GROEP GEGEVENSBESCHERMING ARTIKEL 29

17/NL

WP 248 rev.01

Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679

Vastgesteld op 4 april 2017

Zoals laatstelijk gewijzigd en vastgesteld op 4 oktober 2017

DE GROEP VOOR DE BESCHERMING VAN NATUURLIJKE PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS

ingesteld bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995,

gezien de artikelen 29 en 30,

gezien haar reglement van orde,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD:

Inhoudsopgave

I. Inleiding

Verordening 2016/679[1] (algemene verordening gegevensbescherming, hierna "AVG") is van toepassing vanaf 25 mei 2018. In artikel 35 van de AVG wordt het concept "gegevensbeschermingseffectbeoordeling"[2] geïntroduceerd, net als in Richtlijn 2016/680[3].

Een gegevensbeschermingseffectbeoordeling is een proces dat is bedoeld om de verwerking van persoonsgegevens te beschrijven, de noodzaak en evenredigheid ervan te beoordelen en de daaraan verbonden risico's voor de rechten en vrijheden van natuurlijke personen te helpen beheren[4] door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken. Gegevensbeschermingseffectbeoordelingen zijn belangrijke verantwoordingsinstrumenten omdat ze verwerkingsverantwoordelijken niet alleen helpen om aan de eisen van de AVG te voldoen, maar ook om aan te tonen dat passende maatregelen zijn genomen teneinde ervoor te zorgen dat de verordening wordt nageleefd (zie ook artikel 24)[5]. Met andere woorden: **een**

[1] 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).

[2] In andere contexten wordt vaak de term "privacyeffectbeoordeling" gebruikt om naar hetzelfde concept te verwijzen.

[3] In artikel 27 van Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens is ook gesteld dat een privacyeffectbeoordeling nodig is indien "*de verwerking [...] waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert*".

[4] In de AVG wordt het concept "gegevensbeschermingseffectbeoordeling" niet formeel gedefinieerd, maar

- de minimale inhoud ervan wordt als volgt gespecificeerd in artikel 35, lid 7:
    - "*a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;*
    - *b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;*
    - *c) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en*
    - *d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.*
- de betekenis en rol ervan wordt als volgt verduidelijkt in overweging 84: "*Teneinde de naleving van deze verordening te verbeteren indien de verwerking waarschijnlijk gepaard gaat met hoge risico's in verband met de rechten en vrijheden van natuurlijke personen, dient de verwerkingsverantwoordelijke of de verwerker verantwoordelijk te zijn voor het verrichten van een gegevensbeschermingseffectbeoordeling om met name de oorsprong, de aard, het specifieke karakter en de ernst van dat risico te evalueren.*"

[5] Zie ook overweging 84: "*Met het resultaat van de beoordeling dient rekening te worden gehouden bij het bepalen van de passende maatregelen die moeten worden genomen om aan te tonen dat deze verordening bij de verwerking van persoonsgegevens wordt nageleefd.*"

gegevensbeschermingseffectbeoordeling is een proces voor het verwezenlijken en aantonen van naleving.

Als niet aan de eisen van de gegevensbeschermingseffectbeoordeling wordt voldaan, kan dat krachtens de AVG tot gevolg hebben dat de bevoegde toezichthoudende autoriteit boetes oplegt. Als geen gegevensbeschermingseffectbeoordeling wordt uitgevoerd terwijl dat voor de verwerking wel verplicht is (artikel 35, leden 1, 3 en 4), als een gegevensbeschermingseffectbeoordeling niet correct wordt uitgevoerd (artikel 35, leden 2, 7, 8 en 9), of als de bevoegde toezichthoudende autoriteit niet wordt geraadpleegd terwijl dat wel vereist is (artikel 36, lid 3, onder e)), kan dat leiden tot een administratieve boete van maximaal 10 miljoen EUR of, in het geval van een onderneming, maximaal 2 % van de totale wereldwijde jaaromzet van het voorgaande boekjaar, waarbij het hoogste bedrag van toepassing is.

II. Toepassingsgebied van de richtsnoeren

Bij deze richtsnoeren is rekening gehouden met:

- verklaring 14/EN WP 218 van de Groep gegevensbescherming artikel 29 (WP29)[6];
- de WP29-richtlijnen voor functionarissen voor gegevensbescherming 16/EN WP 243[7];
- het WP29-advies inzake doelbinding 13/EN WP 203[8];
- internationale normen[9].

In overeenstemming met de risicogebaseerde aanpak die in de AVG is vastgelegd, is een gegevensbeschermingseffectbeoordeling niet verplicht voor elke verwerking. Een gegevensbeschermingseffectbeoordeling is alleen verplicht als de verwerking "*waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen*" (artikel 35, lid 1). Met het oog op een consistente interpretatie van de omstandigheden waarin een gegevensbeschermingseffectbeoordeling verplicht is (artikel 35, lid 3), zijn de onderhavige richtsnoeren in de eerste plaats bedoeld om dit begrip te verduidelijken en criteria te geven voor de lijsten die door de gegevensbeschermingsautoriteiten moeten worden opgesteld overeenkomstig artikel 35, lid 4.

Volgens artikel 70, lid 1, onder e), kan het Europees Comité voor gegevensbescherming richtsnoeren, aanbevelingen en beste praktijken uitvaardigen om een consistente toepassing van de AVG te bevorderen. Het doel van dit document is om op dergelijk toekomstig werk van het Europees Comité

---

[6] Statement on the role of a risk-based approach in data protection legal framewworks, vastgesteld op 30 mei 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] WP29-richtlijnen voor functionarissen voor gegevensbescherming 16/NL WP 243, vastgesteld op 13 december 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] WP29-advies 03/2013 inzake doelbinding 13/EN WP 203, vastgesteld op 2 april 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] bv. ISO 31000:2009, *Risicomanagement – Principes en richtlijnen*, Internationale Organisatie voor Standaardisatie (ISO); ISO/IEC 29134 (project), *Informatietechnologie – Beveiligingstechnieken – Privacyeffectbeoordeling – Richtsnoeren*, Internationale Organisatie voor Standaardisatie (ISO).

voor gegevensbescherming te anticiperen en derhalve de relevante bepalingen van de AVG te verduidelijken teneinde verwerkingsverantwoordelijken te helpen om de wet na te leven en teneinde rechtszekerheid te bieden aan verwerkingsverantwoordelijken die een gegevensbeschermingseffectbeoordeling moeten uitvoeren.

Deze richtsnoeren zijn ook bedoeld ter bevordering van de opstelling van:

- een gemeenschappelijke EU-lijst van verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling verplicht is (artikel 35, lid 4);
- een gemeenschappelijke EU-lijst van verwerkingen waarvoor geen gegevensbeschermingseffectbeoordeling vereist is (artikel 35, lid 5);
- gemeenschappelijke criteria betreffende de methode voor het uitvoeren van een gegevensbeschermingseffectbeoordeling (artikel 35, lid 5);
- gemeenschappelijke criteria om te specificeren wanneer de toezichthoudende autoriteit moet worden geraadpleegd (artikel 36, lid 1);
- aanbevelingen, waar mogelijk, op basis van de in EU-lidstaten opgedane ervaring.

III. Gegevensbeschermingseffectbeoordeling: toelichting op de verordening

De AVG vereist dat verwerkingsverantwoordelijken passende maatregelen treffen om de naleving van de AVG te waarborgen en te kunnen aantonen, onder meer rekening houdend met "de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen" (artikel 24, lid 1). De verplichting voor verwerkingsverantwoordelijken om in bepaalde omstandigheden een gegevensbeschermingseffectbeoordeling uit te voeren, moet worden begrepen tegen de achtergrond van hun algemene verplichting om risico's[10] die verbonden zijn aan de verwerking van persoonsgegevens op passende wijze te beheren.

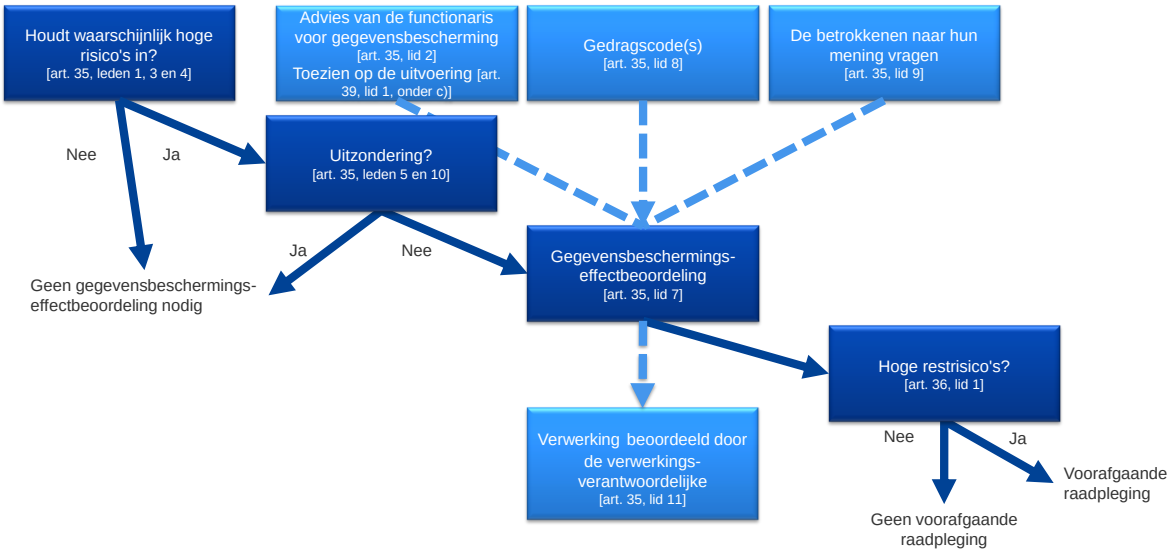
Een "risico" is een scenario dat een gebeurtenis en de gevolgen ervan beschrijft, ingeschat in termen van ernst en waarschijnlijkheid. "Risicobeheer" daarentegen kan worden gedefinieerd als de gecoördineerde activiteiten om een organisatie te sturen en te beheren wat risico's betreft.

