Aanbeveling nr. 01/2018 van 28 februari 2018

Betreft: Aanbeveling uit eigen beweging met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging (CO-AR-2018-001)

De Commissie voor de bescherming van de persoonlijke levenssfeer (hierna "de Commissie");

Gelet op de wet van 8 december 1992 *tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inzonderheid artikel 30;

Gelet op de 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)* (hierna AVG), inzonderheid artikelen 35 en 36;

Gelet op artikelen 26 en 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 en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad;*

Gelet op het verslag van Willem Debeuckelaere;

Brengt op 28 februari 2018 de volgende aanbeveling uit:

1. Inleiding

1. De Algemene Verordening Gegevensbescherming (AVG) voorziet in een aantal nieuwe verplichtingen voor verwerkingsverantwoordelijken.[1] Één van de nieuwe verplichtingen in de AVG betreft de verplichting tot het uitvoeren – in bepaalde omstandigheden – van een "gegevensbeschermingseffectbeoordeling", kortweg "GEB".

2. Een GEB is een **proces** dat bedoeld is 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** door deze risico's in te schatten en maatregelen te bepalen om ze aan te pakken.[2]

3. De Richtlijn Politie & Justitie (Richtlijn 2016/680) voorziet ook in een verplichting tot het uitvoeren van een GEB in bepaalde omstandigheden.[3] De richtsnoeren vervat in deze aanbeveling, die geënt zijn op de bepalingen van de AVG, gelden *mutatis mutandis* voor de interpretatie van de relevante bepalingen van Richtlijn 2016/680.

4. Het opzet van de huidige aanbeveling is om verdere duiding te bieden wat betreft:

(1) de omstandigheden wanneer een GEB verplicht is (afdeling 3);

(2) de essentiële onderdelen van een GEB (afdeling 5);

(3) de omstandigheden waarin een voorafgaande raadpleging verplicht is (afdeling 6);

(4) de actoren die bij een GEB betrokken dienen te worden (afdeling 7); en

(5) een aantal bijzondere bepalingen (afdeling 8).

5. Een eerder ontwerp van deze aanbeveling werd voorgelegd ter publieke consultatie van 20 december 2016 tot 28 februari 2017.[4] De huidige aanbeveling houdt rekening met de opmerkingen en suggesties die door bedrijven, sectorfederaties en academici werden geformuleerd, alsook met de

---

[1] Waar Richtlijn 95/46/EG verwees naar de "voor de verwerking verantwoordelijke", verwijst de AVG naar de "verwerkingsverantwoordelijke".

[2] Groep Gegevensbescherming Artikel 29, Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679, WP 248 rev.01, 4 oktober 2017, p. 4. (hierna: "Groep 29, Richtsnoeren GEB"). Het begrip "gegevensbeschermingseffectbeoordeling" wordt niet als dusdanig gedefinieerd in de AVG, maar wordt in overweging (84) AVG toegelicht als volgt: "*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.*" Wat het begrip "risico" betreft zie verder; nr. 16.

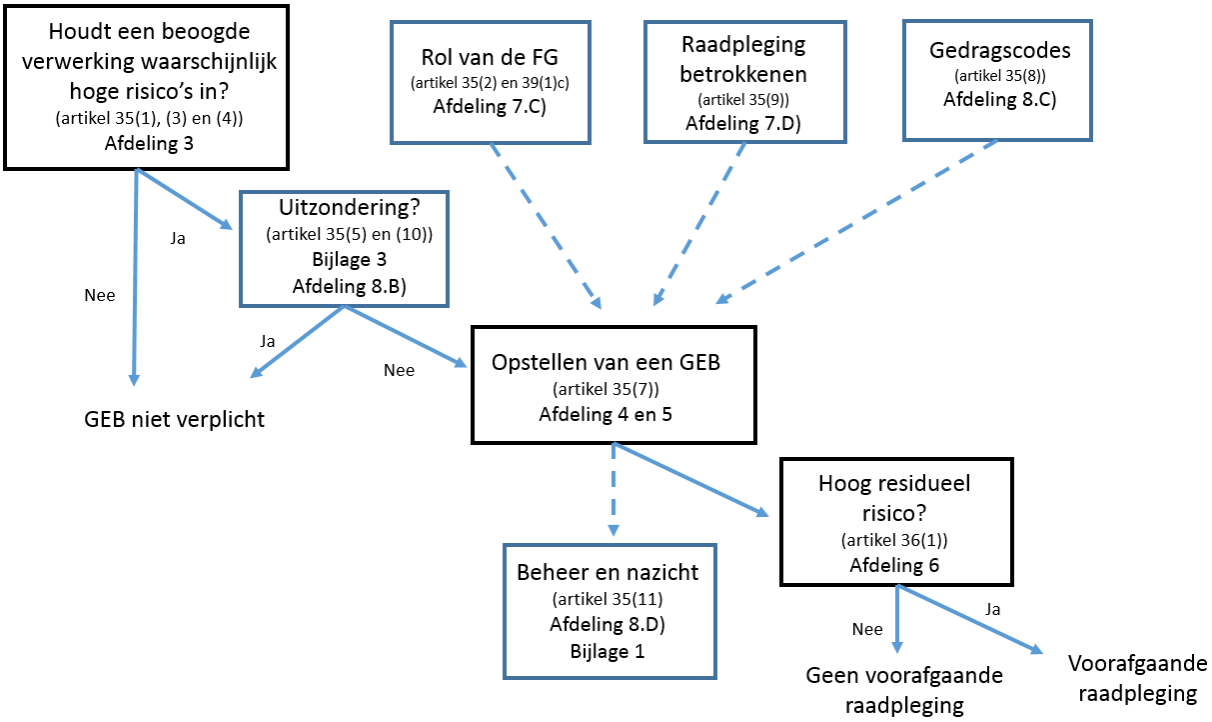
[3] Zie artikelen 27-28 van Richtlijn 2016/680.

[4] https://www.privacycommission.be/nl/publieke-consultatie-over-aanbeveling-gegevensbeschermingseffectbeoordeling

finale versie van de richtsnoeren van de Groep Gegevensbescherming Artikel 29 die in oktober 2017 werden uitgevaardigd.

6. Deze aanbeveling bevat géén vast model of handleiding voor het uitvoeren van een GEB. Hoewel er reeds meerdere modellen en handleidingen voorhanden zijn[5], moedigt de Commissie de sectorfederaties aan om gedragscodes te ontwikkelen die aangepast zijn aan de gegevensverwerkingen binnen hun sector en die in het bijzonder afgestemd zijn op de behoeften van kleine, middelgrote en micro-ondernemingen.[6] Het is echter niet uitgesloten dat de Commissie in de toekomst een formulier en/of aanvullende handleiding ter beschikking stelt dat als uitgangspunt zou kunnen dienen bij het uitvoeren van een GEB of in het kader van een voorafgaande raadpleging.

7. Om de lezer wegwijs te maken in deze aanbeveling en een snelle toegang tot relevante onderdelen te vergemakkelijken, kan het volgende schema nuttig zijn:



[5] Zie Bijlage 1 van Groep 29, Richtsnoeren GEB, p. 26. Zie verder bijv. ook Kruispuntbank voor de Sociale Zekerheid, "AVG Risk Register", raadpleegbaar via https://www.ksz-bcss.fgov.be/sites/default/files/assets/veiligheid_en_privacy/avg_risk_register_nl.xlsm en Rijksoverheid, Model gegevensbeschermingseffectbeoordeling rijksdienst (PIA), September 2017, raadpleegbaar via https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia (hierna: "Rijksoverheid, Model PIA").

[6] Zie ook het themablok "Gedragscodes onder de nieuwe privacywetgeving", https://www.privacycommission.be/nl/gedragscodes-onder-de-nieuwe-privacywetgeving#

2. Waarom een GEB?

8. De verplichting tot het uitvoeren - in bepaalde omstandigheden - van een GEB dient gezien te worden in het licht van twee centrale beginselen van de AVG, met name het beginsel van de verantwoordingsplicht en het beginsel van de risico-gebaseerde aanpak.

9. Het beginsel van de verantwoordingsplicht (zgn. "***accountability***") houdt in dat de verwerkingsverantwoordelijke niet enkel gehouden is om de beginselen en verplichtingen van de AVG na te leven, maar dat hij tevens de naleving ervan moet kunnen aantonen.[7] De GEB vormt een belangrijk instrument in dit verband, aangezien deze kan bijdragen zowel tot de naleving van de beginselen en verplichtingen van de AVG, als het aantonen van de naleving ervan.

10. Het beginsel van de verantwoordingsplicht gaat gepaard met een risico-gebaseerde aanpak (zgn. "***risk-based approach***")[8]. De AVG vereist dat verwerkingsverantwoordelijken passende maatregelen treffen om de naleving van de AVG te waarborgen, onder meer rekening houdend met "*de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen*".[9] De verplichting voor verwerkingsverantwoordelijken om in bepaalde omstandigheden een gegevensbeschermingseffectbeoordeling uit te voeren, moet worden gezien tegen de achtergrond van hun algemene verplichting om de risico's die verbonden zijn aan de verwerking van persoonsgegevens op passende wijze te beheren.[10] Het loutere feit dat niet is voldaan aan de voorwaarden die aanleiding geven tot de verplichting om een GEB uit te voeren, doet dan ook geen afbreuk aan de algemene verplichting van verwerkingsverantwoordelijken om de risico's voor de rechten en vrijheden van betrokkenen op passende wijze te beheren.[11]

11. De risico-gebaseerde aanpak van de AVG heeft als doel om een "**schaalbare en proportionele aanpak**"[12] te bevorderen, zonder daarmee de gegevensbeschermingsbeginselen of de rechten van de betrokkenen op de helling te plaatsen.[13] Dit betekent dat men voor verwerkingen met een hoog risico meer beschermingsmaatregelen zal dienen te nemen dan bij verwerkingen met een laag risico.

---

[7] Artikel 5(2) AVG bepaalt: "*de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht")*".

[8] Zie Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", (vrij vertaald: "Verklaring van de groep 29 van 30 mei 2014 over de rol van een risico-gebaseerde aanpak in juridische kaders voor gegevensbescherming"), WP 218, 30 mei 2014.

[9] Artikel 24(1) AVG.

[10] Groep 29, Richtsnoeren GEB, p. 7.

[11] In de praktijk betekent dit dan ook dat de 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". Groep 29, Richtsnoeren GEB, p. 7.

[12] In het Engels: "*a scalable and proportionate approach to compliance*". (Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", p. 2).

[13] De risico-gebaseerde aanpak ontslaat de verwerkingsverantwoordelijke niet van zijn verplichting om de beginselen en verplichtingen van de AVG na te leven. Zo dienen de beginselen inzake gegevenskwaliteit en de rechten van de betrokkenen steeds te worden eerbiedigd, ongeacht de risico's die een bepaalde verwerking met zich meebrengt. (*Id.*)

12. De verplichting tot het uitvoeren van een GEB is ontwikkeld tegen de achtergrond van Richtlijn 95/46/EG, die voorzag in een algemene verplichting om iedere verwerking van persoonsgegevens aan de toezichthoudende autoriteiten te melden. Die verplichting leidde tot administratieve en financiële lasten, zonder daarmee noodzakelijkerwijze het beschermingsniveau voor persoonsgegevens te verbeteren.[14] Het nieuwe systeem legt daarom het accent op de verplichting van de verwerkingsverantwoordelijke om een voorafgaande GEB uit te voeren voor verwerkingen die "waarschijnlijk een hoog risico" met zich meebrengen en op de maatregelen die kunnen worden genomen om deze risico's te verminderen.

13. Tenslotte kan het uitvoeren van een GEB de verwerkingsverantwoordelijke helpen om de verplichting tot gegevensbescherming door ontwerp (zgn. "***data protection by design***") na te leven. Artikel 25(1) AVG verplicht de verwerkingsverantwoordelijke tot het nemen van passende technische en organisatorische maatregelen, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf. Aangezien een GEB net dient om, voorafgaand aan de verwerking, maatregelen te identificeren om de risico's voor de rechten en vrijheden van natuurlijke personen aan te pakken, kan de GEB hier een belangrijke ondersteunende en/of sturende rol vervullen.

3. Wanneer is het uitvoeren van een GEB verplicht?

14. De AVG vereist niet dat de verwerkingsverantwoordelijke een GEB uitvoert voor iedere verwerking van persoonsgegevens. In regel is het uitvoeren van een GEB slechts verplicht wanneer de gegevensverwerking, gelet op de aard, de omvang, de context en de doeleinden daarvan *waarschijnlijk een hoog risico inhoudt* voor de rechten en vrijheden van natuurlijke personen.[15] Daarnaast lijst artikel 35(3) AVG een aantal gevallen op waarbij het uitvoeren van een GEB steeds verplicht is (waarbij de Europese wetgever dus heeft bepaald dat het om verwerkingen gaat die van nature waarschijnlijk een hoog risico inhouden). Tenslotte voorzien artikel 35(4) en artikel 35(5) AVG dat iedere nationale toezichthoudende autoriteit lijsten opstelt van het soort verwerkingen waarvoor een GEB wel of niet vereist is.

A) Wanneer de verwerking "waarschijnlijk een hoog risico inhoudt" voor de rechten en vrijheden van natuurlijke personen

15. Artikel 35(1) AVG bepaalt dat :

[14] Overweging (89) AVG.

[15] Artikel 35(1) AVG.

"*Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.*"

- *Wat is een "risico" ?*

16. Een "risico" is een scenario dat een gebeurtenis en de gevolgen ervan beschrijft, ingeschat in termen van ernst en waarschijnlijkheid.[16] Anders gezegd, een risico is de **kans** ("waarschijnlijkheid") dat een bepaalde gebeurtenis of bedreiging zich voordoet, met een welbepaalde **impact** ("ernst") tot gevolg.[17] Artikel 35(1) AVG verwijst naar een bijzondere categorie van risico's, m.n. de *risico's voor de rechten en vrijheden van natuurlijke personen*.[18] In het kader van een GEB is een "risico" dan ook een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van natuurlijke personen naar aanleiding van de verwerking van persoonsgegevens.[19] Hoe dit begrip praktisch moet worden ingevuld, zal in Afdeling 5 verder worden toegelicht.[20]

- *Wat is een "hoog risico" ?*

17. Het begrip "hoog risico" wordt door de AVG niet nader omschreven. De Commissie is zich er van bewust dat verschillende organisaties verschillende schalen en methoden hanteren wanneer zij aan risico-inschatting doen. Het is dan ook mogelijk dat deze waarden op een verschillende wijze ingevuld worden, al naar gelang de gebruikte risicoschaal en methode. Het begrip "hoog risico" in de zin van AVG stemt echter niet noodzakelijk overeen met het begrip "hoog risico" zoals men dat terugvindt in andere risico-beheersingsmodellen.

