevoegd te zijn om de bevoegdheden en taken uit te oefenen die haar overeenkomstig deze verordening zijn toegekend. Daaronder dienen met name te vallen: de verwerking in het kader van de activiteiten van een vestiging van de verwerkingsverantwoordelijke of de verwerker op het grondgebied van zijn eigen lidstaat, de verwerking van persoonsgegevens door overheidsinstanties of particuliere organen die optreden in het algemeen belang, **verwerking die gevolgen heeft voor betrokkenen op haar grondgebied**, of verwerking, door een niet in de Unie gevestigde verwerkingsverantwoordelijke of verwerker, gericht op betrokkenen die op haar grondgebied verblijven. Ook het behandelen van door een betrokkene ingediende klachten, het evalueren van de toepassing van deze verordening en het beter bekend maken van het brede publiek met de risico's, regels, waarborgen en de rechten in verband met de verwerking van persoonsgegevens dienen daaronder te vallen.

Tenslotte vragen wij nog aandacht voor het misbruik van recht bij inzageverzoeken, zoals nu verwoord in hoofdstuk III van de AVG en pagina 67 van de MvT. Steeds vaker wordt door de leden van de NVB geconstateerd dat partijen – bijvoorbeeld in verband met (terechte) BKR registraties of in verband met juridische procedures en klachten– namens betrokkene om inzage verzoeken. Betrokkenen betalen deze partijen voor hun diensten. Uiteraard zijn banken bereid om medewerking te verlenen aan een verzoek om inzage van een betrokkene, maar voorkomen moet worden dat dit recht gebruikt wordt als fishing expedition voor het verbeteren van een procespositie zonder dat de juistheid en de rechtmatigheid van een verwerking ter discussie staat. Ook dient voorkomen te worden dat dit als alternatief wordt gebruikt voor artikel 843 Rv voorafgaand aan gerechtelijke procedures of in het kader van klachten.

Bijlage 1 Deel 2

- In het algemeen geldt dat niet in alle gevallen duidelijk is of een verwijzing naar een andere verordening, richtlijn of wet(sartikel), een verwijzing is naar de UAVG, de Verordening (AVG), Richtlijn 95/46 of een andere wet. Voorstel is om dit meer consistent te maken.
- In de toelichting bij artikel 19 UAVG wordt verwezen naar een PM. Graag zou de NVB nog voordat deze wet wordt ingediend de mogelijkheid hebben om hierover geconsulteerd te worden.
- Artikel 20 UAVG benoemt expliciet beleidsregels in lid 1 sub a. Wat is de status van een beleidsregel? In hoeverre komt de definitie van een Beleidsregel zoals AFM die hanteert overeen met de beleidsregel die de AP openbaar kan maken?

'Onder een beleidsregel verstaat de AFM een schriftelijk beleidsuiting dat een of meer algemene en voor herhaalde toepassing vatbare regels bevat over het gebruik van een bevoegdheid van de AFM. Daarnaast kan het ook een algemene voor herhaalde toepassing vatbare regel over de afweging van belangen of de vaststelling van feiten inhouden.'

- In de aanhef van artikel 24 UAVG sluiten de woorden 'niet' en 'tenzij' niet op elkaar aan. We stellen voor om tenzij te vervangen door: 'wanneer' of 'en'
- In artikel 31 lid 3 is de formulering van de tekst niet duidelijk, waardoor niet goed duidelijk is wat met dit lid bedoeld wordt.
- In artikel 42 UAVG wordt gebruik gemaakt van terminologie uit de Wbp terwijl in de AVG voor een meer algemene formulering wordt gekozen. Het gaat om de woorden "instellingen en diensten". De AVG verwijst naar de verwerkingen van persoonsgegevens voor (1) archivering in het algemeen belang, (2) wetenschappelijk of historisch onderzoek, of (3) statistische doeleinden zonder te verwijzen naar een specifieke soort verwerkingsverantwoordelijke. Het lijkt alsof de formulering in het wetsvoorstel een beperking inhoudt ten opzichte van het bepaalde in de AVG. Met name R&D afdelingen van private partijen kunnen analyses uitvoeren op basis van geavanceerde technieken binnen de kaders van deze bepalingen. Om ervoor te zorgen dat geen twijfels ontstaan over welke verwerkingsverantwoordelijken zich op dit artikel kunnen beroepen, stelt de NVB voor om de tekst van de AVG zoveel mogelijk te volgen en de woorden "instellingen en diensten" te schrappen. Hierbij nog enkele tekstsuggesties:
    - P. 89, tweede paragraaf, 5e regel: "Hoewel de bepaling van de verordening verschilt in de formulering, is de strekking van deze uitzondering gelijkblijvend".
    - P. 89, tweede paragraaf laatste zin. "Het continueren van de bestaande bepaling van artikel 44, eerste lid, van de Wbp over deze uitzonderingen ligt hiermee voor de hand."
- Pagina 41 MvT alinea 4.2.1, eerste zin. In deze zin is nu opgenomen dat ingevolge artikel 5 van de AVG een verwerking 'eerlijk' moet zijn. Dit wijkt af van de tekst van artikel 5 AVG. Daarin wordt gesproken over 'behoorlijk.'
- Pagina 43, 4e alinea, 4e zin. Aan het einde van de zin "...de goede vervulling van een publiekrechtelijke taak." ontbreekt een deel van de tekst.
- Pagina 61, alinea 5.2.3, voorlaatste zin, hier mist een deel van artikel 30 lid 4 AVG: "Desgevraagd stellen .... het register ter beschikking van de toezichthoudende autoriteit." Daarom stellen wij voor om de deze zin als volgt aan te vullen, zie in cursief: ... "verplicht om het register ter beschikking te stellen aan de toezichthoudende autoriteit *indien deze daarom verzoekt*."
- Pagina 62, 5.2.4, Beveiliging van de verwerking. Regel 9: Gedragscodes lijken ons geen geëigend middel om een op het risico afgestemd beveiligingsniveau te waarborgen.
- Pagina 64, tweede alinea laatste regel. Gezien de tekst van artikel 35 lid 9: "vraagt in voorkomend geval" lijkt ons dat dit niet 'dienen' zou moeten zijn, maar 'mogen'.
- Op pagina 67 MvT: 3e alinea. In deze passage wordt gesproken over 'gegevens'. Naar mening van de NVB is hier bedoeld 'informatie'. In dezelfde zin wordt gesproken over 'gemeld'. Dit zou 'verstrekt' moeten zijn.
- Pagina 71 Artikel 2 derde alinea laatste zin, de volgende suggestie ter verduidelijking: Blijkens overweging 16 bij de verordening kan ~~hier~~ worden gedacht aan activiteiten betreffende de nationale veiligheid, ~~als~~ zijnde activiteiten die buiten de werkingssfeer van het Unierecht vallen.
- Pagina 79 eerste alinea, regel 5. Deze regel loopt niet lekker, daarom de volgende suggesties: Hier kan aan worden gedacht ~~wanneer~~ bij~~voorbeeld~~ een last onder dwangsom, ~~die~~ wanneer onmiddellijk door degene aan wie de last is opgelegd ~~onmiddellijk voldoet~~ wordt voldaan aan hetgeen in de last is opgelegd.