In artikel 35 wordt verwezen naar een waarschijnlijk hoog risico "voor de rechten en vrijheden van natuurlijke personen". Zoals aangegeven in de Verklaring van de Groep gegevensbescherming artikel 29 over de rol van een risicogebaseerde benadering in rechtskaders inzake gegevensbescherming, heeft de verwijzing naar "de rechten en vrijheden" van betrokkenen voornamelijk betrekking op de rechten op gegevensbescherming en privacy, maar kan ze ook andere grondrechten betreffen zoals vrijheid van meningsuiting, vrijheid van gedachte, vrijheid van verkeer, discriminatieverbod, recht op vrijheid, en vrijheid van geweten en godsdienst.

In overeenstemming met de risicogebaseerde aanpak die door de AVG wordt belichaamd, is een gegevensbeschermingseffectbeoordeling niet verplicht voor elke verwerking. Een gegevensbeschermingseffectbeoordeling is alleen vereist wanneer een soort verwerking "waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen" (artikel 35, lid 1). Het loutere feit dat niet is voldaan aan de voorwaarden die aanleiding geven tot de verplichting om een gegevensbeschermingseffectbeoordeling uit te voeren, doet echter geen afbreuk aan de algemene verplichting van verwerkingsverantwoordelijken om maatregelen te treffen teneinde de risico's voor de rechten en vrijheden van betrokkenen op passende wijze te beheren. In de praktijk betekent dit dat verwerkingsverantwoordelijken de risico's die door hun verwerkingsactiviteiten ontstaan voortdurend moeten beoordelen om te kunnen vaststellen wanneer een soort verwerking "waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen".

[10] Er moet worden benadrukt dat om de risico's voor de rechten en vrijheden van natuurlijke personen te beheren, de risico's moeten worden geïdentificeerd, geanalyseerd, ingeschat, geëvalueerd, aangepakt (bijvoorbeeld afgezwakt) en regelmatig moeten worden herbeoordeeld. Verwerkingsverantwoordelijken kunnen hun verantwoordelijkheid niet ontlopen door risico's via een verzekeringspolis te verzekeren.

De volgende figuur illustreert de basisprincipes met betrekking tot de gegevensbeschermingseffectbeoordeling in de AVG:



A. <u>Waarop heeft een gegevensbeschermingseffectbeoordeling betrekking? Een enkele verwerking of een reeks vergelijkbare verwerkingen.</u>

Een gegevensbeschermingseffectbeoordeling kan betrekking hebben op een enkele verwerking van gegevens. In artikel 35, lid 1, wordt echter het volgende gesteld: "*Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden*". In overweging 92 wordt het volgende toegevoegd: "*Onder bepaalde omstandigheden kan het redelijk en nuttig zijn dat de gegevensbeschermingseffectbeoordeling zich niet beperkt tot een enkel project, bijvoorbeeld wanneer overheidsinstanties of -organen een gemeenschappelijk applicatie- of verwerkingsplatform willen opzetten of wanneer meerdere verwerkingsverantwoordelijken van plan zijn een gemeenschappelijke applicatie- of verwerkingsomgeving in te voeren voor een hele bedrijfstak, of een segment daarvan, of voor een gangbare horizontale activiteit*".

Een enkele gegevensbeschermingseffectbeoordeling zou kunnen worden gebruikt om meerdere verwerkingen die vergelijkbaar zijn in termen van aard, omvang, context, doel en risico's te beoordelen. Gegevensbeschermingseffectbeoordelingen zijn immers gericht op het systematisch bestuderen van nieuwe situaties die tot hoge risico's voor de rechten en vrijheden van natuurlijke personen zouden kunnen leiden, en het is niet nodig om een gegevensbeschermingseffectbeoordeling uit te voeren in gevallen (d.w.z. verwerkingen die in een specifieke context en voor een specifiek doel worden verricht) die al zijn onderzocht. Dit kan het geval zijn wanneer soortgelijke technologie wordt gebruikt om dezelfde soort gegevens te verzamelen voor dezelfde doeleinden. Bijvoorbeeld een groep gemeentelijke overheden die elk een soortgelijk CCTV-systeem opzetten, zou een enkele gegevensbeschermingseffectbeoordeling kunnen uitvoeren die de verwerking door de verschillende verwerkingsverantwoordelijken bestrijkt, of een spoorwegexploitant (één verwerkingsverantwoordelijke) zou de videobewaking in al zijn treinstations kunnen behandelen in één gegevensbeschermingseffectbeoordeling. Dit kan ook van toepassing zijn op vergelijkbare verwerkingen die door verschillende verwerkingsverantwoordelijken worden uitgevoerd. In die gevallen moet een referentie-gegevensbeschermingseffectbeoordeling worden gedeeld of publiek toegankelijk worden gemaakt, moeten de in de gegevensbeschermingseffectbeoordeling beschreven

maatregelen worden geïmplementeerd, en moet de uitvoering van een enkele gegevensbeschermingseffectbeoordeling worden gemotiveerd.

Wanneer gezamenlijke verwerkingsverantwoordelijken bij de verwerking betrokken zijn, moeten ze hun respectieve verplichtingen precies bepalen. In hun gegevensbeschermingseffectbeoordeling moet worden beschreven welke partij verantwoordelijk is voor de verschillende maatregelen die zijn ontworpen om risico's aan te pakken en de rechten en vrijheden van de betrokkenen te beschermen. Elke verwerkingsverantwoordelijke moet uiteenzetten wat zijn behoeften zijn en moet nuttige informatie delen zonder geheimen prijs te geven (bijvoorbeeld bescherming van handelsgeheimen, intellectueel eigendom, vertrouwelijke bedrijfsinformatie) of kwetsbare punten te onthullen.

Een gegevensbeschermingseffectbeoordeling kan ook nuttig zijn om het gegevensbeschermingseffect van een technologisch product te beoordelen, bijvoorbeeld hardware of software, indien dit waarschijnlijk door verschillende verwerkingsverantwoordelijken zal worden gebruikt om verschillende verwerkingen uit te voeren. Natuurlijk blijft de verwerkingsverantwoordelijke die het product lanceert verplicht om zijn eigen gegevensbeschermingseffectbeoordeling uit te voeren met betrekking tot de specifieke implementatie, al kan hij zich hiervoor baseren op een door de productaanbieder uitgevoerde gegevensbeschermingseffectbeoordeling, in voorkomend geval. Een voorbeeld zou kunnen zijn de relatie tussen fabrikanten van slimme meters en nutsbedrijven. Elke productaanbieder of verwerker moet nuttige informatie delen zonder geheimen prijs te geven en zonder veiligheidsrisico's te creëren door kwetsbare punten te onthullen.

B. Welke verwerkingen zijn aan een gegevensbeschermingseffectbeoordeling onderworpen? Afgezien van uitzonderingen, verwerkingen die "*waarschijnlijk een hoog risico inhouden*".

In dit deel wordt beschreven wanneer een gegevensbeschermingseffectbeoordeling verplicht is en wanneer het niet nodig is om een gegevensbeschermingseffectbeoordeling uit te voeren.

Tenzij de verwerking aan een uitzondering voldoet (III.B.a), moet een gegevensbeschermingseffectbeoordeling worden uitgevoerd als een verwerking "*waarschijnlijk een hoog risico inhoudt*" (III.B.b).

a) Wanneer is een gegevensbeschermingseffectbeoordeling verplicht? Als de verwerking "*waarschijnlijk een hoog risico inhoudt*".

De AVG vereist niet dat een gegevensbeschermingseffectbeoordeling wordt uitgevoerd voor elke verwerking die risico's voor de rechten en vrijheden van natuurlijke personen kan inhouden. Een gegevensbeschermingseffectbeoordeling is alleen verplicht als de verwerking "*waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen*" (artikel 35, lid 1, geïllustreerd door artikel 35, lid 3, en aangevuld door artikel 35, lid 4). Een gegevensbeschermingseffectbeoordeling is bijzonder relevant wanneer een nieuwe technologie voor gegevensverwerking wordt geïntroduceerd[11].