18. De Commissie meent dat het begrip "hoog risico" verwijst naar de gegevensverwerkingen waarvan het **waarschijnlijk** is dat zij **wezenlijke nadelige gevolgen** zullen of kunnen hebben voor de fundamentele rechten en vrijheden van natuurlijke personen. "Waarschijnlijk" betekent niet dat er een kleine kans op een wezenlijk gevolg is. Het wezenlijk gevolg moet zich eerder wel voordoen dan niet. Anderzijds betekent dit ook dat er niet daadwerkelijk gevolgen moeten zijn voor individuen:

---

[16] Groep 29, Richtsnoeren GEB, p. 7.

[17] Zie ook ISO, "Risk management – Vocabulary", ISO Guide 73:2009 ("*un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changement de circonstances) et de sa vraisemblance*") (vrije vertaling : "*een risico wordt vaak uitgedrukt als een combinatie van de gevolgen van een gebeurtenis (inclusief een wijziging van omstandigheden) en de daaraan verbonden waarschijnlijkheid dat de gebeurtenis zich voordoet*").

[18] Aangezien een GEB een instrument is om de risico's voor de rechten van de betrokkenen te beheren, staat het perspectief van de betrokkene centraal. Dit verschilt van risicobeheer op andere gebieden (zoals bv. informatiebeveiliging), die doorgaans gericht zijn op de belangen en doelstellingen van de organisatie zelf. (Zie ook Groep 29, Richtsnoeren GEB, p. 21.)

[19] Rijksoverheid, Model PIA, p. 35.

[20] Zie verder, nr. 45 e.v.

de waarschijnlijkheid van een wezenlijk gevolg volstaat om aan dit criterium te voldoen.[21] Een "wezenlijk nadelig gevolg" betekent dat de betrokkene, in de omstandigheid dat het risico zich zou voordoen, gevoelig geraakt zou worden in de uitoefening of het genot van zijn fundamentele rechten en vrijheden.[22]

- *Wanneer is er waarschijnlijk een hoog risico ?*

19. Om uit te maken of het al dan niet waarschijnlijk is dat een voorgenomen verwerking aanleiding kan geven tot een hoog risico, zijn de richtsnoeren ontwikkeld door de Groep 29 van bijzonder belang.[23] De Groep 29 heeft **negen criteria** geïdentificeerd die verwerkingsverantwoordelijken in overweging dienen te nemen bij hun analyse of een voorgenomen verwerking al dan niet *waarschijnlijk een hoog risico inhoudt* voor de rechten en vrijheden van natuurlijke personen, m.n.:

1. Evaluatie of scoretoekenning, met inbegrip van profilering en voorspelling, met name van kenmerken betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene.[24]
2. Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg: dit criterium omvat verwerkingen die gericht zijn 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.[25]
3. Stelselmatige monitoring: dit criterium omvat verwerkingen die gebruikt worden om betrokkenen te observeren, monitoren of te controleren, met inbegrip van gegevensinzameling via netwerken en de stelselmatige monitoring van openbaar toegankelijke ruimten.[26] Dit 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.

---

[21] Groep Gegevensbescherming Artikel 29, Richtlijnen voor het bepalen van de leidende toezichthoudende autoriteit van de verwerkingsverantwoordelijke of de verwerker", WP 244 rev.01, 5 april 2017, p. 4. Zie ook verder, nr. 45 e.v., voor een aantal specifieke voorbeelden.

[22] Voor de invulling van het begrip "wezenlijke gevolgen" zie ook Groep Gegevensbescherming Artikel 29, Richtlijnen voor het bepalen van de leidende toezichthoudende autoriteit van de verwerkingsverantwoordelijke of de verwerker", WP 244 rev.01, 5 april 2017, p. 4 (toelichting bij de begrippen "wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden" in de zin van artikel 4(23) AVG).

[23] Groep 29, Richtsnoeren GEB, p. 10-13.

[24] Zie ook overwegingen (71), (75) en (91) AVG. Voorbeelden van evaluatie of scoretoekenning 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.

[25] Zie ook artikel 35(3)a AVG. Dit criterium is aanwezig wanneer de verwerking bijvoorbeeld kan leiden tot uitsluiting of discriminatie van natuurlijke personen. Een verwerking met slechts beperkte of geen gevolgen voor natuurlijke personen voldoet niet aan dit specifieke criterium. Verdere uitleg over deze begrippen wordt verstrekt in de richtsnoeren van de Groep 29 inzake profilering.

[26] Zie ook artikel 35(3)c AVG. Wat betreft de interpretatie van het begrip "stelselmatig" zie verder; nr. 24.

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.[27]

4. Gevoelige gegevens of gegevens van zeer persoonlijke aard: dit criterium omvat de bijzondere 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.[28] Daarnaast omvat het ook persoonsgegevens die algemeen als gevoelig worden beschouwd omdat ze verband houden met huishoudelijke en privéactiviteiten (zoals bijv. elektronische communicatie waarvan de vertrouwelijkheid moet worden beschermd) of omdat ze de uitoefening van een grondrecht beïnvloeden (zoals bijv. locatiegegevens waarvan de verzameling de vrijheid van beweging kan beïnvloeden) of omdat de onthulling ervan duidelijk gevolgen heeft voor het dagelijkse leven van de betrokkene (zoals financiële gegevens die kunnen worden gebruikt voor betalingsfraude).[29]

5. Verwerking van persoonsgegevens op grote schaal, rekening houdend met
   - het aantal betrokkenen (hetzij als een specifiek aantal hetzij als een deel van de relevante populatie);
   - het volume van gegevens en/of het bereik van verschillende gegevensitems die worden verwerkt;
   - de duur, of het permanente karakter, van de gegevensverwerkingsactiviteit;
   - de geografische omvang van de verwerkingsactiviteit.[30]

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.[31]

7. Gegevens met betrekking tot kwetsbare betrokkenen, zoals bijvoorbeeld kinderen, werknemers, geesteszieken, asielzoekers, bejaarden, patiënten en andere meer kwetsbare segmenten van de

---

[27] Volgende activiteiten worden bijvoorbeeld als een regelmatige en stelselmatige observatie van betrokkenen beschouwd: een telecommunicatienetwerk beheren; telecommunicatiediensten leveren; retargeting via e-mail; marketingactiviteiten op basis van gegevens; profilering en scores toekennen met het oog op risicobeoordeling (bv. voor toekenning van een kredietwaardigheidsscore, bepaling van verzekeringspremies, fraudepreventie, detectie van witwaspraktijken); locatietracering, bv. via mobiele apps; programma's voor klantenbinding; gedragsgerelateerde publiciteit; monitoring van gezondheids- en conditiegegevens via draagbare apparaten; gesloten tv-circuit; gekoppelde apparaten bv. slimme meters, slimme wagens, domotica enz. (Groep Gegevensbescherming Artikel 29, Richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO), WP 243 rev.01, 5 april 2017, p. 11) (hierna: "Groep 29, Richtlijnen voor functionarissen voor gegevensbescherming").

[28] Zie ook overweging (45) AVG. Een voorbeeld hiervan is een algemeen ziekenhuis dat medische dossiers van patiënten bewaart of een privédetective die gegevens van overtreders bewaart.

[29] 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. Bij de beoordeling van dit criterium 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.

[30] Zie ook overwegingen (75) en (91) AVG. Zie ook Groep 29, Richtlijnen voor functionarissen voor gegevensbescherming, p. 9.

[31] Zie verder ook de toelichting in het WP29-advies inzake doelbinding (WP 203), p. 24.

bevolking die speciale bescherming behoeven.[32] De verwerking van dit soort gegevens is een criterium omdat er veelal een onevenwicht bestaat in de relatie tussen de betrokkene en de verwerkingsverantwoordelijke, wat betekent dat de betrokkene mogelijk niet in staat is om gemakkelijk in te stemmen met of bezwaar te maken tegen de verwerking van hun gegevens, of om hun rechten uit te oefenen.

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. Dit is een criterium omdat het gebruik van dergelijke technologie nieuwe vormen van gegevensverzameling en -gebruik kan inhouden, met mogelijk een hoog risico voor de rechten en vrijheden van natuurlijke personen.[33]

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.[34] Dit omvat verwerkingen die erop gericht zijn de toegang van betrokkenen tot een dienst of de mogelijkheid van betrokkenen om een overeenkomst aan te gaan toe te staan, te wijzigen of te weigeren.[35]

20. 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 Groep 29 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 GEB vereist, ongeacht de maatregelen die de verwerkingsverantwoordelijke voornemens is te nemen om de risico's in te perken.[36] In sommige gevallen kan een verwerkingsverantwoordelijke echter oordelen dat een verwerking die aan slechts één van deze criteria voldoet een gegevensbeschermingseffectbeoordeling vereist.[37]

21. 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

---

[32] Zie ook overweging (75) AVG.

[33] Bovendien wordt in de AVG duidelijk gesteld dat het gebruik van een nieuwe technologie aanleiding kan geven tot de noodzaak om een gegevensbeschermingseffectbeoordeling uit te voeren. Zie artikel 35(1) en de overwegingen (89) en (91) AVG. Of een technologie al dan niet als "nieuw" beschouwd dient te worden dient "conform het bereikte niveau van technologische kennis" ingevuld te worden.

[34] Zie artikel 22 en overweging (91) AVG.

[35] 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.

[36] Voor bijkomende voorbeelden van toepassing van deze criteria zie Groep 29, Richtsnoeren GEB, p. 13-14.

[37] Groep 29, Richtsnoeren GEB, p. 13.

opnemen/registreren.[38] Zelfs indien de verwerkingsverantwoordelijke tot de conclusie komt dat de uitvoering van een GEB niet vereist is, is hij nog steeds onderhevig aan zijn algemene verplichting tot behoorlijk risicobeheer overeenkomstig artikel 24(1) AVG.[39]

B) De verwerkingen vermeld in artikel 35(3) AVG

22. Artikel 35(3) AVG somt **drie situaties** op waarin het uitvoeren van een GEB steeds vereist is:

a) ingeval van 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;

b) ingeval van *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; of

c) ingeval van *stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten*.

In die gevallen zal in de regel steeds een voorafgaande GEB uitgevoerd moeten worden.

23. Artikel 35(3)a AVG verwijst naar "*besluiten*" waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen. Het is belangrijk om op te merken dat niet vereist is dat het gaat om een "volautomatische" besluitvorming in de zin van artikel 22 AVG. Bijgevolg is artikel 35(3)a AVG van toepassing ook wanneer de besluitvorming in kwestie niet uitsluitend op geautomatiseerde verwerking is gebaseerd.[40]

24. De AVG definieert niet wat bedoeld wordt met de begrippen "*systematisch*" of "*stelselmatig*".[41] Volgens de Groep 29 dienen deze begrippen op een of meer van de volgende manieren geïnterpreteerd te worden:

- iets wat zich volgens een systeem voordoet;
- vooraf geregeld, georganiseerd of methodisch;
- iets wat zich voordoet in het kader van een algemeen programma voor gegevensverzameling;

[38] Groep 29, Richtsnoeren GEB, p. 14-15.

[39] Zie hoger; nr. 10.

[40] Article 29 Working Party, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", WP251rev.01, 6 februari 2018, p. 29.

[41] De Commissie merkt op dat in de Engelstalige en Franstalige versie van de AVG zowel in lid (a) als (c) het woord "systematic" resp. "systématique" wordt gebruikt.

- iets wat uitgevoerd wordt in het kader van een strategie.[42]

25. Om te bepalen of de verwerking al dan niet "*grootschalig*" is, dient men volgende factoren in aanmerking te nemen:

- het aantal betrokkenen waarover het gaat (hetzij als een specifiek aantal of als een evenredig deel van de relevante populatie);
- de hoeveelheid gegevens en/of het bereik van de verschillende verwerkte gegevensitems;
- de duur of permanentie van de gegevensverwerking;
- de geografische omvang van de verwerkingsactiviteit.[43]

Overweging (91) AVG preciseert dat de verplichting tot het uitvoeren van een voorafgaande effectbeoordeling niet van toepassing is als het gaat om de verwerking van persoonsgegevens van patiënten of cliënten door een individuele arts, een andere zorgprofessional of door een advocaat. In die gevallen mag de verwerking niet als een grootschalige verwerking worden beschouwd.

26. Een "*openbaar toegankelijke ruimte*" is een plaats die openstaat voor elk lid van het publiek, zoals bijvoorbeeld een plein, een winkelcentrum, een straat, een marktplaats, een treinstation of een openbare bibliotheek.[44]

27. De volgende **voorbeelden** illustreren de soorten verwerking beoogd door artikel 35(3) AVG:

a) Leerlingvolgsystemen en e-learning

Er is sprake van een "systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen" in de zin van artikel 35(3)a AVG wanneer de verwerking ertoe strekt om op georganiseerde wijze meerdere persoonlijke aspecten van leerlingen (zoals bijv. kennis, prestaties, sociale vaardigheden, mentale gezondheidstoestand) te registeren en op geautomatiseerde wijze op te volgen, om op basis daarvan beslissingen te nemen omtrent het verdere vormingstraject van individuele leerlingen.[45]

---

[42] *Ibid*, p. 11. Als voorbeelden van activiteiten die als een regelmatige en stelselmatige observatie van betrokkenen worden beschouwd, verwijst de Groep 29 o.m. het beheer van een telecommunicatienetwerk of het leveren van telecommunicatiediensten; retargeting via e-mail; profilering en scores toekennen met het oog op risicobeoordeling (bv. voor toekenning van een kredietwaardigheidsscore, bepaling van verzekeringspremies, fraudepreventie, detectie van witwaspraktijken).

[43] Groep 29, Richtlijnen voor functionarissen voor gegevensbescherming, p. 9. Als voorbeelden van een grootschalige verwerking verwijst de Groep 29 onder meer naar de verwerking van patiëntgegevens in het kader van de regelmatige bedrijfsvoering van een ziekenhuis; verwerking van persoonsgegevens met het oog op gedragsgerelateerde publiciteit door een zoekmachine, etc. (Ibid, p. 10). Bij zogenaamde "big data" toepassingen zal er ook vaak sprake zijn van een grootschalige verwerking.

[44] Groep Gegevensbescherming Artikel 29, Richtlijnen voor het bepalen van de leidende toezichthoudende autoriteit van de verwerkingsverantwoordelijke of de verwerker", WP 244 rev.01, 5 april 2017, p. 11.

[45] Voor een bespreking van de risico's inzake E-learning zie ook International Working Group on Data Protection in Telecommunications ("Berlin Group"), *Working Paper on E-Learning Platforms*, April 2017, raadpleegbaar via https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2017/25042017_en_2.pdf.

b) Financiële profielen

Er is eveneens sprake van een "systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen" in de zin van artikel 35(3)a AVG wanneer persoonsgegevens uit interne[46] en externe[47] bronnen worden samengebracht om de inkomens- of vermogenspositie, de solvabiliteit, de kredietwaardigheid of het bestedingspatroon van betrokkenen te beoordelen of te voorspellen en wanneer deze informatie in aanmerking genomen wordt bij dienstverlening aan de betrokkene of bij de beslissing om een dienstverlening te weigeren of stop te zetten.

c) Ziekenhuisinformatiesystemen en genetisch onderzoek

Er is sprake van een "grootschalige verwerking van bijzondere categorieën van persoonsgegevens" in de zin van artikel 35(3)b AVG wanneer een ziekenhuis de gezondheidsgegevens van zijn patiënten verwerkt, of wanneer een groot aantal zorgprofessionals zulke gegevens via een gemeenschappelijk platform uitwisselt.[48] Hetzelfde geldt wanneer de genetische gegevens van een groot aantal betrokkenen verder worden verwerkt voor wetenschappelijke doeleinden.[49]

d) Cameratoezicht

Er is sprake van een "stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten" in de zin van artikel 35(3)c AVG wanneer een spoorwegexploitant videobewaking invoert in al zijn treinstations[50] of wanneer er geregeld gebruik gemaakt wordt van flexibel cameratoezicht door (bijvoorbeeld) hulpdiensten (bijv. camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams).

C) <u>De lijsten van de toezichthoudende autoriteit</u>

28. Artikel 35(4) AVG verplicht iedere toezichthoudende autoriteit om een lijst op te stellen van het soort verwerkingen waarvoor een GEB verplicht is en om vervolgens deze lijst mee te delen aan het Europees Comité voor gegevensbescherming (ECGB). Een ontwerplijst van het soort verwerkingen waarvoor een GEB verplicht is vindt men terug in bijlage 2.

29. Artikel 35(5) AVG laat daarnaast ook toe om een lijst op te stellen van het soort verwerkingen waarvoor een GEB niet vereist is. Het opstellen van dergelijke lijst is niet verplicht, maar indien zij wordt opgesteld, moet zij voorgelegd worden aan het ECGB. Een ontwerplijst van het soort verwerkingen die vrijgesteld zijn van de verplichting tot het uitvoeren van een GEB vindt men terug in bijlage 3.

---

[46] Bijv. productbezit, transactionele historiek, CRM gegevens, klik- of surf-gedrag, locatiegegevens, enz.

[47] Bijv. familieleden, externe zwarte lijsten, aangekochte gegevens, enz.

[48] Zie ook Groep 29, Richtsnoeren GEB, p. 13 en Groep 29, Richtlijnen voor functionarissen voor gegevensbescherming, p. 10.

[49] In dit verband herinnert er aan dat één GEB een reeks vergelijkbare verwerkingen kan bestrijken wanneer die vergelijkbare hoge risico's inhouden (artikel 35(1) AVG). Zie ook hoger; nr. 92.

[50] Groep 29, Richtsnoeren GEB, p. 8.

30. De Commissie benadrukt dat voormelde lijsten **geen enkele afbreuk** doen aan de **algemene verplichting tot behoorlijk risicobeheer** van verwerkingsverantwoordelijke overeenkomstig artikel 24(1) AVG.[51] Deze algemene verplichting tot risicobeoordeling en risicobeheersing geldt onverminderd het bestaan van een lijst van bijzondere verwerkingen waarvoor het uitvoeren van een GEB verplicht is (of het bestaan van een lijst van verwerkingen waarvoor het uitvoeren GEB niet verplicht is).[52] Bovendien zijn de lijsten geenszins exhaustief: het uitvoeren van een GEB is steeds vereist van zodra de toepassingsvoorwaarden bepaald bij artikel 35(1) AVG voldaan zijn.

31. De ontwerp lijsten die in bijlagen 2 en 3 zijn opgenomen dienen dan ook vooral gezien te worden als aanknopingspunten, die bijkomende houvast bieden wanneer de verwerkingsverantwoordelijke zoekt na te gaan of de uitvoering van een GEB verplicht is.

4. Op welk moment moet een GEB uitgevoerd worden?

32. Wanneer de uitvoering van een GEB verplicht is, moet deze uitgevoerd worden **vóór de verwerking**.[53] Dit is in overeenstemming met het beginsel van gegevensbescherming door ontwerp, dat vereist dat de verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen dient te nemen, rekening houden met de risico's voor de rechten en vrijheden van natuurlijke personen.[54] De GEB dient te worden gezien als een hulpmiddel voor de besluitvorming met betrekking tot de verwerking.

33. Een GEB moet zo vroeg mogelijk bij het ontwerpen van de verwerking worden gestart (liefst van bij de "ideefase" van een nieuwe verwerking), zelfs als sommige verwerkingen nog niet bekend zijn. Het bijwerken van de GEB gedurende het gehele levenscyclusproject zorgt ervoor dat rekening wordt gehouden met gegevensbescherming en privacy en stimuleert het creëren van oplossingen die naleving van de AVG in het algemeen bevorderen[55], en in het bijzonder de verplichting tot gegevensbescherming door ontwerp.

34. Het kan ook nodig zijn om bepaalde stappen van de 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 (bijv. een uitbesteding van een deel van de verwerkingsactiviteit naartoe een verwerker).

---

[51] Zie hoger; nr. 10.

[52] Zie ook Groep 29, Richtsnoeren GEB, p. 7.

[53] Artikel 35(1), 35(10) en overwegingen (90) en (93) AVG.

[54] Artikel 25(1) en overweging (78) AVG.

[55] Groep 29, Richtsnoeren GEB, p. 17.

Het feit dat een GEB 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. Het uitvoeren van een GEB is een **continu proces**, niet een eenmalige oefening.[56] Dit zal des te belangrijker zijn wanneer een verwerkingsactiviteit of -omgeving dynamisch is en onderhevig is aan voortdurende verandering.

5. Wat zijn de essentiële elementen van een GEB?

A) Overzicht

35. Artikel 35(7) AVG bepaalt dat een GEB minstens de volgende elementen moet bevatten:

> "*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*."

B) Beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden

36. Artikel 35(7) AVG vereist in eerste instantie dat de GEB een *systematische beschrijving* van de beoogde verwerkingen en verwerkingsdoeleinden omvat. Het is belangrijk dat er hierbij rekening gehouden wordt met de aard, omvang, context en doelen van de verwerking en de bronnen van de risico's.[57] De beschrijving dient **minstens de volgende elementen** te omvatten:

- een duidelijke functionele beschrijving van de verwerking, inclusief eventuele systeemvereisten en bedrijfsprocessen;

[56] Groep 29, Richtsnoeren GEB, p. 17-18.

[57] Zie ook overweging (90) AVG.

- de persoonsgegevens, de ontvangers en de periode gedurende welke de persoonsgegevens worden geregistreerd;
- de activa waarop persoonsgegevens steunen (bijv. hardware, software, netwerken, mensen, papier of papiertransmissiekanalen).[58]

Andere elementen die relevant zijn om de aard, omvang en context van de verwerkingen te bepalen zijn onder meer: de categorieën van betrokkenen, de schaal van de gegevensverwerking, de oorsprong van de gegevens, de verhouding tussen verwerkingsverantwoordelijke en betrokkenen, de mogelijke gevolgen voor betrokkenen, en hoe gemakkelijk het is om betrokkenen te identificeren.

37. De verwerkingsverantwoordelijke dient erover te waken dat de beoogde verwerkingen en verwerkingsdoeleinden met de nodige precisie worden omschreven. Een verwijzing naar algemene, ruim omschreven doeleinden (zoals bijv. "het verbeteren van de gebruikservaring", "IT beveiliging", "onderzoek") is niet voldoende.[59] Hetzelfde geldt *mutatis mutandis* t.a.v. beoogde verwerkingen. De beschrijving dient de lezer een duidelijk zicht te geven op welke gegevensverwerkingen door de verwerkingsverantwoordelijke worden beoogd. De Commissie raadt ook aan om op een voldoende gedetailleerde en duidelijke wijze de verwerkingsmiddelen te omschrijven. Een visualisatie van de voorgenomen verwerkingen kan helpen om een systematische aanpak te bevorderen.[60] Tot slot is het ook belangrijk dat de verwerkingsverantwoordelijke duidelijk omschrijft welke de gerechtvaardigde belangen van de verwerkingsverantwoordelijke (of van eventuele derden) zijn, in het bijzonder indien de verwerking op artikel 6(1)f AVG is gebaseerd.[61]

C) Proportionaliteitstoets

38. Een GEB moet een beoordeling van de **noodzaak en de evenredigheid** van de verwerkingen met betrekking tot de doeleinden bevatten. De verwerkingsverantwoordelijke moet dan ook uitdrukkelijk verantwoorden (1) waarom de verwerking van persoonsgegevens noodzakelijk is en (2) waarom ieder van de beoogde verwerkingen noodzakelijk is om de beoogde doeleinde(n) te bereiken.

---

[58] Groep 29, Richtsnoeren GEB, p. 28.

[59] Zie ook Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", 2 april 2013, p. 15-16. De omschrijving van de verwerkingsdoeleinden en de verwerkingsactiviteiten moet steeds voldoende gedetailleerd moet zijn om een behoorlijke appreciatie van de risico's mogelijk te maken, in functie van de aard, omvang, context en doeleinden van de verwerking.Bij de beschrijving van de doeleinden van de beoogde verwerkingen kan de lijst van doeleinden vermeld in de toelichting bij de voorafgaande aangifte, ontwikkeld tegen de achtergrond van artikel 17 van de Wet verwerking Persoonsgegevens, van nut zijn. Zie Commissie voor Bescherming van de Persoonlijke Levenssfeer, "Toelichting – Gewone Aangifte", 2007, raadpleegbaar via https://www.privacycommission.be/sites/privacycommission/files/documents/toelichting_gewone_aangifte_0.pdf. Zie ook Commissie voor de Bescherming van de Persoonlijke Levenssfeer, Aanbeveling 06/2017 van 14 juni 2017 betreffende het Register van verwerkingsactiviteiten (artikel 30 van de AVG), p. 11 e.v.

[60] Een nauwkeurige en systematische beschrijving van de beoogde verwerkingen is niet alleen een voordeel voor de lezer, het is ook een essentiële voorwaarde voor de behoorlijke uitvoering van een GEB. Alleen mits een nauwkeurige beschrijving kan men bepalen welke maatregelen aangewezen zijn om de risico's te beperken.

[61] Zie bijv. ook ISO/IEC 29134, "Information technology – Security Techniques – Guidelines for privacy impact assessment, 2017, p. 10-11 en 13-14; Rijksoverheid, Model PIA, p. 15 en CNIL, Privacy Impact Assessment (PIA) Tools (templates and knowledge bases), 2015, p. 4-6. De aanduiding van de gerechtvaardigde belangen kan desgevallend ook in het kader van de proportionaliteitstoets plaatsvinden. Zie verder, nr. 40.

Indien verschillende verwerkingen of verwerkingsmiddelen aangewend zouden kunnen worden om de beoogde doeleinde(n) te bereiken, dan moet de verwerkingsverantwoordelijke in beginsel kiezen voor die verwerkingsmiddelen die het minst ingrijpend zijn.[62] De verwerkingsverantwoordelijke doet er in voorkomend geval goed aan te documenteren waarom de gekozen verwerkingsmiddelen minder ingrijpend zijn dan de alternatieven.

39. Bij de beoordeling van de evenredigheid dient de verwerkingsverantwoordelijke ook de **doeltreffendheid** van de voorgenomen verwerking te onderzoeken (is het redelijkerwijze te verwachten dat de voorgenomen verwerking haar (legitieme) doeleinde zal bereiken?).[63] Tot slot dient de verwerkingsverantwoordelijke er ook over te waken dat een **passend evenwicht** tussen de relevante belangen behouden blijft.[64]

40. Bijgevolg dienen bij de beoordeling van de noodzaak en de evenredigheid van de beoogde verwerking dienen **minstens de volgende elementen** in rekening te worden gebracht:

- de gespecificeerde, expliciete en legitieme doeleinde(n) van de beoogde verwerking;
- de rechtsgrond waarop de gegevensverwerking wordt gebaseerd (artikel 6) AVG[65];
- een verantwoording waarom de verwerkte persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is zijn (artikel 5(1)c AVG);
- een verantwoording van de beoogde bewaartermijn van de persoonsgegevens, die slechts mogen worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren niet langerdan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is (artikel 5(1)e AVG)[66];
- een verantwoording waarom de belangen van de betrokkene niet zwaarder doorwegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van eventuele derden.

41. Tot slot is het ook aangewezen dat de verwerkingsverantwoordelijke een overzicht biedt van alle maatregelen die worden genomen om aan de verplichtingen van de AVG te voldoen.[67] Dit zal de

---

[62] Zie ook Rijksoverheid, Model PIA, p. 16.

[63] Zie ook artikel 5(1)c AVG (persoonsgegevens moeten "*toereikend* zijn, *ter zake dienend* en *beperkt tot wat noodzakelijk is* voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking")".

[64] De beoordeling van het belangenevenwicht in dit stadium van de GEB zal in de regel slechts voorlopig zijn, aangezien zij nog geen rekening houdt met de beoogde beschermingsmaatregelen (zie verder; nrs. 56 e.v.). Zie verder ook Groep 29, Richtsnoeren GEB, p. 28.

[65] In principe kan een verwerkingsactiviteit die slechts één doeleinde nastreeft slechts aan de hand van één van de rechtsgronden vervat artikel 6 AVG gerechtvaardigd worden. Het is evenwel mogelijk dat eenzelfde verwerking meerdere doeleinden nastreeft. In dat geval is het mogelijk dat er meer dan één rechtsgrond in aanmerking komt om de beoogde gegevensverwerking te rechtvaardigen. Zie Groep Gegevensbescherming Artikel 29, Guidelines for consent under 2016/679, WP 259, 28 november 2017, p. 22.

[66] Groep 29, Richtsnoeren GEB, p. 28.

[67] Het is niet vereist dat deze maatregelen in dit stadium van de AVG worden omschreven, de verwerkingsverantwoordelijke kan er ook voor kiezen om dit in een eerder stadium (bijv. bij de beschrijving van de beoogde gegevensverwerking) of in een afzonderlijk document op te nemen.

verwerkingsverantwoordelijke in eerste instantie toelaten om aan te tonen dat aan de AVG is voldaan.[68] Daarnaast zullen deze maatregelen allicht ook een invloed uitoefenen op de latere risicobeoordeling.[69] Zo verwacht de Commissie dat een GEB ook een overzicht biedt van:

- de maatregelen die bijdragen aan de rechten van de betrokkenen, waaronder
    - o informatie verstrekt aan de betrokkene (artikelen 12, 13 en 14 AVG);
    - o het recht van inzage en het recht op overdraagbaarheid van gegevens (artikelen 15 en 20 AVG);
    - o het recht op rectificatie en het recht op gegevenswissing (artikelen 16, 17 en 19 AVG);
    - o het recht van bezwaar en het recht op beperking van de verwerking (artikelen 18, 19 en 21 AVG);
- hoe de relaties met verwerkers worden geregeld (artikel 28 AVG);
- welke waarborgen omtrent internationale doorgifte(n) desgevallend zullen worden voorzien (hoofdstuk V AVG).[70]

D) Risicobeoordeling

- *Wat is een "risicobeoordeling" ?*

42. Het begrip "risicobeoordeling" verwijst naar het geheel van procedures om risico's te (1) identificeren, (2) analyseren en (3) beoordelen.[71] **Identificatie** van risico's verwijst naar het proces dat ertoe strekt om risico's te onderzoeken, erkennen en beschrijven.[72] De **analyse** van het risico verwijst naar het proces dat er toe strekt om de aard van een risico na te gaan en om het risiconiveau te bepalen.[73] De **evaluatie** van het risico bestaat in een vergelijking van het resultaat van de risico analyse met vooraf bepaalde risico-criteria om te bepalen of het risico (en/of de grootte daarvan) al dan niet aanvaardbaar of draaglijk is.[74]

---

[68] Artikel 37(7)d AVG.