In gevallen waarin het niet duidelijk is of een gegevensbeschermingseffectbeoordeling vereist is, raadt de WP29 aan om deze toch uit te voeren omdat een gegevensbeschermingseffectbeoordeling een

[11] Zie de overwegingen 89, 91 en artikel 35, leden 1 en 3, voor andere voorbeelden.

nuttig instrument is dat verwerkingsverantwoordelijken helpt om aan de wetgeving inzake gegevensbescherming te voldoen.

Hoewel in andere omstandigheden een gegevensbeschermingseffectbeoordeling vereist kan zijn, worden in artikel 35, lid 3, enkele voorbeelden gegeven van wanneer een verwerking "*waarschijnlijk een hoog risico inhoudt*":

- "*(a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen*[12]*;*
- *b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10*[13]*; of*
- *(c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten*".

Zoals de woorden "*met name*" in de inleidende zin van artikel 35, lid 3, AVG aangeven, is dit als een niet-exhaustieve lijst bedoeld. Er kunnen verwerkingen zijn die niet onder deze lijst vallen maar toch vergelijkbaar hoge risico's inhouden. Deze verwerkingen moeten ook aan een gegevensbeschermingseffectbeoordeling worden onderworpen. Om die reden gaan de onderstaande criteria soms verder dan een eenvoudige uitleg over wat moet worden verstaan onder de drie voorbeelden in artikel 35, lid 3, AVG.

Om een concretere reeks verwerkingen te geven die een gegevensbeschermingseffectbeoordeling vereisen op grond van hun inherente hoge risico, rekening houdend met de bijzondere elementen van artikel 35, lid 1, en artikel 35, lid 3, onder a) tot en met c), de lijst die op nationaal niveau moet worden vastgesteld overeenkomstig artikel 35, lid 4, en de overwegingen 71, 75 en 91, en andere verwijzingen in de AVG naar verwerkingen die "*waarschijnlijk een hoog risico inhouden*"[14], moeten de volgende negen criteria in aanmerking worden genomen.

1. Evaluatie of scoretoekenning, met inbegrip van profielbepaling en voorspelling, met name van *"kenmerken betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene"* (overwegingen 71 en 91). Voorbeelden hiervan zijn een financiële instelling die haar klanten screent op basis van een kredietreferentiedatabank, een databank die wordt ingezet in de strijd tegen witwaspraktijken en terrorismefinanciering, of een fraudedatabank, of een biotechnologiebedrijf dat rechtstreeks aan consumenten genetische tests aanbiedt om ziekte-/gezondheidsrisico's te beoordelen en te voorspellen, of een bedrijf dat gedrags- of marketingprofielen opstelt op basis van het gebruik van of de navigatie op zijn website.

---

[12] Zie overweging 71: "*om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken*".

[13] Zie overweging 75: "*wanneer persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, en bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen*".

[14] Zie bijvoorbeeld de overwegingen 75, 76, 92 en 116.

2. Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg: verwerking die gericht is op het nemen van beslissingen met betrekking tot betrokkenen "*waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden*" of die "*de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen*" (artikel 35, lid 3, onder a)). De verwerking kan bijvoorbeeld leiden tot uitsluiting of discriminatie van natuurlijke personen. Verwerking met weinig of geen gevolg voor natuurlijke personen voldoet niet aan dit specifieke criterium. Verdere uitleg over deze begrippen wordt verstrekt in de komende WP29-richtsnoeren inzake profielbepaling.
3. Stelselmatige monitoring: verwerking die wordt gebruikt voor het observeren, monitoren of controleren van betrokkenen, inclusief via netwerken verzamelde gegevens of "*stelselmatige [...] monitoring van openbaar toegankelijke ruimten*" (artikel 35, lid 3, onder c))[15]. Dit type monitoring is een criterium omdat de persoonsgegevens kunnen worden verzameld in omstandigheden waarin de betrokkenen mogelijk niet weten wie hun gegevens verzamelt en hoe die gegevens zullen worden gebruikt. Bovendien kan het voor natuurlijke personen onmogelijk zijn om te voorkomen dat ze aan een dergelijke verwerking in een openbare (of openbaar toegankelijke) ruimte worden onderworpen.
4. Gevoelige gegevens of gegevens van zeer persoonlijke aard: dit omvat speciale categorieën persoonsgegevens zoals omschreven in artikel 9 (bijvoorbeeld informatie over de politieke opvattingen van personen), evenals persoonsgegevens met betrekking tot strafrechtelijke veroordelingen of strafbare feiten zoals omschreven in artikel 10. Een voorbeeld hiervan is een algemeen ziekenhuis dat medische dossiers van patiënten bewaart of een privédetective die gegevens van overtreders bewaart. Naast deze bepalingen van de AVG kunnen sommige gegevenscategorieën worden beschouwd als categorieën die het mogelijke risico voor de rechten en vrijheden van natuurlijke personen verhogen. Deze persoonsgegevens worden als gevoelig (zoals deze term algemeen wordt begrepen) beschouwd omdat ze verband houden met huishoudelijke en privéactiviteiten (zoals elektronische communicatie waarvan de vertrouwelijkheid moet worden beschermd) of omdat ze de uitoefening van een grondrecht beïnvloeden (zoals locatiegegevens waarvan de verzameling de vrijheid van verkeer in vraag stelt) of omdat de schending ervan duidelijk gevolgen heeft voor het dagelijkse leven van de betrokkene (zoals financiële gegevens die kunnen worden gebruikt voor betalingsfraude). In dit opzicht kan het relevant zijn of de gegevens al openbaar zijn gemaakt door de betrokkene of door derden. Het feit dat persoonsgegevens openbaar zijn, kan als een factor worden beschouwd bij de beoordeling of de gegevens naar verwachting verder zullen worden gebruikt voor bepaalde doeleinden. Dit criterium kan ook betrekking hebben op gegevens zoals persoonlijke documenten, e-mails, dagboeken, notities uit e-readers met notitiefuncties, en zeer persoonlijke informatie in "life-logging"-applicaties.

[15] Voor de WP29 kan "*stelselmatig*" een of meer van de volgende betekenissen hebben (zie de WP29-richtlijnen voor functionarissen voor gegevensbescherming 16/EN WP 243):

- plaatsvindend volgens een systeem;
- vooraf geregeld, georganiseerd of methodisch;
- plaatsvindend in het kader van een algemeen plan voor gegevensverzameling;
- uitgevoerd als onderdeel van een strategie.

De WP29 interpreteert "*openbaar toegankelijke ruimte*" als een plaats die openstaat voor elk lid van het publiek, bijvoorbeeld een plein, een winkelcentrum, een straat, een marktplaats, een treinstation of een openbare bibliotheek.

5. Op grote schaal verwerkte gegevens: in de AVG wordt niet gedefinieerd wat grootschalig is, al worden in overweging 91 enkele richtsnoeren gegeven. In ieder geval raadt de WP29 aan om met name de volgende factoren in aanmerking te nemen bij het bepalen of een verwerking op grote schaal wordt uitgevoerd[16]:
    a. het aantal betrokkenen, hetzij als een specifiek aantal hetzij als een deel van de relevante populatie;
    b. het volume van gegevens en/of het bereik van verschillende gegevensitems die worden verwerkt;
    c. de duur, of het permanente karakter, van de gegevensverwerkingsactiviteit;
    d. de geografische omvang van de verwerkingsactiviteit.
6. Matching of samenvoeging van datasets, bijvoorbeeld datasets die voortkomen uit twee of meer gegevensverwerkingen die voor verschillende doeleinden zijn uitgevoerd en/of door verschillende verwerkingsverantwoordelijken zijn uitgevoerd op een wijze die de redelijke verwachtingen van de betrokkene zou overschrijden[17].
7. Gegevens met betrekking tot kwetsbare betrokkenen (overweging 75): de verwerking van dit soort gegevens is een criterium vanwege de toegenomen machtsongelijkheid tussen de betrokkenen en de verwerkingsverantwoordelijke, wat betekent dat de natuurlijke personen mogelijk niet in staat zijn om gemakkelijk in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen. Kwetsbare betrokkenen kunnen kinderen omvatten (kinderen kunnen worden geacht niet in staat te zijn om bewust en bedachtzaam in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens), werknemers, kwetsbaardere segmenten van de bevolking die speciale bescherming behoeven (geesteszieken, asielzoekers, bejaarden, patiënten enz.), en in elk geval waarin een onevenwichtigheid in de relatie tussen de positie van de betrokkene en de verwerkingsverantwoordelijke kan worden vastgesteld.
8. Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen, zoals het combineren van het gebruik van vingerafdrukken en gezichtsherkenning voor een betere fysieke toegangscontrole enz. In de AVG wordt duidelijk gesteld (artikel 35, lid 1, en de overwegingen 89 en 91) dat het gebruik van een nieuwe technologie, gedefinieerd "*conform het bereikte niveau van technologische kennis*" (overweging 91), aanleiding kan geven tot de noodzaak om een gegevensbeschermingseffectbeoordeling uit te voeren. Dit komt omdat het gebruik van dergelijke technologie nieuwe vormen van gegevensverzameling en -gebruik kan inhouden, mogelijk met een hoog risico voor de rechten en vrijheden van natuurlijke personen. De persoonlijke en sociale gevolgen van het gebruik van een nieuwe technologie kunnen immers onbekend zijn. Een gegevensbeschermingseffectbeoordeling zal de verwerkingsverantwoordelijke helpen om dergelijke risico's te begrijpen en aan te pakken. Bijvoorbeeld bepaalde toepassingen van het "internet der dingen" kunnen een aanzienlijk effect hebben op het dagelijkse leven en de privacy van natuurlijke personen; en bijgevolg een gegevensbeschermingseffectbeoordeling vereisen.
9. Wanneer als gevolg van de verwerking zelf *"betrokkenen [...] een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst"* (artikel 22 en overweging 91). Dit omvat verwerkingen die erop gericht zijn de toegang van betrokkenen tot een dienst

[16] Zie de WP29-richtlijnen voor functionarissen voor gegevensbescherming 16/EN WP 243.
[17] Zie de toelichting in het WP29-advies inzake doelbinding 13/EN WP 203, blz. 24.

of de mogelijkheid van betrokkenen om een overeenkomst aan te gaan toe te staan, te wijzigen of te weigeren. Een voorbeeld hiervan is een bank die zijn klanten screent op basis van een databank met kredietreferenties om te beslissen of ze al dan niet een lening aangeboden krijgen.