[69] Zie verder, nr. 42.

[70] Groep 29, Richtsnoeren GEB, p. 28.

[71] ISO, "Risk management – Vocabulary", ISO Guide 73:2009 (vrije vertaling van: "*ensemble du processus d'identification des risques, d'analyse du risque et d'évaluation du risque*"). De verwerkingsverantwoordelijke dient bij de identificatie van risico's de nodige voorzichtigheid aan de dag te leggen en op mogelijke risico's te anticiperen, ook wanneer de aard van het risico niet op voorhand gekend is. De inschatting van het risiconiveau vindt immers pas plaats bij de latere analyse van de geïdentificeerde risico's.

[72] *Id.* (vrije vertaling van : "*processus de recherche, de reconnaissance et de description des risques*"). Identificatie van risico's omvat de identificatie van de oorsprong van risico's, gebeurtenissen, hun oorzaken en mogelijke gevolgen (*Id.*)

[73] *Id.* (vrije vertaling van: "*processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque*"). (*Id.*)

[74] *Id.* (vrije vertaling van: "*processus de comparaison des résultats de l'analyse du risque avec les critères de risque afin de déterminer si le risque et/ou son importance sont acceptables ou tolérables*")

43. Bij risicobeheer kan er doorgaans een onderscheid gemaakt worden tussen het "inherente" risico en het "residuele" risico. Het "**inherente**" risico verwijst naar de waarschijnlijkheid dat een negatieve impact zich zal voordoen wanneer er geen beschermingsmaatregelen genomen worden.[75] Het "**residuele**" risico verwijst daarentegen naar de waarschijnlijkheid dat een negatieve impact zich zal voordoen, ondanks de maatregelen die genomen worden om het (inherent) risico te beïnvloeden (beperken).[76]

44. De verwerkingsverantwoordelijke die een GEB uitvoert zal, op het ogenblik van de uitvoering ervan, reeds verschillende maatregelen genomen hebben om aan de verplichtingen van de AVG te voldoen. Deze **bestaande maatregelen** kunnen een invloed uitoefenen op de inschatting van de risico's voor de rechten en vrijheden van natuurlijke personen. Het is dan ook belangrijk dat deze worden gedocumenteerd, zodat zij mede in aanmerking genomen kunnen worden bij de inschatting en de bepaling van de uiteindelijke residuele risico's.[77]

- *Om welke risico's gaat het?*

45. Artikel 35(1) AVG verwijst niet enkel naar het recht op privacy of het recht op gegevensbescherming, maar naar risico's voor de rechten en vrijheden van natuurlijke personen in het algemeen.[78] Relevante risico's kunnen desgevallend ook betrekking hebben op andere fundamentele rechten en vrijheden, zoals bijv. de vrijheid van meningsuiting, vrijheid van gedachte, geweten en godsdienst, het verbod op discriminatie en het recht op vrijheid van beweging.[79]

46. De verwerking van persoonsgegevens kan verschillende risico's inhouden voor de rechten en vrijheden van natuurlijke personen. Overweging (75) van de AVG geeft aantal (niet-limitatieve) **voorbeelden** van negatieve gevolgen voor de rechten en vrijheden van natuurlijke personen die zich kunnen voordoen naar aanleiding van een verwerking van persoonsgegevens, namelijk:

- discriminatie;
- identiteitsdiefstal of –fraude;
- financiële verliezen;

---

[75] Bij de analyse (inschatting) van het risico wordt rekening gehouden met de aanwezigheid (of afwezigheid) en doeltreffendheid van reeds bestaande technische en organisatorische maatregelen die het risico beperken. IEC/ISO, "Risk management – Risk management techniques", IEC/ISO 31010, v1.0, 2009-11, p. 12. Zie ook de figuur op Groep 29, Richtsnoeren GEB, p. 20.

[76] Zie ook ISO, "Risk management – Vocabulary", ISO Guide 73:2009, die "risque résiduel" omschrijft als "*risque subsistant après le traitement du risque*") (vrije vertaling : "*risico dat overblijft na de behandeling van het risico*"). Het is belangrijk om op te merken dat het volledig uitsluiten van risico's in principe niet mogelijk is. Er zal altijd een residueel risico overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom hij dit aanvaardbaar acht. (Rijksoverheid, Model PIA, p. 37.) Zie ook verder; nr. 59.

[77] Zie ook hoger, nr. 41. De verwerkingsverantwoordelijke kiest in regel vrij waar in de GEB deze maatregelen worden gedocumenteerd.

[78] Zie ook overwegingen (74) tot en met (77) AVG.

[79] Groep 29, Richtsnoeren GEB, p. 7.

- reputatieschade;
- verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens;
- ongeoorloofde ongedaanmaking van pseudonimisering;
- de omstandigheid dat betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen; en
- enig ander aanzienlijk economisch of maatschappelijk nadeel.[80]

Bijkomende **voorbeelden** van mogelijke nadelige gevolgen voor de rechten en vrijheden van betrokkenen zijn onder meer:

- verlies van een kans;
- aantasting van gemoedsrust of welzijn;
- stigmatisering of stereotypering;
- het ontzeggen of beperken van toegang tot ruimten of evenementen die anders toegankelijk voor het publiek zijn;
- oneerlijke behandeling (bijv. differentiële prijsstelling);
- manipulatie (bijv. het uitbuiten van emoties);
- gedragsaanpassing (bijv. zelfcensuur); en
- aantasting van de fysieke of morele integriteit.[81]

- *Nood aan een contextuele analyse*

47. Niet iedere verwerking van persoonsgegevens geeft aanleiding tot dezelfde risico's. Bovendien kan de ernst en/of waarschijnlijkheid van een risico sterk variëren naargelang iedere verwerking. De risicobeoordeling dient steeds plaats te vinden in functie van het geheel van bijzondere omstandigheden van elke verwerking (of groep van vergelijkbare verwerkingen[82]). Zo bepaalt overweging (76) AVG dat

> "*De waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkene moeten worden bepaald <u>onder verwijzing naar</u> de aard, het toepassingsgebied, de context en de doeleinden van de verwerking*."

Het is dus in functie van het geheel van bijzondere omstandigheden van elke verwerking dat de verwerkingsverantwoordelijke de risico's voor de rechten en vrijheden van personen moet inschatten

[80] Overweging (75) AVG wijst daarnaast ook op een aantal elementen die risico verhogend kunnen werken. Deze elementen kwamen eerder al aan bod onder afdeling 3, aangezien zij werden verwerking in de 9 criteria van de Groep 29. Zie hoger; nr. 19.

[81] Zie ook Groep Gegevensbescherming Artikel 29, Richtlijnen voor het bepalen van de leidende toezichthoudende autoriteit van de verwerkingsverantwoordelijke of de verwerker, WP 244 rev.01, 5 april 2017, p. 4 (voorbeelden van "wezenlijke gevolgen" in de zin van artikel 4(23) AVG).

[82] Overeenkomstig artikel 35(1) AVG kan één GEB een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden (zie verder; nr. 92).

en de passende maatregelen moet nemen om de toepassing van de bepalingen van de AVG te waarborgen.[83]

48. Het inschatten van risico's houdt in dat men de waarschijnlijkheid en ernst van het risico in kaart brengt. Bij de **inschatting** van het risico dient de verwerkingsverantwoordelijke zich de volgende vragen te stellen: hoe groot is de mogelijke impact op betrokkenen en hoe waarschijnlijk is het dat deze impact zich voordoet? Op deze vragen is niet altijd een zwart-wit antwoord mogelijk, in de praktijk zal het vaak gaan om een afweging. Aan de hand hiervan kan het **risiconiveau** worden bepaald.[84]

49. Bij de beoordeling van de risico's is het belangrijk dat er rekening gehouden met de oorsprong, de aard, het specifieke karakter en de ernst van de risico's in kwestie.[85] Dit houdt in het bijzonder in dat men voor elk risico **minstens de volgende elementen** in kaart brengt:

- de bronnen van de risico's[86];
- de mogelijke gevolgen voor de rechten en vrijheden van de betrokkenen, in het bijzonder in geval van gebeurtenissen zoals onrechtmatige toegang, ongewenste wijziging en verdwijning van gegevens;
- de bedreigingen die kunnen leiden tot onrechtmatige toegang, ongewenste wijziging en de verdwijning van gegevens; en
- de waarschijnlijkheid en ernst van het risico.[87]

50. Overwegingen (84) en (90) AVG maken duidelijk dat de GEB zich in eerste instantie richt op het aanpakken van de "hoge" of "grote" risico's. Indien er bij een bepaalde verwerking bijv. een hoog risico is op reputatieschade maar slechts een zeer laag risico op discriminatie, dan dient dit laatste risico niet noodzakelijk als zodanig in de risicobeoordeling van een GEB te worden opgenomen. Desalniettemin raadt de Commissie aan om in het kader van een GEB alle risico's die niet verwaarloosbaar zijn uitdrukkelijk in kaart te brengen en afdoende beschermingsmaatregelen te identificeren, aangezien zelfs middelgrote risico's een belangrijke factor kunnen zijn bij de beoordeling van de proportionaliteit van de beoogde gegevensverwerking.[88] Bovendien ontslaat de uitvoering van een GEB de verwerkingsverantwoordelijke niet van zijn algemene verplichting om maatregelen te treffen om alle risico's voor de rechten en vrijheden van betrokkenen op passende wijze te beheren.

---

[83] Zoals eerder aangegeven zijn de volgende elementen relevant om de aard, omvang en context van de verwerkingen te bepalen: de persoonsgegevens, de ontvangers en de periode gedurende welke de persoonsgegevens worden geregistreerd de categorieën van betrokkenen, de schaal van de gegevensverwerking, de oorsprong van de gegevens, de verhouding tussen verwerkingsverantwoordelijke en betrokkenen en hoe gemakkelijk het is om betrokkenen te identificeren. Zie hoger, nr. 36.

[84] Rijksoverheid, Model PIA, p. 36.

[85] Zie overweging (84) AVG.

[86] Zie overweging (90) AVG.

[87] Groep 29, Richtsnoeren GEB, p. 28.

[88] Zie hoger; nr. 38 e.v.

Tot slot dient een GEB hoe dan ook een overzicht te bevatten van al de maatregelen die genomen worden om aan te tonen dat aan de AVG is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.[89] Ook vanuit die optiek is het belangrijk dat alle relevante risico's in rekening worden gebracht.

- *Welke methode dient men te gebruiken bij het beoordelen en beheer van risico's?*

51. De verwerkingsverantwoordelijke mag vrij kiezen welke methode hij wenst te hanteren, op voorwaarde dat deze leidt tot een **objectieve beoordeling** van het risico[90] en rekening houdt met de **minimale elementen** die de AVG voorschrijft. Het is aan de verwerkingsverantwoordelijke om een methode te hanteren die hem in staat stelt om de vereisten van de AVG na te leven. Dit betekent ook dat de keuze voor de ene of de andere methode verantwoord moet kunnen worden, rekening houdend met de aard, het toepassingsgebied, de context en de doeleinden van de verwerking.

52. Desalniettemin is de Commissie van oordeel dat een behoorlijk risicobeheer **een aantal minimale kenmerken** vertoont die worden opgesomd in bijlage 1 bij deze aanbeveling.

53. De Commissie acht het belangrijk dat iedere verwerkingsverantwoordelijke die een GEB onderneemt, een methode hanteert die aangepast is aan de noden en context van haar eigen onderneming. De behoefte aan een contextuele analyse belet niet dat een verwerkingsverantwoordelijke gebruik maakt van gestandaardiseerde procedures of modellen die door (of te samen met) andere entiteiten werden ontwikkeld (bijv. op niveau van een bepaalde sector of bedrijfstak) bij het uitvoeren van een risicobeoordeling.

54. Bovendien raadt de Commissie ten stelligste aan dat de verwerkingsverantwoordelijke zich baseert op reeds bestaande methoden inzake risicobeheer. Het gebruik van internationale standaarden, zoals deze ontwikkeld door de Internationale Organisatie voor Standaarden (ISO)[91], alsook gedragscodes ontwikkeld of erkend op Europees niveau, is hierbij van bijzonder belang.[92]

55. Ongeacht welke methode uiteindelijk door de verwerkingsverantwoordelijke weerhouden wordt, acht de Commissie het onontbeerlijk dat de verwerkingsverantwoordelijke uitdrukkelijk aangeeft welke

---

[89] Artikel 35(7)d AVG. Zie verder, nr. 56 e.v..

[90] Overweging (76) AVG bevestigt het objectieve karakter van deze beoordeling van het risico ten opzichte van de verwerking en de gevolgen hiervan voor de rechten en vrijheden van personen: "*Het risico moet worden bepaald op basis van een objectieve beoordeling en vastgesteld moet worden of de verwerking gepaard gaat met een risico of een hoog risico.*"

[91] In het bijzonder ISO 31000 (Risk management); ISO 27005 (Information security risk management) en ISO/IEC 29134 (Guidelines for privacy impact assessment). Zoals hoger aangegeven blijft iedere verwerkingsverantwoordelijke principieel vrij in zijn keuze over de methode die men hanteert. De verwerkingsverantwoordelijke is dan ook niet verplicht een welbepaalde (internationale of andere) standaard te hanteren, noch om een persoon aan te duiden die gecertificeerd is om volgens welbepaalde norm een GEB uit te voeren.

[92] Wat betreft gedragscodes erkend of ontwikkeld op Europees niveau zie ook nr. 94 e.v.

methode gekozen werd en dat deze op een consistente wijze wordt toegepast doorheen heel het proces van de GEB.