In de meeste gevallen kan een verwerkingsverantwoordelijke ervan uitgaan dat voor een verwerking die aan twee criteria voldoet een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd. Over het algemeen gaat de WP29 ervan uit dat hoe groter het aantal criteria waaraan een verwerking voldoet, hoe waarschijnlijker het is dat ze een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen, en dus een gegevensbeschermingseffectbeoordeling vereist, ongeacht de maatregelen die de verwerkingsverantwoordelijke voornemens is te nemen.

In sommige gevallen **kan een verwerkingsverantwoordelijke echter oordelen dat een verwerking die aan slechts een van deze criteria voldoet een gegevensbeschermingseffectbeoordeling vereist.**

De volgende voorbeelden illustreren hoe de criteria moeten worden gebruikt om te beoordelen of een bepaalde verwerking een gegevensbeschermingseffectbeoordeling vereist:

Voorbeelden van verwerking	**Mogelijke relevante criteria**	**Gegevensbeschermingseffectbeoordeling waarschijnlijk vereist?**
Een ziekenhuis verwerkt genetische en gezondheidsgegevens van zijn patiënten (ziekenhuisinformatiesysteem).	- Gevoelige gegevens of gegevens van zeer persoonlijke aard. - Gegevens over kwetsbare betrokkenen. - Op grote schaal verwerkte gegevens.	Ja
Het gebruik van een camerasysteem om het rijgedrag op snelwegen te controleren. De verwerkingsverantwoordelijke is van plan een intelligent videoanalysesysteem te gebruiken om auto's eruit te pikken en nummerplaten automatisch te herkennen.	- Stelselmatige monitoring. - Innovatief gebruik of innovatieve toepassing van technologische of organisatorische oplossingen.	
Een bedrijf monitort stelselmatig de activiteiten van zijn werknemers, inclusief hun werkplek, internetactiviteit enz.	- Stelselmatige monitoring. - Gegevens over kwetsbare betrokkenen.	
Het verzamelen van openbare socialemediagegevens met het oog op het genereren van profielen.	- Evaluatie of scoretoekenning. - Op grote schaal verwerkte gegevens. - Matching of samenvoeging van datasets.	

Voorbeelden van verwerking	Mogelijke relevante criteria	Gegevensbeschermingseffectbeoordeling waarschijnlijk vereist?
	- Gevoelige gegevens of gegevens van zeer persoonlijke aard:	
Een instelling die een nationale kredietrating- of fraudedatabank creëert.	- Evaluatie of scoretoekenning. - Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg. - Voorkomt dat de betrokkene een recht uitoefent of een beroep doet op een dienst of overeenkomst. - Gevoelige gegevens of gegevens van zeer persoonlijke aard:	
Opslag, voor archiveringsdoeleinden, van gepseudonimiseerde persoonlijke gevoelige gegevens over kwetsbare betrokkenen van onderzoeksprojecten of klinische proeven	- Gevoelige gegevens. - Gegevens over kwetsbare betrokkenen. - Voorkomt dat betrokkenen een recht uitoefenen of een beroep doen op een dienst of overeenkomst.	
Een verwerking van "persoonsgegevens van patiënten of cliënten door een individuele arts, een andere zorgprofessional of door een advocaat" (overweging 91).	- Gevoelige gegevens of gegevens van zeer persoonlijke aard. - Gegevens over kwetsbare betrokkenen.	Nee
Een online tijdschrift dat een mailinglist gebruikt om zijn abonnees een algemene dagelijkse verzamelmail te sturen.	- Op grote schaal verwerkte gegevens.	
Een internetwinkel die op zijn website advertenties voor oldtimeronderdelen toont en daarbij beperkte profielbepaling toepast op basis van items die op zijn eigen website zijn bekeken of gekocht.	- Evaluatie of scoretoekenning.	

Omgekeerd is het mogelijk dat een verwerkingsverantwoordelijke een verwerking die overeenkomt met de bovenvermelde gevallen toch niet beschouwt als een verwerking die "waarschijnlijk een hoog risico inhoudt". In dergelijke gevallen moet de

verwerkingsverantwoordelijke motiveren en documenteren waarom geen gegevensbeschermingseffectbeoordeling is uitgevoerd en moet hij in die documentatie de meningen van de functionaris voor gegevensbescherming opnemen/registreren.

Daarnaast moeten alle verwerkingsverantwoordelijken overeenkomstig het verantwoordingsbeginsel "*een register (bijhouden) van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden*", inclusief onder meer de verwerkingsdoeleinden, een beschrijving van de gegevenscategorieën en de ontvangers van de gegevens en "*indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1,*" (artikel 30, lid 1) en moeten ze beoordelen of een hoog risico waarschijnlijk is, zelfs als zij uiteindelijk besluiten om geen gegevensbeschermingseffectbeoordeling uit te voeren.

Opmerking: toezichthoudende autoriteiten moeten een lijst van de verwerkingen die een gegevensbeschermingseffectbeoordeling vereisen opstellen, openbaar maken en meedelen aan het Europees Comité voor gegevensbescherming (artikel 35, lid 4)[18]. De hierboven beschreven criteria kunnen toezichthoudende autoriteiten helpen om een dergelijke lijst op te stellen en indien nodig meer specifieke inhoud toe te voegen in een latere fase. Bijvoorbeeld de verwerking van eender welk type biometrische gegevens of gegevens van kinderen zou ook kunnen worden beschouwd als relevant voor de opstelling van een lijst overeenkomstig artikel 35, lid 4.

b) Wanneer is geen gegevensbeschermingseffectbeoordeling vereist? Als het niet zo is dat de verwerking "*waarschijnlijk een hoog risico inhoudt*", of als een vergelijkbare gegevensbeschermingseffectbeoordeling bestaat, of als ze vóór mei 2018 is geautoriseerd, of als ze een rechtsgrond heeft, of als ze in de lijst staat van verwerkingen waarvoor geen gegevensbeschermingseffectbeoordeling is vereist.

WP29 is van mening dat een gegevensbeschermingseffectbeoordeling niet is vereist in de volgende gevallen:

- **als het niet zo is dat de verwerking "*waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen*"** (artikel 35, lid 1);
- **als de aard, de omvang, de context en het doel van de verwerking zeer vergelijkbaar zijn met de verwerking waarvoor een gegevensbeschermingseffectbeoordeling is uitgevoerd**. In dergelijke gevallen kunnen de resultaten van de gegevensbeschermingseffectbeoordeling voor een vergelijkbare verwerking worden gebruikt (artikel 35, lid 1[19]);
- als de verwerkingen vóór mei 2018 door een toezichthoudende autoriteit zijn gecontroleerd in specifieke omstandigheden die niet zijn gewijzigd[20] (zie III.C);
- **als een verwerking,** krachtens artikel 6, lid 1, onder c) of e), **een rechtsgrond heeft** in het Unierecht of het lidstatelijke recht, de specifieke verwerking door de wet wordt geregeld **en er**

[18] In die context geldt het volgende: "*wanneer [dergelijke] lijsten betrekking hebben op verwerkingen met betrekking tot het aanbieden van goederen of diensten aan betrokkenen of op het observeren van hun gedrag in verschillende lidstaten, of op verwerkingen die het vrije verkeer van persoonsgegevens in de Unie wezenlijk kunnen beïnvloeden, past de bevoegde toezichthoudende autoriteit [...] het in artikel 63 bedoelde coherentiemechanisme toe*" (artikel 35, lid 6).

[19] "*Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden"*.

[20] "*Besluiten van de Commissie en door de toezichthoudende autoriteiten verleende toestemmingen die op Richtlijn 95/46/EG zijn gebaseerd, blijven van kracht totdat zij worden gewijzigd, vervangen of ingetrokken*" (overweging 171).

al een gegevensbeschermingseffectbeoordeling is uitgevoerd in het kader van de vaststelling van die rechtsgrond (artikel 35, lid 10)[21], tenzij een lidstaat heeft gesteld dat het noodzakelijk is om voorafgaand aan de verwerkingen een gegevensbeschermingseffectbeoordeling uit te voeren;

- **als de verwerking is opgenomen in de optionele lijst (opgesteld door de toezichthoudende autoriteit) van verwerkingen** waarvoor geen gegevensbeschermingseffectbeoordeling vereist is (artikel 35, lid 5). Een dergelijke lijst kan verwerkingsactiviteiten bevatten die voldoen aan de voorwaarden die deze autoriteit heeft gespecificeerd, met name door middel van richtlijnen, specifieke beslissingen of vergunningen, nalevingsregels enz. (bijvoorbeeld in Frankrijk, vergunningen, vrijstellingen, vereenvoudigde regels, nalevingspakketten ...). In dergelijke gevallen en onder voorbehoud van herbeoordeling door de bevoegde toezichthoudende autoriteit, is geen gegevensbeschermingseffectbeoordeling vereist, maar alleen als de verwerking strikt binnen het toepassingsgebied valt van de desbetreffende procedure die in de lijst is vermeld en volledig aan alle relevante eisen van de AVG blijft voldoen.

C. Wat met reeds bestaande verwerkingen? In bepaalde omstandigheden is een gegevensbeschermingseffectbeoordeling vereist.

De vereiste om een gegevensbeschermingseffectbeoordeling uit te voeren, geldt voor bestaande verwerkingen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen en waarvoor de risico's zijn veranderd, rekening houdend met de aard, de omvang, de context en de doeleinden van de verwerking.

Een gegevensbeschermingseffectbeoordeling is niet nodig voor verwerkingen die door een toezichthoudende autoriteit of de functionaris voor gegevensbescherming zijn gecontroleerd, overeenkomstig artikel 20 van Richtlijn 95/46/EG, en die worden uitgevoerd op een wijze die sinds de recentste controle niet is gewijzigd. Immers: "*Besluiten van de Commissie en door de toezichthoudende autoriteiten verleende toestemmingen die op Richtlijn 95/46/EG zijn gebaseerd, blijven van kracht totdat zij worden gewijzigd, vervangen of ingetrokken*" (overweging 171).

Omgekeerd betekent dit dat elke gegevensverwerking waarvan de uitvoeringsvoorwaarden (omvang, doel, verzamelde persoonsgegevens, identiteit van de verwerkingsverantwoordelijken of ontvangers, bewaartermijn van de gegevens, technische en organisatorische maatregelen enz.) sinds de recentste controle door de toezichthoudende autoriteit of de functionaris voor gegevensbescherming zijn veranderd en die waarschijnlijk een hoog risico inhoudt, aan een gegevensbeschermingseffectbeoordeling moet worden onderworpen.

[21] Als een gegevensbeschermingseffectbeoordeling wordt uitgevoerd tijdens de uitwerking van de wetgeving die een rechtsgrond voor een verwerking biedt, zal die beoordeling waarschijnlijk moeten worden herzien voordat de verwerkingen worden uitgevoerd, aangezien de goedgekeurde wetgeving dusdanig van de voorgestelde wetgeving kan afwijken dat de afwijking gevolgen heeft voor privacy- en gegevensbeschermingskwesties. Bovendien zijn er op het moment dat de wetgeving wordt aangenomen mogelijk niet genoeg technische gegevens beschikbaar met betrekking tot de feitelijke verwerking, zelfs als deze gepaard ging met een gegevensbeschermingseffectbeoordeling. In dergelijke gevallen kan het nog steeds nodig zijn om een specifieke gegevensbeschermingseffectbeoordeling uit te voeren voordat de werkelijke verwerkingen worden uitgevoerd.

Bovendien kan een gegevensbeschermingseffectbeoordeling vereist zijn na een verandering van de risico's die uit de verwerking voortvloeien[22], bijvoorbeeld omdat een nieuwe technologie in gebruik is genomen of omdat persoonsgegevens voor een ander doel worden gebruikt. Gegevensverwerkingen kunnen snel evolueren en er kunnen nieuwe kwetsbare punten ontstaan. Daarom dient te worden opgemerkt dat de herziening van een gegevensbeschermingseffectbeoordeling niet alleen nuttig is voor continue verbetering, maar ook essentieel is om het niveau van gegevensbescherming in een veranderende omgeving op termijn te handhaven. Een gegevensbeschermingseffectbeoordeling kan ook noodzakelijk worden omdat de organisatorische of maatschappelijke context voor de verwerkingsactiviteit is veranderd, bijvoorbeeld omdat de gevolgen van bepaalde geautomatiseerde beslissingen belangrijker zijn geworden of omdat nieuwe categorieën betrokkenen kwetsbaar worden voor discriminatie. Elk van deze voorbeelden kan een element zijn dat leidt tot een verandering van het risico dat uit de betrokken verwerkingsactiviteit voortvloeit.

Omgekeerd kunnen bepaalde veranderingen het risico ook doen afnemen. Bijvoorbeeld een verwerking kan zo evolueren dat beslissingen niet langer worden geautomatiseerd, of een monitoringactiviteit wordt niet langer stelselmatig uitgevoerd. In dat geval kan uit de herziening van de uitgevoerde risicoanalyse blijken dat de uitvoering van een gegevensbeschermingseffectbeoordeling niet meer nodig is.

Het is een goede praktijk om **een gegevensbeschermingseffectbeoordeling continu te herzien en regelmatig opnieuw te beoordelen.** Zelfs als een gegevensbeschermingseffectbeoordeling niet vereist is op 25 mei 2018, is het derhalve nodig dat de verwerkingsverantwoordelijke op het juiste moment een gegevensbeschermingseffectbeoordeling uitvoert als onderdeel van zijn algemene verantwoordingsplicht.

D. Hoe een gegevensbeschermingseffectbeoordeling uitvoeren?

a) Op welk moment moet een gegevensbeschermingseffectbeoordeling worden uitgevoerd? Voorafgaand aan de verwerking.

De gegevensbeschermingseffectbeoordeling moet worden uitgevoerd "*vóór de verwerking*" (artikel 35, leden 1 en 10, en overwegingen 90 en 93)[23]. Dit is in overeenstemming met de beginselen van gegevensbescherming door ontwerp en door standaardinstellingen (artikel 25 en overweging 78). De gegevensbeschermingseffectbeoordeling dient te worden gezien als een hulpmiddel voor de besluitvorming met betrekking tot de verwerking.

De gegevensbeschermingseffectbeoordeling moet zo vroeg mogelijk bij het ontwerpen van de verwerking worden gestart, zelfs als sommige verwerkingen nog niet bekend zijn. Het bijwerken van de gegevensbeschermingseffectbeoordeling gedurende het gehele levenscyclusproject zorgt ervoor dat rekening wordt gehouden met gegevensbescherming en privacy en stimuleert het creëren van oplossingen die de naleving bevorderen. Het kan ook nodig zijn om bepaalde stappen van de

[22] Wat betreft de context, de verzamelde gegevens, doeleinden, functionaliteiten, verwerkte persoonsgegevens, ontvangers, gegevenscombinaties, risico's (ondersteunende activa, risicobronnen, mogelijke effecten, bedreigingen enz.), beveiligingsmaatregelen en internationale doorgiften.

[23] Behalve wanneer het gaat om een reeds bestaande verwerking die vooraf door de toezichthoudende autoriteit is gecontroleerd, in welk geval de gegevensbeschermingseffectbeoordeling moet worden uitgevoerd voordat de verwerking belangrijke veranderingen ondergaat.

beoordeling te herhalen naarmate het ontwikkelingsproces vordert, omdat de selectie van bepaalde technische of organisatorische maatregelen van invloed kan zijn op de ernst of waarschijnlijkheid van de risico's die de verwerking inhoudt.

Het feit dat de gegevensbeschermingseffectbeoordeling mogelijk moet worden bijgewerkt nadat de verwerking daadwerkelijk van start is gegaan, is geen geldige reden om die beoordeling uit te stellen of niet uit te voeren. De gegevensbeschermingseffectbeoordeling is een continu proces, vooral als een verwerking dynamisch is en onderhevig is aan voortdurende verandering. **Het uitvoeren van een gegevensbeschermingseffectbeoordeling is een continu proces, niet een eenmalige oefening**.

b) Wie is verplicht om een gegevensbeschermingseffectbeoordeling uit te voeren? De verwerkingsverantwoordelijke, samen met de functionaris voor gegevensbescherming en de verwerkers.

Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om ervoor te zorgen dat de gegevensbeschermingseffectbeoordeling wordt uitgevoerd (artikel 35, lid 2). De gegevensbeschermingseffectbeoordeling kan door iemand anders, binnen of buiten de organisatie, worden uitgevoerd, maar de verwerkingsverantwoordelijke blijft de eindverantwoordelijke voor die taak.

Als een functionaris voor gegevensbescherming is aangewezen, moet de verwerkingsverantwoordelijke ook diens advies inwinnen (artikel 35, lid 2), en dat advies moet samen met de beslissingen van de verwerkingsverantwoordelijke in de gegevensbeschermingseffectbeoordeling worden gedocumenteerd. De functionaris voor gegevensbescherming dient ook toe te zien op de uitvoering van de gegevensbeschermingseffectbeoordeling (artikel 39, lid 1, onder c)). Nadere richtsnoeren zijn opgenomen in de WP29-richtlijnen voor functionarissen voor gegevensbescherming 16/EN WP 243.