E) Beoogde maatregelen

56. Een GEB omvat niet enkel een risicobeoordeling, maar ook een overzicht van 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 de AVG is voldaan.[93]

57. Relevante maatregelen kunnen van zowel technische, organisatorische als juridische aard zijn, zo bijvoorbeeld

- *organisatorische maatregelen*: verhoging van bewustmaking, vorming, beleidsmaatregelen, functiescheiding (zgn. "Chinese wall"), rapportage, periodieke controles, extra keuze-, inspraak of bezwaarmogelijkheden voor betrokkenen, etc.
- *technische maatregelen*: technische beperkingen op de inzameling en/of mededeling van persoonsgegevens (bijv. gebruik van bijzondere cryptografische technieken om aan dataminimalisatie te doen), het anonimiseren, pseudonimiseren en/of versleutelen van persoonsgegevens nadat ze worden ingezameld, technische beperkingen op het hergebruik van persoonsgegevens (doelbinding), meerfactor-authenticatie, logging en monitoring, opsplitsing van gegevens, bijkomende back-ups, etc.
- *juridische maatregelen*: contractuele waarborgen, bindende bedrijfsvoorschriften, etc.[94]

58. Wanneer de beoogde gegevensverwerking gebruik maakt van profilering of zgn. "big data" analyses, kan het risico op verwerking van onjuiste gegevens en/of onrechtstreekse discriminatie toenemen. In dergelijke gevallen dient de verwerkingsverantwoordelijke passende wiskundige en statistische procedures te hanteren en technische en organisatorische maatregelen te treffen waarmee factoren die aanleiding geven tot onjuistheden van persoonsgegevens worden gecorrigeerd en het risico op fouten wordt geminimaliseerd.[95] De verwerkingsverantwoordelijke dient bovendien te voorkomen dat de verwerking discriminerende gevolgen zou hebben op grond van ras of etnische afkomst, politieke overtuiging, godsdienst of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische of gezondheidsstatus, of seksuele gerichtheid, of gevolgen zou hebben die leiden tot maatregelen met een vergelijkbaar effect.[96] Om te vermijden dat zulke gevolgen

[93] Artikel 35(7)d AVG.

[94] Zie verder ook Commission Informatique et Libertés, CNIL, Measures fort he privacy risk treamtent – Good Practices Catalogue, 2012, 92 p.; Information Commissioner's Office (ICO), Conducting privacy impact assessments – code of practice, p. 27-30 en Rijksoverheid, Model PIA, p. 37-38.

[95] Overweging (71) AVG.

[96] Idem. Zie verder ook Commissie voor de bescherming van persoonlijke levenssfeer, Big Data Rapport, 2017, p. 19-31 en Rijksoverheid, Model PIA, p. 39.

plaatsvinden, dient ook gekeken te worden naar de mogelijkheid dat een welbepaald risico een onevenredig grote kans heeft om bij bepaalde minderheden of beschermde groepen op te treden.

59. Bij de evaluatie van de beoogde maatregelen om de risico's aan te pakken, dient de verwerkingsverantwoordelijke zich ervan te vergewissen dat de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen op behoorlijke wijze in acht worden genomen.[97] Hierbij dient men steeds het totaalbeeld voor ogen te houden: de aard, omvang, context en het doel van de verwerking, de risico's, de stand van de techniek en de uitvoeringskosten.[98] Naarmate de risico's groter zijn, zal de verwachting ten aanzien van de verwerkingsverantwoordelijke omtrent te nemen maatregelen hoger liggen. Het is dus niet zo dat de verwerkingsverantwoordelijke steeds alle mogelijke maatregelen moet nemen. De AVG vereist enkel dat de maatregelen de risico's tot een aanvaardbaar niveau brengen en dat er een passend evenwicht is tussen de beoogde maatregelen en de betrokken risico's.[99]

60. De kostprijs van de beoogde maatregelen mag op zich geen reden zijn om over te gaan tot een verwerking zonder afdoende waarborgen. Indien de verwerkingsverantwoordelijke niet in staat is om voldoende waarborgen te voorzien en het risico tot een aanvaardbaar niveau te herleiden gelet op de beschikbare technologie en uitvoeringskosten, dient hij desgevallend hetzij van de verwerking af te zien, hetzij over te gaan tot een voorafgaande raadpleging van de toezichthoudende autoriteit.[100]

61. Bij de identificatie van de beoogde maatregelen dient de verwerkingsverantwoordelijke uitdrukkelijk aan te geven welke maatregelen dienen om welke risico's te beperken. Daarbij is het aanbevolen dat de verwerkingsverantwoordelijke ook uitdrukkelijk aangeeft:

- welke middelen nodig zullen zijn om de maatregelen te implementeren;
- welke persoon (of personen) verantwoordelijk zullen zijn voor het implementeren van de maatregelen;
- het tijdsbestek waarbinnen de maatregelen uitgevoerd zullen worden;
- hoe de doeltreffendheid van de maatregelen gecontroleerd en geëvalueerd zal worden.[101]

---

[97] Artikel 35(7)d AVG *in fine*.

[98] Zie ook artikelen 25(1) en 32(1) AVG.

[99] Rijksoverheid, Model PIA, p. 37. Het is ook belangrijk om op te merken dat het volledig uitsluiten risico's in principe niet mogelijk is. Er zal altijd een residueel risico overblijven. De verwerkingsverantwoordelijke dient te beschrijven hoe hij tot dit restrisico is gekomen en waarom hij dit aanvaardbaar acht. (*Id.*)

[100] Overweging (84) AVG. Zie verder nr. 63.

[101] ISO/IEC 29134, "Information technology – Security techniques – Guidelines for privacy impact assessment", 2017, p. 23. Wat het beheer en nazicht van de GEB betreft zie verder, nr. 96.

6. Wanneer is een voorafgaande raadpleging verplicht?

62. Artikel 36(1) AVG bepaalt dat:

> *"Wanneer uit een gegevensbeschermingseffectbeoordeling krachtens artikel 35 blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, raadpleegt de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit.*"

63. Uit de bewoording van artikel 36(1) AVG blijkt dat een voorafgaande raadpleging slechts verplicht is wanneer het *residuele* risico hoog is.[102] Een voorafgaande raadpleging is dan ook slechts vereist wanneer de GEB uitwijst dat de verwerking gepaard gaat met een hoog risico dat de verwerkingsverantwoordelijke niet kan beperken door maatregelen die met het oog op de beschikbare technologie en de uitvoeringskosten redelijk zijn.[103] Indien het risico afdoende beperkt kan worden aan de hand van passende technische en organisatorische maatregelen, dient er géén voorafgaande raadpleging plaats te vinden.[104]

64. Een onaanvaardbaar hoog restrisico bestaat bijvoorbeeld wanneer het waarschijnlijk is dat de betrokkenen met aanzienlijke of onomkeerbare gevolgen zou kunnen worden geconfronteerd (bijvoorbeeld een onrechtmatige toegang tot gegevens die leidt tot een bedreiging voor het leven van de betrokkenen, een ontslag, een financieel gevaar). Zo zou het duidelijk lijken dat het risico zich zal voordoen door de onmogelijkheid om toegang voldoende af te schermen vanwege de wijze waarop ze worden gedeeld, gebruikt of gedistribueerd, of wanneer een bekend kwetsbaar punt niet wordt weggewerkt of verholpen.[105]

65. Indien de toezichthoudende autoriteit van mening is dat de beoogde verwerking niet conform de AVG is of de risico's onvoldoende zijn onderkend of beperkt, geeft zij, binnen een maximumtermijn van acht weken na de ontvangst van het verzoek om raadpleging schriftelijk advies aan de verwerkingsverantwoordelijke en in voorkomend geval aan de verwerker, en mag zij al haar in artikel 58 AVG bedoelde bevoegdheden uitoefenen, inclusief de bevoegdheid om een tijdelijke of definitieve verwerkingsbeperking, inclusief een verwerkingsverbod, op te leggen.[106] Die termijn van 8 weken kan

---

[102] Artikel 35(1) AVG heeft, in tegenstelling tot artikel 36(1) AVG, betrekking op het "inherente" risico van de voorgenomen gegevensverwerking. Zie ook Groep 29, Richtsnoeren GEB, p. 10. Wat het onderscheid tussen het "inherente" en het "residuele" risico betreft zie hoger; nr. 43.

[103] Overweging (84) AVG.

[104] Groep 29, Richtsnoeren GEB, p. 23.

[105] Groep 29, Richtsnoeren GEB, p. 23.

[106] Artikel 58(2)e AVG.

met zes bijkomende weken worden verlengd.[107] De termijnen kunnen worden opgeschort totdat de toezichthoudende autoriteit informatie heeft verkregen waarom zij met het oog op de raadpleging heeft verzocht (artikel 36(2) AVG).

66. Wanneer een voorafgaande raadpleging verplicht is, verstrekt de verwerkingsverantwoordelijke de volgende informatie (artikel 36(3) AVG):

a) indien van toepassing, de respectieve verantwoordelijkheden van de verwerkingsverantwoordelijke, bij de verwerking betrokken gezamenlijke verwerkingsverantwoordelijken en verwerkers, in het bijzonder voor verwerking binnen een concern;

b) de doeleinden en de middelen van de voorgenomen verwerking;

c) de maatregelen en waarborgen die worden geboden ter bescherming van de rechten en vrijheden van betrokkenen uit hoofde van de AVG ;

d) indien van toepassing, de contactgegevens van de functionaris voor gegevensbescherming;

e) de gegevensbeschermingseffectbeoordeling waarin bij artikel 35 AVG is voorzien; en

f) alle andere informatie waar de toezichthoudende autoriteit om verzoekt.

7. Wie speelt er welke rol bij de uitvoering van een GEB?

A) De verwerkingsverantwoordelijke(n)

67. De verplichting tot het uitvoeren van een GEB rust in eerste instantie op de verwerkingsverantwoordelijke. Hij is diegene die de eindverantwoordelijkheid draagt en aanspreekbaar is indien de GEB niet (of niet naar behoren) wordt uitgevoerd wanneer dit overeenkomstig artikel 35 AVG wel verplicht is. De GEB kan door iemand anders, binnen of buiten de organisatie, worden uitgevoerd, maar de verwerkingsverantwoordelijke blijft de eindverantwoordelijke.[108]

68. De Commissie acht het onontbeerlijk dat de verwerkingsverantwoordelijke ervoor zorgt dat de juiste personen binnen de onderneming betrokken worden bij het risicobeoordelingsproces.[109] Om te vermijden dat het proces van risicobeoordeling herleid zou worden tot een louter schriftelijke oefening, dienen diegenen die best geplaatst zijn om bij te dragen aan een volwaardige risicobeoordeling tijdig

[107] Bij een dergelijke verlenging stelt de toezichthoudende autoriteit de verwerkingsverantwoordelijke en, in voorkomend geval, de verwerker binnen een maand na ontvangst van het verzoek om raadpleging in kennis van onder meer de redenen voor de vertraging.

[108] Groep 29, Richtsnoeren GEB, p. 18.

[109] Zie ook bijlage 1, punt 6.

betrokken te worden in het proces van identificatie, evaluatie en beheersing van risico's. De Commissie denkt hier in eerste instantie niet enkel aan de functionaris voor de gegevensbescherming en/of veiligheidsconsulent, maar ook aan de ontwikkelaars van nieuwe toepassingen (bijv. ICT-architecten), analisten, bedrijfsjuristen, zij die strategische beslissingen inzake projectontwikkeling nemen, verantwoordelijken voor de aanbesteding, verantwoordelijken voor personeelsbeheer, personeelsleden (of hun vertegenwoordigers) die gebruik zullen maken van de persoonsgegevens in kwestie bij de uitoefening van hun taken, etc.[110]

69. Het is een goede praktijk om de specifieke taken en verantwoordelijkheden van personen binnen de onderneming te omschrijven en te documenteren, rekening houdend met het interne beleid, de interne processen en regels. Bijvoorbeeld:

- als specifieke bedrijfseenheden voorstellen om een GEB uit te voeren, dienen die eenheden vervolgens input te geven voor de GEB en dienen ze te worden betrokken bij het valideren van deze GEB;
- indien passend wordt aanbevolen om het advies te vragen van onafhankelijke deskundigen van verschillende beroepen (advocaten, IT-deskundigen, beveiligingsdeskundigen, sociologen, ethici, etc.).
- het hoofd informatiebeveiliging (Chief Information Security Officer, CISO), indien aangesteld, alsmede de functionaris voor gegevensbescherming, zouden kunnen voorstellen dat de verwerkingsverantwoordelijke een GEB 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 GEB uit te voeren op een specifieke verwerking, afhankelijk van de veiligheids- of operationele behoeften.[111]

70. Indien de verwerkingsverantwoordelijke een functionaris voor gegevensbescherming heeft aangewezen, is de verwerkingsverantwoordelijke hoe dan ook verplicht om diens advies in te winnen[112], en dat advies moet samen met de beslissingen van de verwerkingsverantwoordelijke in de

[110] Het verdient de aanbeveling om de taak en rol van ieder van deze personen bij de uitvoering van (onderdelen van) een GEB uitdrukkelijk te documenteren. Voor een voorbeeld van hoe die verdeling er kan uit zien zie Commission Nationale de l'Informatique et des Libertés (CNIL), "Privacy Impact Assessment (PIA) - Methodology (how to carry out a PIA)", 2015, p. 9.

[111] Groep 29, Richtsnoeren GEB, p. 19.

[112] Artikel 35(2) AVG.

GEB worden gedocumenteerd.[113] De functionaris voor gegevensbescherming dient ook toe te zien op de uitvoering van de GEB.[114]

71. Bovendien raadt de Commissie ook aan dat de uiteindelijke beslissingen die worden genomen naar aanleiding van een GEB op een hiërarchisch voldoende hoog niveau worden genomen. De goedkeuring van een GEB, of de beslissing om niet tot uitvoering van een GEB over te gaan, zou bijvoorbeeld formeel ter goedkeuring van de directieleden of een intern gemandateerd orgaan kunnen worden voorgelegd.[115] Aangezien de uitvoering van een GEB slechts verplicht is wanneer er sprake is van waarschijnlijk een hoog risico voor de fundamentele rechten en vrijheden van natuurlijke personen, is het logisch dat de beslissingen die naar aanleiding van een GEB uitdrukkelijk rechtstreeks of onrechtstreeks gedragen worden door het hoogste orgaan van de onderneming.

72. Wanneer gezamenlijke verwerkingsverantwoordelijken bij de verwerking betrokken zijn, moeten ze hun respectieve verplichtingen precies bepalen. In hun GEB 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.[116]

B) De verwerker

73. De verwerker dient, afhankelijk van de aard van de verwerking, aan de verwerkingsverantwoordelijke bijstand te verlenen bij het uitvoeren van een GEB. In eerdere ontwerpversies van de AVG werd zelfs uitdrukkelijk voorzien dat de verplichting tot het uitvoeren van een GEB als dusdanig ook rechtstreeks op de verwerker zou komen te rusten. In de finale versie van de AVG wordt echter bepaald dat de *overeenkomst* tussen de verwerkingsverantwoordelijke en de verwerker moet bepalen dat de verwerker:

> "*rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie de verwerkingsverantwoordelijke bijstand verleent bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36*".[117]

[113] Groep 29, Richtsnoeren GEB, p. 18.

[114] Artikel 39(1)c AVG. Zie ook verder; nr. 76.

[115] Zie ook bijlage 1, punt 7.

[116] Groep 29, Richtsnoeren GEB, p. 8.

[117] Artikel 28(3)f AVG.

74. Overweging (95) AVG bevestigt dat de verwerker de verwerkingsverantwoordelijke, "indien nodig en op verzoek" dient bij te staan om ervoor te zorgen dat de verplichtingen ingevolge de uitvoering van een GEB en voorafgaande raadpleging van de toezichthoudende autoriteit worden nagekomen.

75. In het licht van voormelde bepalingen dient de omvang van bijstandsplicht van de verwerker bepaald te worden in het licht van (1) de aard van de verwerking; (2) de informatie die ter beschikking van de verwerker staat; (3) de opportuniteit van de bijstand vanwege de verwerker om te komen tot een volwaardige en correcte risicobeoordeling en –beheersing.

C) De functionaris voor gegevensbescherming

76. De Commissie acht het vanzelfsprekend dat de functionaris voor gegevensbescherming, wanneer die is aangeduid, de verwerkingsverantwoordelijke adviseert bij het uitvoeren van een GEB. Artikel 35(2) AVG bevestigt uitdrukkelijk dat wanneer een functionaris voor gegevensbescherming is aangewezen, de verwerkingsverantwoordelijke bij het uitvoeren van een GEB diens advies zal inwinnen.

77. De eindverantwoordelijkheid voor de behoorlijke uitvoering van de GEB ligt, net als bij de andere verplichtingen waarin de AVG voorziet, bij de verwerkingsverantwoordelijke en niet bij de functionaris voor gegevensbescherming. In de AVG staat immers duidelijk dat het de verwerkingsverantwoordelijke is die passende maatregelen moet treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd.[118] De rol van de functionaris is bijgevolg een adviesrol, geen beslissingsrol.[119]

78. Zoals hierboven reeds aangegeven acht de Commissie het onontbeerlijk dat de verwerkingsverantwoordelijke de nodige maatregelen neemt om ervoor te zorgen dat de juiste personen binnen de onderneming betrokken worden bij het risicobeoordelingsproces. Het is niet de bedoeling dat de functionaris voor gegevensbescherming geheel op eigen houtje een GEB opstelt.[120]

79. De adviesrol van de functionaris voor gegevensbescherming dient o.m. betrekking te hebben op de volgende aangelegenheden:

- of er al dan niet een GEB moet worden uitgevoerd;

[118] Groep 29, Richtlijnen voor functionarissen voor gegevensbescherming, p. 21. Zie artikelen 5(2) en 24(1) AVG.

[119] Enige ander lezing zou bovendien mogelijks tot een belangenconflict kunnen leiden: zie Groep 29, Richtlijnen voor functionarissen voor gegevensbescherming, p. 20 ("*Dit houdt met name in dat de functionaris voor gegevensbescherming binnen de organisatie geen functie kan bekleden waarbij hij of zij de doelstellingen van en de middelen voor de verwerking van persoonsgegevens moet bepalen*").

[120] Dit blijkt uit o.m. uit artikel 39(1)c AVG, dat bepaalt dat de functionaris voor gegevensbescherming desgevraagd *advies* verstrekt en *toeziet* op de uitvoering ervan.

- welke methode bij een GEB moet worden gevolgd;
- of de GEB intern uitgevoerd of uitbesteed moet worden;
- welke waarborgen (waaronder technische en organisatorische maatregelen) moeten worden toegepast om eventuele risico's voor de rechten en belangen van de betrokkenen te beperken;
- of de GEB al dan niet correct is uitgevoerd en of de conclusies (de verwerking al dan niet uitvoeren en welke waarborgen toepassen) al dan niet in overeenstemming zijn met de AVG.[121]

Als de verwerkingsverantwoordelijke niet met het door de functionaris voor gegevensbescherming verleende advies instemt, moet in de documentatie over de GEB specifiek en schriftelijk worden gemotiveerd waarom met het advies geen rekening is gehouden.[122]

D) <u>De betrokkenen of hun vertegenwoordigers</u>

80. Artikel 35(9) AVG bepaalt dat:

"*De verwerkingsverantwoordelijke vraagt in voorkomend geval de betrokkenen of hun vertegenwoordigers naar hun mening over de voorgenomen verwerking, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van verwerkingen.*".

81. De Commissie merkt op dat het afzonderlijk lezen van de Engelstalige, Franstalige en Nederlandstalige versies van artikel 35(9) AVG tot uiteenlopende interpretaties zou kunnen leiden. Waar de Nederlandstalige versie aangeeft dat de raadpleging van de betrokkenen of hun vertegenwoordigers "*in voorkomend geval*" dient plaats te vinden, geeft de Engelstalige tekst aan dat dergelijke raadpleging dient plaats te vinden "*where appropriate*". De Franstalige tekst spreekt van "*le cas écheant*".

82.De Commissie is van mening dat het idee achter de gekozen bewoording eenduidig is, meer bepaald dat de beslissing om al dan niet over te gaan tot de raadpleging van de betrokkenen (of hun vertegenwoordigers) in de eerste plaats aan de verwerkingsverantwoordelijke toekomt. Het is voor de verwerkingsverantwoordelijke echter niet geheel vrijblijvend om de betrokkenen of hun vertegenwoordigers al dan niet te raadplegen. Waar er voldoende gewichtige redenen bestaan om tot dergelijke raadpleging over te gaan, gelet op de aard, de omvang, de context en het doel van de verwerking, alsook de mogelijke impact op de betrokkenen, dan is het nodig dat dergelijke raadpleging ook daadwerkelijk plaatsvindt. Een raadpleging van betrokkenen is in het bijzonder aangewezen

[121] Groep 29, Richtlijnen voor functionarissen voor gegevensbescherming, p. 22.

[122] Idem. De Groep 29 raadt verder aan dat de verwerkingsverantwoordelijke bijvoorbeeld in de overeenkomst van de functionaris voor gegevensbescherming, maar ook in informatie die aan werknemers, management (en andere betrokkenen, indien van toepassing) wordt verstrekt, duidelijk de precieze taken van de functionaris voor gegevensbescherming en hun omvang vast te leggen, met name wat betreft het uitvoeren van een gegevensbeschermingseffectbeoordeling.

wanneer zij over essentiële informatie beschikken of belangrijke opmerkingen kunnen aanleveren die relevant zijn voor de uitvoering van de GEB. 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.[123]

83. De raadpleging van betrokkenen of hun vertegenwoordigers kan een belangrijke meerwaarde betekenen, zowel bij de identificatie en beoordeling van de risico's van de verwerking, als bij de finaliseren van een GEB, om na te gaan of alle risico's op een afdoende wijze in kaart werden gebracht. De omvang van de raadpleging (welke personen en hoeveel) wordt best bepaald in functie van het risico en de omvang van de verwerking. Indien een voorgenomen verwerking enkel risico's met zich meebrengt voor een beperkt aantal betrokkenen (bijv. werknemers van een kleine organisatie), dan kan de raadpleging beperkt worden tot een beperkt aantal van die werknemers en/of hun vertegenwoordigers. Indien de voorgenomen verwerking risico's inhoudt voor een groot aantal betrokkenen (bijv. alle inwoners), dan dient er een ruimere raadpleging georganiseerd te worden.[124]

84. De verwerkingsverantwoordelijke beslist in beginsel vrij hoe betrokkenen of hun vertegenwoordigers geraadpleegd worden. Hun mening kan op velerlei manieren gevraagd worden, 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).[125] Indien hij over hun contactgegevens beschikt, kan hij hen rechtstreeks aanschrijven met de vraag naar hun mening over de voorgenomen gegevensverwerking (bijv. via email). Waar de identiteit van de betrokkenen niet op voorhand gekend is, zou de verwerkingsverantwoordelijke bijv. een publieke consultatie kunnen organiseren. Waar passend kan de verwerkingsverantwoordelijke ook een gezamenlijk overlegmoment inlassen. Ofschoon artikel 35(9) AVG enkel naar de "betrokkenen of hun vertegenwoordigers" verwijst, kan het inwinnen van standpunten van organisaties die meer in het algemeen de belangen van betrokkenen of consumenten behartigen ook een meerwaarde betekenen.

85. De verwerkingsverantwoordelijke dient er in het kader van de raadpleging over te waken dat de vragen worden gesteld op een manier die tot betrouwbare resultaten leidt (bijv. door middel van een gevalideerde vragenlijst).

---

[123] Groep 29, Richtsnoeren GEB, p. 18-19.

[124] ISO/IEC 29134, "Information technology – Security techniques – Guidelines for privacy impact assessment", 2017, p. 13.

[125] Groep 29, Richtsnoeren GEB, p. 18.

86. 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.[126]

E) De toezichthoudende autoriteit

87. Zoals reeds vermeld is een voorafgaande raadpleging slechts verplicht indien blijkt dat het residuele risico van de voorgenomen verwerking hoog is. Indien het risico afdoende beperkt kan worden aan de hand van passende technische en organisatorische maatregelen, dient er géén voorafgaande raadpleging plaats te vinden.

88. De Commissie onderschrijft de beleidskeuze van de Europese wetgever waarbij enkel problematische gevallen voorafgaand ter advies worden voorgelegd. Dit is een toepassing van het "verantwoordelijkheidsbeginsel" en het benadrukt tevens dat de toezichthoudende autoriteit haar activiteiten moet kunnen toespitsen daar waar de nood het zwaarst doorweegt. Dit neemt niet weg dat de verwerkingsverantwoordelijke moet klaar staan om, op verzoek van de toezichthoudende autoriteit, een GEB voor te leggen voor al die verwerkingen die een waarschijnlijk hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen.

F) Het brede publiek

89. Er bestaat geen wettelijke verplichting tot het publiceren van een GEB. Het is de verwerkingsverantwoordelijke die zelf beslist om een GEB al dan niet te publiceren. De Commissie moedigt verwerkingsverantwoordelijken echter aan om publicatie van een GEB te overwegen.[127] De gepubliceerde GEB hoeft niet de volledige beoordeling te bevatten, vooral wanneer de GEB 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 GEB, of zelfs gewoon een verklaring dat een GEB is uitgevoerd.[128]

[126] Groep 29, Richtsnoeren GEB, p. 18.

[127] Groep 29, Richtsnoeren GEB, p. 22. Publicatie kan het vertrouwen in de verwerkingen van de verwerkingsverantwoordelijke verhogen en blijk geven van transparantie. Het is een bijzonder goede praktijk om een GEB 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. (Id.)

[128] Groep 29, Richtsnoeren GEB, p. 22.

8. Bijzondere bepalingen

A) Verwerking op grond van een wettelijke verplichting of algemeen belang

90. Artikel 35(10) AVG voorziet twee omstandigheden waarin de verplichting tot het uitvoeren van een GEB mogelijks niet van toepassing is, m.n.:

- wanneer de voorgenomen verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust; en
- wanneer de voorgenomen verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Opdat deze uitzondering van toepassing zou zijn, is echter vereist dat:

- de verwerking haar rechtsgrond heeft in het Unierecht of in het recht van de lidstaat dat op de verwerkingsverantwoordelijke van toepassing is;
- de specifieke verwerking of geheel van verwerkingen in kwestie daarbij wordt geregeld; en
- er reeds als onderdeel van een algemene effectbeoordeling in het kader van de vaststelling van deze rechtsgrond een GEB is uitgevoerd.[129]

Bovendien staat het de wetgever nog steeds vrij om te bepalen dat er nog steeds een GEB uitgevoerd dient te worden voorafgaand aan de verwerking.[130]

91. De Commissie herinnert eraan dat de toezichthoudende autoriteit in de regel dient te worden geraadpleegd tijdens de voorbereiding van een wetgevings- of regelgevingsmaatregel die betrekking heeft op de bescherming van persoonsgegevens.[131] Het al dan niet bestaan van een voorafgaande raadpleging doet echter geen afbreuk aan de algemene verplichting van de verwerkingsverantwoordelijke om aan risicobeheersing te doen overeenkomstig artikel 24(1) AVG. Bovendien is de Commissie van oordeel dat de uitvoering van een (aanvullende) GEB in bepaalde gevallen nog steeds opportuun of noodzakelijk kan zijn, in het bijzonder wanneer men tijdens de voorbereiding van een wetgevings- of regelgevingsmaatregel geen duidelijk zicht heeft op de gegevensverwerkingen die bij de uitvoering zullen plaatsvinden.[132]

---

[129] Overweging (93) AVG verduidelijkt enigszins deze bepaling: "*In het kader van de vaststelling van het lidstatelijke recht waarop de vervulling van de taken van de overheidsinstantie of het overheidsorgaan is gebaseerd, en waarin de specifieke verwerking of reeks verwerkingen wordt geregeld, kunnen de lidstaten het noodzakelijk achten een dergelijke beoordeling uit te voeren voordat met de verwerking wordt begonnen.*"

[130] Artikel 35(10) AVG *in fine*.

[131] Zie artikel 57(1)c AVG.

[132] Zie ook Groep 29, Richtsnoeren GEB, p. 16 ("*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*

B) Vergelijkbare of gezamenlijke verwerkingsactiviteiten

92. Een GEB kan betrekking hebben op een enkele gegevensverwerking of op een reeks vergelijkbare verwerkingen.[133] Een enkele GEB kan volstaan voor meerdere verwerkingen die vergelijkbaar zijn in termen van aard, omvang, context, doel en risico's. Een GEB is 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 GEB 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.[134]

93. In bepaalde gevallen kan het redelijk en nuttig zijn dat de GEB 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.[135] De Commissie moedigt verwerkingsverwerkingsverantwoordelijken die van plan zijn om een gemeenschappelijk applicatie- of verwerkingsplatform op te zetten aan om op gezamenlijke basis een GEB uit te voeren (in de omstandigheden waar de uitvoering van een GEB vereist is[136]). Dezelfde aanbeveling geldt ook voor verwerkingsverantwoordelijken die uit hoofde van hun activiteiten onderdeel uitmaken van een overkoepelende organisatie of vereniging (zoals bijv. scholen, sportclubs, jeugdbewegingen, artsen, advocaten, journalisten, enz.) wanneer ieder van deze verwerkingsverantwoordelijken een reeks vergelijkbare verwerkingen beogen die vergelijkbare hoge risico's inhouden.

C) Gedragscodes

94. Artikel 35(8) AVG bepaalt dat:

> "*Bij het beoordelen van het effect van de door een verwerkingsverantwoordelijke of verwerker verrichte verwerkingen, en met name ter wille van een gegevensbeschermingseffectbeoordeling, wordt de naleving van de in artikel 40 bedoelde goedgekeurde gedragscodes naar behoren in aanmerking genomen.*"

---

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.")

[133] Artikel 35(1) AVG. Zie ook Groep 29, Richtsnoeren GEB, p. 8.

[134] Artikel 35(1) AVG. Zie ook Groep 29, Richtsnoeren GEB, p. 8. 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. (*Id.*)

[135] Overweging (92) AVG.

[136] Zie hierover hoger, afdeling 3.