Als de verwerking geheel of gedeeltelijk door een gegevensverwerker wordt uitgevoerd, **moet de verwerker de verwerkingsverantwoordelijke helpen met het uitvoeren van de gegevensbeschermingseffectbeoordeling** en alle noodzakelijke informatie verstrekken (in overeenstemming met artikel 28, lid 3, onder f)).

De verwerkingsverantwoordelijke moet "*de betrokkenen of hun vertegenwoordigers naar hun mening [vragen]*" (artikel 35, lid 9), "*in voorkomend geval*". De WP29 is van oordeel dat:

- deze meningen op velerlei manieren kunnen worden gevraagd, afhankelijk van de context (bv. een generieke studie met betrekking tot het doel en de middelen van de verwerking, een vraag aan de personeelsvertegenwoordigers of gebruikelijke enquêtes die naar toekomstige klanten van de verwerkingsverantwoordelijke worden verzonden), om te verzekeren dat de verwerkingsverantwoordelijke een wettige basis heeft voor het verwerken van persoonsgegevens die bij het informeren naar die meningen betrokken zijn. Al moet worden opgemerkt dat toestemming voor verwerking uiteraard geen manier is om de betrokkenen naar hun mening te vragen;
- als de uiteindelijke beslissing van de verwerkingsverantwoordelijke afwijkt van de meningen van de betrokkenen, moeten zijn reden om al dan niet door te gaan worden gedocumenteerd;
- als de verwerkingsverantwoordelijke besluit dat het niet passend is om de betrokkenen naar hun mening te vragen, bijvoorbeeld omdat hierdoor de vertrouwelijkheid van de bedrijfsplannen van het bedrijf in het gedrang zou komen of omdat dit onevenredig of niet

haalbaar zou zijn, moet hij zijn motivering voor het niet informeren naar de meningen van de betrokkenen documenteren.

Ten slotte is het een goede praktijk om andere specifieke taken en verantwoordelijkheden te omschrijven en te documenteren, afhankelijk van het interne beleid en interne processen en regels, bijvoorbeeld:

- als specifieke bedrijfseenheden voorstellen om een gegevensbeschermingseffectbeoordeling uit te voeren, dienen die eenheden vervolgens input te geven voor de gegevensbeschermingseffectbeoordeling en dienen ze te worden betrokken bij het valideren van de gegevensbeschermingseffectbeoordeling;
- indien passend wordt aanbevolen om het advies te vragen van onafhankelijke deskundigen van verschillende beroepen[24] (advocaten, IT-deskundigen, beveiligingsdeskundigen, sociologen, ethici enz.).
- de taken en verantwoordelijkheden van de verwerkers moeten contractueel worden omschreven; en de gegevensbeschermingseffectbeoordeling moet worden uitgevoerd met de hulp van de verwerker, rekening houdend met de aard van de verwerking en de informatie die de verwerker ter beschikking staat (artikel 28, lid 3, onder f));
- het hoofd informatiebeveiliging (Chief Information Security Officer, CISO), indien aangesteld, alsmede de functionaris voor gegevensbescherming, zouden kunnen voorstellen dat de verwerkingsverantwoordelijke een gegevensbeschermingseffectbeoordeling uitvoert voor een specifieke verwerking, en dienen de belanghebbenden te helpen met de methode, met het evalueren van de kwaliteit van de risicobeoordeling en of het restrisico aanvaardbaar is, en met het ontwikkelen van kennis die specifiek is voor de context van de verwerkingsverantwoordelijke;
- het hoofd informatiebeveiliging (Chief Information Security Officer, CISO), indien aangesteld, en/of de IT-afdeling, moeten de verwerkingsverantwoordelijke bijstaan en zouden kunnen voorstellen om een gegevensbeschermingseffectbeoordeling uit te voeren op een specifieke verwerking, afhankelijk van de veiligheids- of operationele behoeften.

c) Wat is de methode voor het uitvoeren van een gegevensbeschermingseffectbeoordeling ? Verschillende methoden, maar gemeenschappelijke criteria.

[24] *Aanbevelingen voor een kader voor privacyeffectbeoordeling voor de Europese Unie, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

In de AVG zijn de minimale kenmerken van een gegevensbeschermingseffectbeoordeling beschreven (artikel 35, lid 7, en de overwegingen 84 en 90):

- "*een [...] beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden*";
- "*een beoordeling van de noodzaak en de evenredigheid van de verwerkingen*";
- "*een beoordeling van de [...] risico's voor de rechten en vrijheden van betrokkenen*";
- "*de beoogde maatregelen om:*
  - "*de risico's aan te pakken*";
  - "*aan te tonen dat aan deze verordening is voldaan*".

De volgende figuur illustreert het generische iteratieve proces voor het uitvoeren van een gegevensbeschermingseffectbeoordeling[25]:

Bij de beoordeling van het effect van een gegevensverwerking moet rekening worden gehouden met de naleving van een gedragscode (artikel 40) (artikel 35, lid 8). Dit kan nuttig zijn om aan te tonen dat adequate maatregelen zijn gekozen of geïmplementeerd, mits de gedragscode passend is voor de verwerking. Er dient ook rekening te worden gehouden met certificeringen, zegels en merktekens waarmee kan worden aangetoond dat verwerkingsverantwoordelijken en verwerkers bij verwerkingen handelen in overeenstemming met de AVG (artikel 42), evenals met bindende bedrijfsvoorschriften.

[25] Er moet worden onderstreept dat het hier afgebeelde proces iteratief is: in de praktijk is het waarschijnlijk dat elk van de fasen meerdere keren wordt herhaald voordat de gegevensbeschermingseffectbeoordeling kan worden afgerond.

Alle relevante eisen die in de AVG zijn beschreven, bieden een breed, algemeen kader voor het ontwerpen en uitvoeren van een gegevensbeschermingseffectbeoordeling. De praktische implementatie van een gegevensbeschermingseffectbeoordeling zal afhangen van de eisen die in de AVG zijn uiteengezet, die kunnen worden aangevuld met meer gedetailleerde praktische richtsnoeren. De uitvoering van de gegevensbeschermingseffectbeoordeling is dus schaalbaar. Dit betekent dat zelfs een kleine verwerkingsverantwoordelijke een gegevensbeschermingseffectbeoordeling kan ontwerpen en uitvoeren die geschikt is voor zijn verwerkingen.

In overweging 90 van de AVG worden een aantal onderdelen van de gegevensbeschermingseffectbeoordeling geschetst die overlappen met welomschreven onderdelen van risicobeheer (bv. ISO 31000[26]). Wat risicobeheer betreft, is een gegevensbeschermingseffectbeoordeling gericht op het "beheren van risico's" voor de rechten en vrijheden van natuurlijke personen, met behulp van de volgende processen, door:

- bepaling van de context: "*rekening houdend met de aard, omvang, context en doelen van de verwerking en de bronnen van de risico's*";
- beoordeling van de risico's: "*de specifieke waarschijnlijkheid en de ernst van de grote risico's [...] beoordelen*";
- aanpak van de risico's: "*om dat risico te beperken*", "*persoonsgegevens te beschermen*" en "*aan te tonen dat aan deze verordening is voldaan*".

Opmerking: de gegevensbeschermingseffectbeoordeling overeenkomstig de AVG is een instrument om risico's voor de rechten van de betrokkenen te beheren, waarbij dus hun perspectief wordt ingenomen, zoals het geval is in bepaalde domeinen (bv. maatschappelijke veiligheid). Omgekeerd is risicomanagement op andere gebieden (bv. informatiebeveiliging) gericht op de organisatie.

De AVG laat verwerkingsverantwoordelijken vrij om de precieze structuur en vorm van de gegevensbeschermingseffectbeoordeling te bepalen, zodat zij deze beoordeling kunnen doen passen bij bestaande werkmethoden. Er zijn verschillende gevestigde processen in de EU en wereldwijd waarbij rekening wordt gehouden met de in overweging 90 beschreven onderdelen. Ongeacht haar vorm moet een gegevensbeschermingseffectbeoordeling echter een echte risicobeoordeling zijn op basis waarvan verwerkingsverantwoordelijken maatregelen kunnen nemen om de risico's aan te pakken.

Er kunnen verschillende methoden (zie bijlage 1 voor voorbeelden van gegevensbeschermings- en privacyeffectbeoordelingsmethoden) worden gebruikt als hulpmiddel bij de uitvoering van de basiseisen die in de AVG zijn beschreven. Om deze verschillende benaderingen mogelijk te maken en om verwerkingsverantwoordelijken in de mogelijkheid te stellen aan de AVG te voldoen, zijn gemeenschappelijke criteria vastgesteld (zie bijlage 2). Deze criteria verduidelijken de basiseisen van de verordening, maar laten voldoende ruimte voor verschillende uitvoeringsvormen. Deze criteria kunnen worden gebruikt om aan te tonen dat een bepaalde methode voor gegevensbeschermingseffectbeoordelingen voldoet aan de door de AVG vereiste standaarden. **Het is aan de verwerkingsverantwoordelijke om een methode te kiezen, maar de gekozen methode moet voldoen aan de criteria in bijlage 2**.