95. Artikel 40 AVG bepaalt dat "*de lidstaten, de toezichthoudende autoriteiten, het Comité en de Commissie (...) de opstelling van gedragscodes [*bevorderen] *die, met inachtneming van de specifieke kenmerken van de diverse gegevensverwerkingssectoren en de specifieke behoeften van kleine, middelgrote en micro-ondernemingen, moeten bijdragen tot de juiste toepassing van deze verordening*". Overeenkomstig artikel 35(8) AVG moet de verwerkingsverantwoordelijke dergelijke gedragscodes in aanmerking nemen wanneer een GEB uitgevoerd wordt. De Commissie vestigt er tenslotte nog de aandacht op dat de Europese Commissie, bij middel van een uitvoeringshandeling, bepaalde gedragscodes, na de goedkeuring ervan door het ECGB, algemeen verbindend kan verklaren.[137]

D) Beheer en nazicht

96. Artikel 35(11) AVG bepaalt dat de verwerkingsverantwoordelijke, indien nodig, dient te toetsen of de verwerking overeenkomstig de GEB wordt uitgevoerd. Dergelijke toetsing dient ten minste plaats te vinden wanneer sprake is van een verandering van het risico dat de verwerkingen inhouden.[138]

97. Artikel 35(11) AVG bevat twee onderdelen: enerzijds bevat zij een verplichting om indien nodig na te gaan of de gegevensverwerking daadwerkelijk overeenkomstig de GEB wordt uitgevoerd (met inbegrip van de aangeduide beschermingsmaatregelen). Anderzijds bevat zij de verplichting om de GEB te herzien indien er een sprake is van een verandering van het risico.

98. Een verandering van het risico van de verwerking kan aan verschillende elementen te wijten zijn, zoals een wijziging in de gebruikte verwerkingsmiddelen of een evolutie in de stand van de techniek (bijv. wanneer nieuwe technieken voor dataminimalisatie voorhanden zijn) of de ontdekking van een nieuwe kwetsbaarheid in beveiliging die de aanname van bijkomende of nieuwe beveiligingsmaatregelen verantwoorden.[139] Het nazicht van een GEB kan ook noodzakelijk worden omdat de organisatorische of maatschappelijke context voor de verwerkingsactiviteit is veranderd (bijv. 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.[140]

99. Omgekeerd kunnen bepaalde veranderingen het risico ook doen afnemen. Een verwerking kan bijv. zo evolueren dat beslissingen niet langer worden geautomatiseerd, of een monitoringactiviteit

---

[137] Artikel 40(9) AVG.

[138] Artikel 35 (11) AVG.

[139] Zie ook F. Bieker, M. Friedwald, M. Hansen, H. Obersteller en M. Rost, "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation", in S. Schiffner et al. (Eds.), APF (Annual Privacy Forum) 2016, 2016, p. 24.

[140] Groep 29, Richtsnoeren GEB, p. 17.

wordt niet langer stelselmatig uitgevoerd. In dat geval kan uit de herziening van de uitgevoerde risicoanalyse blijken dat de uitvoering van een GEB niet meer nodig is.[141]

100. Aangezien risico's doorgaans evolueren met de tijd, raadt de Commissie aan om bij de uitvoering van een GEB uitdrukkelijk een periodiek nazicht in te bouwen.[142] De frequentie van het periodiek nazicht dient bepaald te worden in functie van het risico die de verwerking inhoudt. Bovendien kan de uitvoering van een GEB zelf factoren aan het licht brengen die een bijzondere opvolging vereisen (bijv. technische of organisatorische maatregelen waarvan de effectiviteit nog niet vast staat). In het kader van een goed risicobeheer verwacht de Commissie dat de verwerkingsverantwoordelijke minstens om de 3 jaar een nazicht inbouwt. De Commissie raadt aan dat ook de uitkomst van het nazicht formeel ter goedkeuring van het bestuur van de organisatie of van een intern gemandateerd orgaan van de verwerkingsverantwoordelijke wordt voorgelegd.[143]

E) <u>Wat met reeds bestaande verwerkingen?</u>

101. De verplichting tot het uitvoeren van een GEB is van toepassing vanaf 25 mei 2018. Verwerkingen die aanleiding geven tot een waarschijnlijk hoog risico en die aanvangen na 25 mei 2018 zullen bijgevolg voorafgegaan moeten worden door een GEB. Voor reeds bestaande verwerkingen is een GEB in beginsel slechts vereist indien de risico's voor de rechten en vrijheden voor natuurlijke personen na 25 mei 2018 veranderen, bijvoorbeeld omdat een nieuwe technologie in gebruik is genomen of omdat persoonsgegevens voor een ander doel worden gebruikt.[144]

102. Het voorgaande betekent niet dat verwerkingsverantwoordelijken enkel tot uitvoering van een GEB moeten overgaan wanneer de verwerking zelf wordt aangepast. Zoals hoger gesteld kunnen de risico's die een verwerking inhoudt ook evolueren door veranderingen in de omgeving waarin de gegevensverwerking plaatsvindt (bijv. maatschappelijke context, gevolgen van de verwerking) waardoor nieuwe kwetsbaarheden kunnen ontstaan.[145] Van zodra er sprake is van een verandering van het risico dat de verwerking inhoudt (en de verwerking nog steeds waarschijnlijk een hoog risico inhoudt), is de uitvoering van een GEB verplicht.

103. De Commissie beveelt verwerkingsverantwoordelijke in ieder geval aan om, als een goede praktijk, over te gaan tot het uitvoeren van een GEB voor alle bestaande verwerkingen die een waarschijnlijk hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. Zelfs wanneer een GEB strikt genomen niet vereist is op 25 mei 2018, is het nodig dat de

---

[141] Groep 29, Richtsnoeren GEB, p. 16-17.

[142] Zie ook hoger, nr. 61.

[143] Zie ook hoger; nr. 71.

[144] Groep 29, Richtsnoeren GEB, p. 16-17.

[145] Zie hoger; nr. 98.

verwerkingsverantwoordelijke op het juiste moment een GEB uitvoert als onderdeel van zijn algemene verantwoordingsplicht en risicobeheer.[146]

104. Verwerkingen die reeds het voorwerp hebben uitgemaakt van een (algemene of specifieke) machtiging door een van de Sectorale Comités van de Commissie dienen in beginsel niet het voorwerp uit te maken van een GEB voor zover de verwerking overeenkomstig de voorafgaande modaliteiten van de machtiging wordt uitgevoerd. Overweging (171) AVG bepaalt immers dat door de toezichthoudende autoriteiten verleende toestemmingen die op Richtlijn 95/46/EG zijn gebaseerd, van kracht blijven totdat zij worden gewijzigd, vervangen of ingetrokken.[147] Omgekeerd betekent dit dat elke verwerking waarvan de uitvoeringsvoorwaarden (omvang, doel, verzamelde persoonsgegevens, identiteit van de verwerkingsverantwoordelijken of ontvangers, bewaartermijn van de gegevens, technische en organisatorische maatregelen enz.) sinds de machtiging zijn veranderd en die waarschijnlijk een hoog risico inhoudt, aan een GEB moet worden onderworpen.[148]

F) Mogelijke boete in geval van niet-naleving

105. Als niet aan de eisen van artikelen 35 en 36 AVG wordt voldaan, kan dat een boete tot gevolg hebben. Als er geen GEB wordt uitgevoerd terwijl dat voor de verwerking wel verplicht is (artikel 35 AVG, leden 1, 3 en 4), of als een GEB niet correct wordt uitgevoerd (artikel 35 AVG, leden 2, 7, 8 en 9), of als de bevoegde toezichthoudende autoriteit niet wordt geraadpleegd terwijl dat wel vereist is (artikel 36 AVG, 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.[149]

De Wnd. Administrateur, De Voorzitter,

(get.) An Machtens (get.) Willem Debeuckelaere

[146] Groep 29, Richtsnoeren GEB, p. 17.

[147] Zie in dit verband ook artikel 111 van de Wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit* (B.S., 10 januari 2018).

[148] Groep 29, Richtsnoeren GEB, p. 16. Zoals hierboven aangegeven zal ingevolge artikel 35(10) AVG de verplichting tot het uitvoeren van een GEB onder bepaalde voorwaarden niet van toepassing zijn wanneer de voorgenomen verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of wanneer de voorgenomen verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Zie hoger, nrs. 90-91.

[149] Groep 29, Richtsnoeren GEB, p. 5.

9. Bijlage 1 : Minimale kenmerken van een behoorlijk risicobeheer

Iedere verwerkingsverantwoordelijke kiest zelf welke procedure en methode hij wenst te hanteren bij het inschatten en beheren van risico's, op voorwaarde dat deze beantwoordt aan een aantal minimumkenmerken van betrouwbaarheid en objectiviteit.[150] Om te vermijden dat er een situatie van rechtsonzekerheid zou ontstaan bij gebrek aan bijkomende elementen waaraan de kwaliteit van een risicobeoordeling getoetst kan worden, formuleert de Commissie hieronder een aantal **minimale kenmerken**. De Commissie beklemtoont dat het hier gaat om minimale kenmerken, die op zich geen garantie inhouden dat de beoogde verwerking(en) conform de AVG zal (zullen) plaatsvinden.

1. Methodologisch onderbouwd

Risicobeheer en risicobeoordeling dienen methodologisch onderbouwd te zijn, bij voorkeur aan de hand van reeds bestaande methoden inzake risicobeheer. Internationale standaarden, zoals deze ontwikkeld door de Internationale Organisatie voor Standaarden (ISO)[151], alsook gedragscodes ontwikkeld of erkend op Europees niveau, zijn hierbij van bijzonder belang.
De verwerkingsverantwoordelijke mag evenwel vrij kiezen welke methode hij wenst te hanteren, op voorwaarde dat deze leidt tot een objectieve beoordeling van het risico en rekening houdt met de minimale elementen die de AVG voorschrijft. De verwerkingsverantwoordelijke dient wel uitdrukkelijk aan te geven welke methode gekozen werd en dient erover te waken dat deze op een consistente wijze wordt toegepast.

2. Gestructureerd

Een behoorlijk risicobeheer verloopt op een gestructureerde wijze, waarbij men doorgaans de volgende stappen kan onderscheiden[152]:

- communicatie en consultatie met interne en externe belanghebbenden;
- definitie van de relevante context (inclusief een beschrijving van het voorwerp van de risicoanalyse, definitie van de criteria om de risico's voor de rechten en vrijheden van natuurlijke personen in te schatten en de definitie van (on)aanvaardbare risicowaarden);
- identificatie, analyse en evaluatie van risico's (inclusief de identificatie van kwetsbaarheden, bedreigingen, en de toekenning van een risicowaarde);

---

[150] Zie ook hoger, nr. 51. Het is belangrijk dat de gekozen methode toelaat om risico's te analyseren van het perspectief van de betrokkene. Aangezien een GEB een instrument is om de risico's voor de rechten van de betrokkenen te beheren, staat het perspectief van de betrokkene centraal. Dit verschilt van risicobeheer op andere gebieden (zoals bv. informatiebeveiliging), die doorgaans gericht zijn op de belangen en doelstellingen van de organisatie zelf.

[151] Zie o.m. ISO 31000 (Risk management) en ISO 27005 (Information security risk management). Deze standaarden hebben een algemene draagwijdte en zijn niet specifiek toegespitst op het uitvoeren van een GEB. Bij de toepassing ervan dient rekening te houden met de bijzondere invulling die de AVG geeft aan het begrip "risico", alsook met de mogelijk waarborgen en mechanismen die ingezet kunnen worden om deze risico's te beperken.

[152] Gebaseerd op IEC/ISO, "Risk management – Risk management techniques", IEC/ISO 31010, v1.0, 2009-11, p. 8.

- identificatie van passende risico-beperkende maatregelen (i.e. de technische, organisatorische en juridische maatregelen die noodzakelijk zijn om het risico tot een aanvaardbaar niveau te herleiden); en
- beheer en nazicht.

3. Op maat

Een risicobeoordeling is steeds maatwerk en is aangepast aan de context en het risicoprofiel van de onderneming die beoordeling uitvoert.[153] Een behoorlijke risicobeoordeling bestaat niet uit een eenvoudig kopiëren van eerder gevoerde analyses maar vergt een concrete inschatting op basis van de specifieke context (i.e. onder verwijzing naar de aard, het toepassingsgebied, de context en de doeleinden van de verwerking). Niets belet daarentegen dat een verwerkingsverantwoordelijke gebruik maakt van procedures of modellen die door (of te samen met) andere entiteiten werden ontwikkeld (bijv. op niveau van een bepaalde sector of bedrijfstak) bij het uitvoeren van risicobeoordeling.

4. Begrijpelijk

De uitkomst van een risicobeoordeling dient leesbaar en toegankelijk zijn voor een zo breed mogelijk publiek. De uitkomst mag niet enkel leesbaar is voor (risico)experten, technici of gespecialiseerd personeel. Beknopte samenvattingen en visuele weergaves (bvb. kleurgrafiek, tabel met cijfers) kunnen de toegankelijkheid van de risicobeoordeling (zowel het proces als de schriftelijke weergave daarvan) bevorderen.[154]

5. Voldoende genuanceerd

Een risicobeoordeling dient voldoende schalen te bevatten teneinde een genuanceerde evaluatie van geïdentificeerde risico mogelijk te maken. Het voorzien van slechts drie schalen (laag, medium en hoog) om risico's te beoordelen is niet altijd voldoende om tot een correcte appreciatie te leiden. Een duidelijke omschrijving van de criteria die gehanteerd worden om het risico niveau in te schatten is hoe dan ook onontbeerlijk.

6. Communicatie en consultatie

Een behoorlijk systeem van risicobeheersing betrekt diegenen die best geplaatst zijn om bij te dragen aan het proces van identificatie, analyse, evaluatie en beheersing van risico's. Tot deze groep behoort niet enkel de functionaris voor de gegevensbescherming en/of veiligheidsconsulent, maar ook de ontwikkelaars van nieuwe toepassingen, zij die strategische beslissingen inzake projectontwikkeling

---

[153] IEC/ISO, "Risicomanagement – Principes en richtlijnen", ISO 31000, v1.0, 2009-11, p. 8.

[154] De Commissie begrijpt dat de documentatie die in de loop van het risico-beoordelingsproces gegenereerd wordt, blijk kan geven van een hogere graad van techniciteit, die mogelijks niet onmiddellijk toegankelijk is voor niet-experten. De Commissie onderstreept hier enkel dat de uitkomst van de risicobeoordeling steeds leesbaar en toegankelijk moet zijn.

nemen en de personeelsleden (of hun vertegenwoordigers) die gebruik zullen maken van de persoonsgegevens in kwestie bij de uitoefening van hun taken. In voorkomend geval vraagt de verwerkingsverantwoordelijke de mening van de betrokkenen of hun vertegenwoordigers, met inachtneming van de bescherming van commerciële of algemene belangen of de beveiliging van de verwerking.

7. Beheer en nazicht

Er dient een gedateerde en schriftelijke rapportering van de uitgevoerde risicobeoordelingen te bestaan. Een intern gemandateerd orgaan dat beslissingen neemt (bvb. directiecomité, strategisch comité of veiligheidscomité met een mandaat van de raad van bestuur) dient periodiek op de hoogte te worden gebracht van de uitkomst (of status) van het risicobeoordelingsproces. Dit gemandateerd orgaan dient de inschatting van de risico's alsook de maatregelen ter beperking van de risico's formeel goed te keuren.

Het proces van risicobeoordeling mag evenwel niet herleid worden tot een louter bureaucratisch proces. De verwerkingsverantwoordelijke dient passende maatregelen te nemen om ervoor te zorgen dat het behoorlijk beheer van risico's onderdeel wordt van de "bedrijfscultuur" van de verwerkingsverantwoordelijke.

Een uitgevoerde risicobeoordeling dient periodiek nagezien te worden en minstens in het geval van wijzigende omstandigheden die een wezenlijke invloed kunnen uitoefenen op een beoordeling die in het verleden werd uitgevoerd. De frequentie van het periodiek nazicht dient bepaald te worden in functie van het risico die de verwerking inhoudt. Bovendien raadt de Commissie ook aan dat de uitkomst van het nazicht formeel ter goedkeuring van het hoogste orgaan in de organisatie van de verwerkingsverantwoordelijke wordt voorgelegd.

10. Bijlage 2: Lijst van het soort verwerkingen waarvoor een GEB verplicht is (art. 35(4) van de AVG)[155]

Iedere toezichthoudende autoriteit dient in toepassing van artikel 35(4) van de AVG een lijst op te stellen van het soort verwerkingen waarvoor een GEB verplicht is. Een dergelijk ontwerp van lijst werd voorbereid door de Commissie voor de bescherming van de persoonlijke levenssfeer en aangepast door de Gegevensbeschermingsautoriteit op 13 juni 2018. De Autoriteit heeft vervolgens deze lijst meegedeeld aan het Europees Comité voor gegevensbescherming (ECGB) opdat dit een advies zou uitbrengen overeenkomstig artikel 64 van de AVG.

Het Comité heeft zich uitgesproken in zijn advies 2/2018 van 25 september 2018. De Autoriteit heeft haar ontwerp aangepast om te voldoen aan de aanbevelingen van het Comité.

Ter herinnering, wanneer deze lijst betrekking heeft 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, dient, voorafgaand aan de vaststelling van de lijst, het in artikel 63 bedoelde coherentiemechanisme toegepast te worden.[156].

De Autoriteit benadrukt dat het bestaan van een lijst van verwerkingen waarvoor het uitvoeren van een GEB verplicht is, op geen enkele manier afbreuk doet aan de algemene verplichting van de verwerkingsverantwoordelijke om aan behoorlijke risicobeoordeling en risicobeheersing te doen. De uitvoering van een GEB stelt de verwerkingsverantwoordelijke ook geenszins vrij van de verplichting tot het naleven van de overige verplichtingen van de AVG of van andere verplichtingen, opgelegd door sector-specifieke of algemene wetgeving. Bovendien is de onderstaande lijst geenszins exhaustief: het uitvoeren van een GEB is steeds vereist van zodra de aan toepassingsvoorwaarden bepaald bij artikel 35(1) van de AVG voldaan is.[157] Overigens vestigt de Autoriteit de aandacht op de *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen (GEB) en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679*door de werkgroep artikel 29 goedgekeurd op 4 april 2017 en laatst gewijzigd en goedgekeurd op 4 oktober 2017, die een essentieel element vormen van de lijst die opgesteld werd door de Autoriteit aangezien deze richtsnoeren een gemeenschappelijke basis bieden die toelaat de coherentie in de schoot van de Unie te verzekeren

[155] De Autoriteit heeft de lijst aangepast zoals gepubliceerd op 28 februari 2018 om rekening te houden met het advies van het ECGB van 25 september 2018. Het algemeen secretariaat van de GBA heeft vervolgens op 16 januari 2019 een aangepast lijst aangenomen. Na deze lijst te hebben bekengemaakt op de website van de GBA, heeft de GBA haar beslissing van 16 januari 2019 laten publiceren in het Belgisch Staatsblad van 22 maart 2019. Deze lijst zal in werking treden op 1 april 2019.

[156] Artikel 35(6) van de AVG.

[157] De loutere omstandigheid dat een voorgenomen gegevensverwerking niet overeenstemt met een van soorten verwerking die voorkomen in de lijst (bijvoorbeeld omdat een van de eigenschappen niet aanwezig is) betekent dan ook niet dat de verwerking vrijgesteld zou zijn van de verplichting tot het uitvoeren van een GEB overeenkomstig artikel 35(1) van de AVG.

waarbij elke nationale lijst deze richtsnoeren verder aanvult en verduidelijkt. Tot slot vestigt de Commissie er nog de aandacht op dat deze lijsten evolutief zijn en aangepast kunnen worden wanneer blijkt dat zij hun beoogde doel niet bereiken.

Naast de gevallen voorzien bij artikel 35(3) van de AVG, en rekening houdende met de uitzondering voorzien bij artikel 35(10), zal de uitvoering van een GEB steeds verplicht zijn:

1. wanneer de verwerking gebruik maakt van biometrische gegevens met het oog op de unieke identificatie van betrokkenen[158] die zich in een openbare ruimte bevinden of in privéruimten die toegankelijk zijn voor het publiek;
2. wanneer persoonsgegevens ingezameld worden bij derden om vervolgens in aanmerking te worden genomen bij de beslissing om een welbepaalde dienstverleningsovereenkomst met een natuurlijke persoon te weigeren of stop te zetten;
3. wanneer gezondheidsgegevens van een betrokkene op geautomatiseerde wijze worden ingezameld aan de hand van een actieve inplantbare medische voorziening[159] ;
4. wanneer er op grote schaal gegevens ingezameld worden bij derden teneinde de economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van natuurlijke personen te analyseren of voorspellen;
5. wanneer er op systematische wijze bijzondere categorieën van persoonsgegevens in de [160]zin van artikel 9 van de AVG of gegevens van zeer persoonlijke aard (zoals gegevens over armoede, werkloosheid, betrokkenheid van jeugdzorg of maatschappelijk werk, gegevens omtrent huishoudelijke en privé-activiteiten, locatiegegevens) systematisch worden uitgewisseld tussen meerdere verwerkingsverantwoordelijken;
6. wanneer er sprake is van een grootschalige verwerking van gegevens die gegeneerd worden door middel van toestellen met sensoren die via het internet of via een ander medium gegevens versturen (‘internet of things’- toepassingen, zoals slimme televisies, slimme huishoudelijke

[158] Artikel 4(14) van de AVG definieert “biometrische gegevens” als persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

[159] Het gaat om elke actieve medische voorziening die is ontworpen om geheel of gedeeltelijk te worden ingeplant in het menselijk lichaam of in een natuurlijke opening en bedoeld is om er te blijven na de interventie.

[160] De bijzondere categorieën gegevens omvatten, overeenkomstig artikel 9 van de AVG, in het bijzonder persoonsgegevens over ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, alsook de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over de gezondheid of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

apparaten, connected toys, smart cities, slimme energiemeters, enz.) en deze verwerking dient om de economische situatie, de gezondheid, de persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van natuurlijke personen te analyseren of te voorspellen;

7. wanneer er sprake is van een grootschalige en/of systematische verwerking van telefonie-, internet- of andere communicatiegegevens, metagegevens of locatiegegevens van of herleidbaar tot natuurlijke personen (bijvoorbeeld wifi-tracking of verwerking van locatiegegevens van reizigers in het openbaar vervoer) wanneer de verwerking niet strikt noodzakelijk is voor een door de betrokkene gevraagde dienst;

8. wanneer er sprake is van grootschalige verwerkingen van persoonsgegevens waarbij op systematische wijze via geautomatiseerde verwerking gedrag[161] van natuurlijke personen geobserveerd, verzameld, vastgelegd of beïnvloed wordt, inclusief voor advertentiedoeleinden.

De verwerkingsverantwoordelijke die een van de hogergenoemde soorten verwerkingen beoogt, is verplicht om een GEB uit te voeren vooraleer hij tot de verwerking overgaat. Dit betekent echter niet noodzakelijk dat er ook een voorafgaande raadpleging dient plaats te vinden. Als het risico afdoende beperkt kan worden aan de hand van passende technische en organisatorische maatregelen, is er geen voorafgaande raadpleging vereist.

[161] Bijv. kijk-, luister-, surf-, klik-, fysiek-, of aankoopgedrag.

11. Bijlage 3: Ontwerp lijst van het soort verwerking waarvoor geen GEB verplicht is (art. 35(5) AVG).

Artikel 35(5) AVG laat aan de toezichthoudende autoriteit toe om een lijst op te stellen van het soort verwerkingen waarvoor een GEB niet vereist is.

De Commissie wenst te benadrukken dat onderstaande lijst geen enkele afbreuk doet aan de algemene verplichting van de verwerkingsverantwoordelijke om aan behoorlijke risicobeoordeling en risicobeheersing te doen overeenkomstig artikel 24(1) AVG.[162] Deze algemene verplichting tot risicobeoordeling en risicobeheersing geldt onverminderd het bestaan van een lijst van bijzondere verwerkingen waarvoor het uitvoeren van een GEB als dusdanig niet verplicht is. Tot slot vestigt de Commissie er nog de aandacht op dat deze lijsten evolutief zijn en aangepast kunnen worden wanneer blijkt dat zij hun beoogde doel niet bereiken.

Voor de volgende soorten verwerking is de uitvoering van een GEB niet vereist:

1. verwerkingen door private entiteiten die noodzakelijk zijn om te voldoen aan een *wettelijke verplichting* die op hen rusten, mits bij wet bepaald werd welke de doeleinden van de verwerking zijn, welke categorieën van persoonsgegevens verwerkt worden en wat de waarborgen zijn ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;
2. verwerkingen van persoonsgegevens die uitsluitend betrekking hebben op gegevens welke noodzakelijk zijn voor de *loonadministratie* van personen in dienst van of werkzaam ten behoeve van de verantwoordelijke voor de verwerking wanneer de gegevens uitsluitend worden gebruikt voor die loonadministratie, alleen worden meegedeeld aan de ontvangers die daartoe gerechtigd zijn en niet langer worden bewaard dan nodig voor de doeleinden van de verwerking;
3. verwerkingen van persoonsgegevens die uitsluitend betrekking hebben op de *administratie van het personeel* in dienst van of werkzaam ten behoeve van de verantwoordelijke voor de verwerking, voor zover deze verwerking geen betrekking heeft op gegevens betreffende de gezondheid van de betrokken persoon, noch op bijzondere categorieën van gegevens in de zin van artikel 9 AVG, noch op strafrechtelijke veroordelingen en strafbare feiten in de zin van artikel 10 AVG of op gegevens die een beoordeling van de betrokken persoon tot doel hebben en de verwerkte persoonsgegevens niet langer worden bewaard dan nodig voor de personeelsadministratie en alleen in het kader van de toepassing van een wets- of verordeningsbepaling of indien nodig voor de verwezenlijking van de doelstellingen van de verwerking aan derden worden meegedeeld;

[162] Zie hoger; nr. 10.

4. verwerkingen van persoonsgegevens die uitsluitend betrekking hebben op de *boekhouding* van de verantwoordelijke voor de verwerking wanneer de gegevens uitsluitend worden gebruikt voor die boekhouding, de verwerking alleen betrekking heeft op personen van wie de gegevens noodzakelijk zijn voor de boekhouding en de persoonsgegevens niet langer worden bewaard dan nodig voor de doeleinden van de verwerking en de verwerkte persoonsgegevens alleen aan derden worden meegedeeld in het kader van de toepassing van een wets- of verordeningsbepaling of wanneer de mededeling noodzakelijk is voor de boekhouding;

5. verwerkingen van persoonsgegevens die uitsluitend betrekking hebben op de *administratie van aandeelhouders en vennoten* wanneer de verwerking alleen betrekking heeft op gegevens nodig voor die administratie, die gegevens alleen personen betreffen van wie de gegevens nodig zijn voor die administratie, de gegevens alleen in het kader van de toepassing van een wets- of verordeningsbepaling aan derden worden meegedeeld en de persoonsgegevens niet langer worden bewaard dan nodig voor de doeleinden van de verwerking;

6. verwerkingen van persoonsgegevens verricht door een *stichting, een vereniging of enig andere instelling zonder winstoogmerk* in het kader van haar gewone activiteiten, voor zover de verwerking uitsluitend betrekking heeft op persoonsgegevens betreffende de eigen leden, betreffende personen met wie de verantwoordelijke voor de verwerking regelmatige contacten onderhoudt en betreffende begunstigers van de stichting, vereniging of instelling en er geen personen worden geregistreerd op grond van gegevens verkregen van derden en de verwerkte persoonsgegevens niet langer worden bewaard dan nodig voor de administratie van de leden, van de contactpersonen en van de begunstigers en alleen in het kader van de toepassing van een wets- of verordeningsbepaling aan derden worden meegedeeld;

7. verwerkingen van persoonsgegevens die uitsluitend betrekking hebben op de *registratie van bezoekers* in het kader van een toegangscontrole wanneer de verwerkte gegevens beperkt blijven tot de naam en het beroepsadres van de bezoeker, de identificatie van zijn werkgever, de identificatie van het voertuig van de bezoeker, de naam, afdeling en functie van de bezochte persoon en het tijdstip van het bezoek en waarbij de verwerkte persoonsgegevens mogen uitsluitend worden gebruikt voor de toegangscontrole en niet langer worden bewaard dan nodig voor dat doel;

8. verwerkingen van persoonsgegevens verricht door *onderwijsinstellingen* met het oog op het beheer van hun relaties met hun leerlingen of studenten in het kader van hun onderwijsopdrachten, voor zover de verwerking alleen betrekking heeft op persoonsgegevens betreffende potentiële, huidige en gewezen leerlingen of studenten van de betrokken onderwijsinstelling en er geen personen worden geregistreerd op grond van gegevens verkregen van derden en alleen in het kader van de toepassing van een wets- of verordeningsbepaling aan derden worden meegedeeld en niet langer worden bewaard dan nodig voor het beheer van de relatie met de leerling of student;

9. verwerkingen van persoonsgegevens die uitsluitend betrekking hebben op het *beheer van de klanten of leveranciers* van de verantwoordelijke voor de verwerking, voor zover de verwerking alleen betrekking heeft op bestaande en gewezen klanten of leveranciers van de verantwoordelijke voor de verwerking en de verwerking geen betrekking heeft op bijzondere categorieën van gegevens in de zin van artikel 9 AVG, noch op strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10 AVG en er, wat de klantenadministratie betreft, geen gegevens afkomstig van derden worden geregistreerd en de verwerkte persoonsgegevens niet langer worden bewaard dan nodig voor de normale bedrijfsvoering van de verantwoordelijke voor de verwerking en mogen alleen in het kader van de toepassing van een wets- of verordeningsbepaling of voor de normale bedrijfsvoering aan derden worden meegedeeld.