[26] Risicobeheerprocessen: communicatie en raadpleging, bepaling van de context, beoordeling van risico's, aanpak van risico's, monitoring en herziening (zie begrippen en definities, en inhoudsopgave, in de vooruitblik naar de ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

De WP29 stimuleert de ontwikkeling van sectorspecifieke kaders voor gegevensbeschermingseffectbeoordelingen. De reden hiervoor is dat dergelijke kaders kunnen steunen op specifieke sectorkennis, wat betekent dat de gegevensbeschermingseffectbeoordeling kan worden gericht op de bijzonderheden van een bepaald type verwerking (bijvoorbeeld bepaalde soorten gegevens, bedrijfsactiva, mogelijke effecten, bedreigingen, maatregelen). Dit betekent dat de gegevensbeschermingseffectbeoordeling de problemen kan aanpakken die zich voordoen in een bepaalde economische sector, bij gebruik van specifieke technologieën of bij uitvoering van bepaalde soorten verwerkingen.

Indien nodig *"verricht de verwerkingsverantwoordelijke een toetsing om te beoordelen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd, zulks ten minste wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden"* (artikel 35, lid 11[27]).

d) Is het verplicht om de gegevensbeschermingseffectbeoordeling te publiceren? Nee, maar de publicatie van een samenvatting kan het vertrouwen vergroten, en de volledige gegevensbeschermingseffectbeoordeling moet aan de toezichthoudende autoriteit worden meegedeeld in geval van voorafgaande raadpleging of op verzoek van de gegevensbeschermingsautoriteit.

Het publiceren van een gegevensbeschermingseffectbeoordeling is geen wettelijke verplichting van de AVG; het is de verwerkingsverantwoordelijke die beslist om de beoordeling al dan niet te publiceren. Verwerkingsverantwoordelijken dienen echter te overwegen om ten minste delen te publiceren, zoals een samenvatting of een conclusie van hun gegevensbeschermingseffectbeoordeling.

De publicatie zou tot doel hebben meer vertrouwen te wekken in de verwerkingen van de verwerkingsverantwoordelijke, en om blijk te geven van verantwoording en transparantie. Het is een bijzonder goede praktijk om eengegevensbeschermingseffectbeoordeling te publiceren indien de verwerking gevolgen heeft voor leden van het publiek. Dit kan met name het geval zijn wanneer een overheidsinstantie een gegevensbeschermingseffectbeoordeling uitvoert.

De gepubliceerde gegevensbeschermingseffectbeoordeling hoeft niet de volledige beoordeling te bevatten, vooral wanneer de gegevensbeschermingseffectbeoordeling specifieke informatie over de beveiligingsrisico's voor de verwerkingsverantwoordelijke zou kunnen bevatten of wanneer ze handelsgeheimen of commercieel gevoelige informatie zou kunnen prijsgeven. In deze gevallen zou de gepubliceerde versie kunnen bestaan uit slechts een samenvatting van de belangrijkste bevindingen van de gegevensbeschermingseffectbeoordeling, of zelfs gewoon een verklaring dat een gegevensbeschermingseffectbeoordeling is uitgevoerd.

Als een gegevensbeschermingseffectbeoordeling hoge restrisico's aan het licht brengt, is de verwerkingsverantwoordelijke verplicht om de toezichthoudende autoriteit voorafgaand aan de verwerking te raadplegen (artikel 36, lid 1). In het kader hiervan moet de gegevensbeschermingseffectbeoordeling volledig worden verstrekt (artikel 36, lid 3, onder e)). De

[27] In artikel 35, lid 10, wordt alleen de toepassing van artikel 35, leden 1 tot en met 7, uitdrukkelijk uitgesloten.

toezichthoudende autoriteit kan haar advies geven[28]. Ze mag geen handelsgeheimen prijsgeven of zwakke punten in de beveiliging onthullen, behoudens de beginselen die in elke lidstaat van toepassing zijn op de toegang van het publiek tot officiële documenten.

E. Wanneer dient de toezichthoudende autoriteit te worden geraadpleegd? Als de restrisico's hoog zijn.

Zoals hierboven toegelicht:

- een gegevensbeschermingseffectbeoordeling is vereist wanneer een verwerking "*waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen*" (artikel 35, lid 1, zie III.B.a). Bijvoorbeeld de verwerking van gezondheidsgegevens op grote schaal wordt beschouwd als een verwerking die waarschijnlijk een hoog risico inhoudt, en vereist een gegevensbeschermingseffectbeoordeling;
- dan is het de verantwoordelijkheid van de gegevensverantwoordelijke om de risico's voor de rechten en vrijheden van de betrokkenen te beoordelen en beoogde maatregelen[29] vast te stellen teneinde deze risico's tot een acceptabel niveau te beperken en om aan te tonen dat aan de AVG is voldaan (artikel 35, lid 7, zie III.C.c). Een voorbeeld zou kunnen zijn de opslag van persoonsgegevens op laptops met gebruikmaking van geschikte technische en organisatorische beveiligingsmaatregelen (effectieve versleuteling van volledige schijven, robuust sleutelbeheer, passende toegangscontrole, beveiligde back-ups enz.) naast bestaande beleidsregels (kennisgeving, toestemming, recht van inzage, recht van bezwaar enz.).

Indien in het bovenvermelde laptopvoorbeeld wordt geoordeeld dat de risico's voldoende zijn beperkt door de verwerkingsverantwoordelijke en na lezing van artikel 36, lid 1, en de overwegingen 84 en 94, kan de verwerking plaatsvinden zonder raadpleging van de toezichthoudende autoriteit. Het is in gevallen waarin de vastgestelde risico's niet voldoende door de verwerkingsverantwoordelijke kunnen worden aangepakt (wat betekent dat de restrisico's hoog blijven), dat de verwerkingsverantwoordelijke de toezichthoudende autoriteit moet raadplegen.

Een voorbeeld van een onaanvaardbaar hoog restrisico is een geval waarin de betrokkenen kunnen worden geconfronteerd met aanzienlijke of zelfs onomkeerbare gevolgen die zij mogelijk niet te boven komen (bijvoorbeeld een onrechtmatige toegang tot gegevens die leidt tot een bedreiging voor het leven van de betrokkenen, een ontslag, een financieel gevaar) en/of als het duidelijk lijkt dat het risico zich zal voordoen (bijvoorbeeld door de onmogelijkheid om het aantal mensen die toegang hebben tot de gegevens te beperken vanwege de wijze waarop ze worden gedeeld, gebruikt of gedistribueerd, of wanneer een bekend kwetsbaar punt niet wordt weggewerkt of verholpen).

[28] Schriftelijk advies aan de verwerkingsverantwoordelijke is alleen nodig als de toezichthoudende autoriteit van oordeel is dat de beoogde verwerking niet in overeenstemming is met de regelgeving als bedoeld in artikel 36, lid 2.

[29] Inclusief rekening houden met bestaande richtsnoeren van het Europees Comité voor gegevensbescherming en toezichthoudende autoriteiten en rekening houden met de stand van de techniek en de uitvoeringskosten zoals voorgeschreven in artikel 35, lid 1.

Als de verwerkingsverantwoordelijke niet genoeg maatregelen kan vinden om de risico's tot een acceptabel niveau te beperken (d.w.z. de restrisico's zijn nog steeds hoog), dient de toezichthoudende autoriteit te worden geraadpleegd[30].

Bovendien moet een verwerkingsverantwoordelijke de toezichthoudende autoriteit raadplegen telkens wanneer het lidstatelijke recht verwerkingsverantwoordelijken verplicht om de toezichthoudende autoriteit te raadplegen en/of haar voorafgaande toestemming te verkrijgen in verband met zijn verwerking in het kader van de vervulling van een taak van algemeen belang die door hem wordt uitgevoerd, onder meer wanneer de verwerking verband houdt met sociale bescherming en volksgezondheid (artikel 36, lid 5).

Er dient echter te worden vermeld dat, ongeacht of de raadpleging van de toezichthoudende autoriteit vereist is op basis van het niveau van het restrisico, de verplichting om de gegevensbeschermingseffectbeoordeling te bewaren en te zijner tijd bij te werken blijft bestaan.

IV. Conclusies en aanbevelingen

Gegevensbeschermingseffectbeoordelingen zijn een nuttige manier voor verwerkingsverantwoordelijken om gegevensverwerkingssystemen te implementeren die aan de AVG voldoen en kunnen voor sommige soorten verwerkingen verplicht zijn. Ze zijn schaalbaar en kunnen verschillende vormen aannemen, maar de basisvereisten van een effectieve gegevensbeschermingseffectbeoordeling zijn in de AVG uiteengezet. Gegevensverwerkingsverantwoordelijken dienen de uitvoering van een gegevensbeschermingseffectbeoordeling te zien als een nuttige en positieve activiteit die helpt om aan de wettelijke eisen te voldoen.

In artikel 24, lid 1, wordt de basisverantwoordelijkheid van de verwerkingsverantwoordelijke wat betreft de naleving van de AVG beschreven: "*Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd*".

De gegevensbeschermingseffectbeoordeling is een belangrijk onderdeel van de naleving van de verordening indien een gegevensverwerking die een hoog risico inhoudt wordt gepland of plaatsvindt. Dit betekent dat verwerkingsverantwoordelijken de in dit document uiteengezette criteria moeten gebruiken om te bepalen of al dan niet een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd. In het interne beleid inzake verwerkingsverantwoordelijken zou deze lijst kunnen worden uitgebreid met vereisten die verder gaan dan de wettelijke vereisten van de AVG. Dit zou meer vertrouwen moeten wekken bij de betrokkenen en andere verwerkingsverantwoordelijken.

[30] Opmerking: "*pseudonimisering en versleuteling van persoonsgegevens*" (evenals gegevensminimalisering, toezichtsmechanismen enz.) zijn niet noodzakelijk passende maatregelen. Ze zijn slechts voorbeelden. Welke maatregelen passend zijn, is afhankelijk van de context en de risico's die specifiek aan de verwerkingen verbonden zijn.

Als een verwerking wordt gepland die waarschijnlijk een hoog risico inhoudt, moet de verwerkingsverantwoordelijke:

- een methode voor gegevensbeschermingseffectbeoordelingen kiezen (voorbeelden in bijlage 1) die aan de criteria in bijlage 2 voldoet, of een systematisch proces van gegevensbeschermingseffectbeoordelingen specificeren en implementeren dat:
  - aan de criteria in bijlage 2 voldoet;
  - in bestaande ontwerp-, ontwikkelings-, veranderings-, risico- en operationele-evaluatieprocessen is geïntegreerd in overeenstemming met interne processen, de context en de cultuur;
  - de desbetreffende belanghebbenden betrekt en hun verantwoordelijkheden duidelijk omschrijft (verwerkingsverantwoordelijke, functionaris voor gegevensbescherming, betrokkenen of hun vertegenwoordigers, bedrijf, technische diensten, verwerkers, informatiebeveiligingsfunctionaris enz.);
- het rapport van de gegevensbeschermingseffectbeoordeling aan de bevoegde toezichthoudende autoriteit verstrekken indien dat verplicht is;
- de toezichthoudende autoriteit raadplegen als hij er niet in geslaagd is voldoende maatregelen te bepalen om de hoge risico's te beperken;
- de gegevensbeschermingseffectbeoordeling en de verwerking waarop ze van toepassing is periodiek herzien, ten minste wanneer het aan de verwerking verbonden risico is veranderd;
- de genomen beslissingen documenteren.

Bijlage 1 – Voorbeelden van bestaande EU-kaders voor gegevensbeschermingseffectbeoordelingen

In de AVG wordt niet gespecificeerd welk proces voor gegevensbeschermingseffectbeoordeling moet worden gevolgd, maar wordt in plaats daarvan toegestaan dat verwerkingsverantwoordelijken een kader introduceren dat hun bestaande werkpraktijken aanvult, mits er in dat kader rekening wordt gehouden met de in artikel 35, lid 7, beschreven onderdelen. Een dergelijk kader kan worden aangepast aan de verwerkingsverantwoordelijke of kan een gemeenschappelijk kader zijn voor een bepaalde sector. Eerder gepubliceerde kaders die zijn ontwikkeld door gegevensbeschermingsautoriteiten in de EU en sectorspecifieke EU-kaders omvatten (maar zijn niet beperkt tot):

Voorbeelden van generieke EU-kaders:

- DE: Standard Data Protection Model, V.1.0 – Proefversie, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Voorbeelden van sectorspecifieke EU-kaders:

- Kader voor effectbeoordeling op het gebied van de bescherming van de persoonlijke levenssfeer en persoonsgegevens voor RFID-toepassingen[32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Model voor de privacyeffectbeoordeling van slimme netten en slimme metersystemen[33]

---

[31] Unaniem erkend (bij onthouding van Beieren) door de 92ste Conferentie van de onafhankelijke gegevensbeschermingsautoriteiten van de Duitse bondsstaat en deelstaten in Kühlungsborn op 9-10 november 2016.

[32] Zie ook:

- Aanbeveling van de Commissie van 12 mei 2009 over de tenuitvoerlegging van de beginselen inzake de bescherming van de persoonlijke levenssfeer en persoonsgegevens in door radiofrequentie-identificatie ondersteunde toepassingen.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Advies 9/2011 betreffende het herziene voorstel van de industrie voor een effectbeoordelingskader wat betreft de bescherming van de persoonlijke levenssfeer en persoonsgegevens bij RFID-toepassingen.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[33] Zie ook Advies 07/2013 betreffende het model voor de beoordeling van het effect op de gegevensbescherming van slimme netten en slimme metersystemen ("EBGB-model"), opgesteld door

http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Een internationale norm zal ook richtlijnen geven inzake methoden voor het uitvoeren van een gegevensbeschermingseffectbeoordeling (ISO/IEC 29134[34]).

deskundigengroep 2 van de taskforce voor slimme netten van de Commissie. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

[34] ISO/IEC 29134 (project), *Informatietechnologie – Beveiligingstechnieken – Privacyeffectbeoordeling – Richtsnoeren*, Internationale Organisatie voor Standaardisatie (ISO).

Bijlage 2 – Criteria voor een aanvaardbare gegevensbeschermingseffectbeoordeling

De WP29 stelt de volgende criteria voor die verwerkingsverantwoordelijken kunnen gebruiken om te beoordelen of een gegevensbeschermingseffectbeoordeling, of een methode voor het uitvoeren van een gegevensbeschermingseffectbeoordeling, volledig genoeg is om aan de AVG te voldoen:

- ☐ er wordt een systematische beschrijving van de verwerking verstrekt (artikel 35, lid 7, onder a)):
  - ☐ er wordt rekening gehouden met de aard, omvang, context en doelen van de verwerking (overweging 90);
  - ☐ de persoonsgegevens, de ontvangers en de periode gedurende welke de persoonsgegevens worden bewaard worden geregistreerd;
  - ☐ er wordt een functionele beschrijving van de verwerking verstrekt;
  - ☐ de activa waarop persoonsgegevens steunen (hardware, software, netwerken, mensen, papier of papiertransmissiekanalen) worden geïdentificeerd;
  - ☐ er wordt rekening gehouden met de naleving van de goedgekeurde gedragscodes (artikel 35, lid 8);
- ☐ de noodzaak en evenredigheid worden beoordeeld (artikel 35, lid 7, onder b)):
  - ☐ de beoogde maatregelen om aan de verordening te voldoen worden bepaald (artikel 35, lid 7, onder d), en overweging 90), waarbij rekening wordt gehouden met:
    - ☐ maatregelen die bijdragen aan de evenredigheid en noodzaak van de verwerking op basis van:
      - ☐ een of meer gespecificeerde, expliciete en legitieme doeleinden (artikel 5, lid 1, onder b));
      - ☐ rechtmatigheid van de verwerking (artikel 6);
      - ☐ toereikend, ter zake dienend en beperkt tot wat noodzakelijke gegevens zijn (artikel 5, lid 1, onder c));
      - ☐ beperkte bewaartermijn (artikel 5, lid 1, onder e));
    - ☐ maatregelen die bijdragen aan de rechten van de betrokkenen:
      - ☐ informatie verstrekt aan de betrokkene (artikelen 12, 13 en 14);
      - ☐ recht van inzage en recht op overdraagbaarheid van gegevens (artikelen 15 en 20);
      - ☐ recht op rectificatie en recht op gegevenswissing (artikelen 16, 17 en 19);
      - ☐ recht van bezwaar en recht op beperking van de verwerking (artikelen 18, 19 en 21);
      - ☐ relaties met verwerkers (artikel 28);
      - ☐ waarborgen omtrent internationale doorgifte(n) (hoofdstuk V);
      - ☐ voorafgaande raadpleging (artikel 36).
- ☐ de risico's voor de rechten en vrijheden van betrokkenen worden beheerd (artikel 35, lid 7, onder c)):
  - ☐ er wordt rekening gehouden met de oorsprong, de aard, het specifieke karakter en de ernst van de risico's (zie overweging 84) of, meer specifiek, voor elk risico (onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens) vanuit het perspectief van de betrokkenen:
    - ☐ er wordt rekening gehouden met de bronnen van de risico's (overweging 90);
    - ☐ de mogelijke gevolgen voor de rechten en vrijheden van de betrokkenen worden geïdentificeerd in geval van gebeurtenissen zoals onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens;
    - ☐ bedreigingen die kunnen leiden tot onrechtmatige toegang, ongewenste wijziging en de verdwijning van gegevens worden geïdentificeerd;
    - ☐ de waarschijnlijkheid en ernst worden ingeschat (overweging 90);
  - ☐ de beoogde maatregelen om de risico's aan te pakken worden bepaald (artikel 35, lid 7, onder d), en overweging 90);

- ☐ de belanghebbenden worden betrokken:
  - ☐ het advies van de functionaris voor gegevensbescherming wordt ingewonnen (artikel 35, lid 2);
  - ☐ indien nodig wordt de betrokkenen of hun vertegenwoordigers naar hun mening gevraagd (artikel 35, lid 9).