Ontwerp van aanbeveling uit eigen beweging met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging voorgelegd voor publieke bevraging (CO-AR-2016-004)

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming ("AVG") van toepassing. De AVG bevestigt reeds bestaande gegevensbeschermingsprincipes, maar voorziet ook in een aantal nieuwe rechten en verplichtingen. Al enige tijd ontvangt de Commissie voor de Bescherming van de Persoonlijke Levenssfeer steeds meer vragen over juiste draagwijdte van deze nieuwe rechten en verplichtingen.

Één van de nieuwe verplichtingen in de AVG betreft de verplichting tot het uitvoeren – in bepaalde omstandigheden – van een "gegevensbeschermingseffectbeoordeling", kortweg "GEB". Een GEB is een proces dat ertoe strekt om risico's te evalueren in verband met de rechten en vrijheden van natuurlijke personen, die ontstaan of dreigen te ontstaan naar aanleiding van de verwerking van persoonsgegevens, evenals om de mogelijkheden tot beheersing van deze risico's te evalueren. De nieuwe verplichting tot het uitvoeren van GEB roept meteen een aantal praktische vragen op, zoals: wanneer is het uitvoeren van een GEB verplicht? Wat zijn de vereiste elementen van GEB? Welke actoren dienen bij een GEB betrokken te worden?

Vooraleer een aanbeveling uit eigen beweging uit te brengen over dit thema, wenst de Commissie advies en suggesties in winnen van de diverse betrokken actoren: verwerkingsverantwoordelijken, verwerkers en betrokkenen. Bovendien verwacht de Commissie dat de Groep 29[1] en ENISA[2] op relatief korte termijn bijkomende richtlijnen zullen uitvaardigen over de methode voor het verrichten van een GEB onder de AVG. Waar de Commissie dit opportuun acht, zullen deze bijkomende richtlijnen in de finale versie van de aanbeveling worden opgenomen.

Deze raadpleging, bekend gemaakt op 20 december 2016, wordt afgesloten op 28 februari 2017. Daarna zal de Commissie alle opmerkingen in overweging nemen bij uitwerking van haar aanbeveling uit eigen beweging.

Alle adviezen, opmerkingen of andere voorstellen worden gericht aan de Privacycommissie per post (Drukpersstraat 35, 1000 Brussel) of per mail (commission@privacycommission.be).

[1] Zie de prioriteiten afgebakend door de Groep 29 in haar de verklaring van 2 februari 2016, gepubliceerd op http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf

[2] Zie de aankondiging van ENISA van januari 2016 m.b.t (onder meer) het aspect van risicobeoordeling van de GDPR op dit vlak https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa2019s-position-on-the-general-data-protection-regulation-gdpr/

Ontwerp van aanbeveling nr [nummer]/[jaartal]
van [datum]

Betreft: Ontwerp van aanbeveling uit eigen beweging met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging (CO-AR-2016-004)

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 artikelen 35 en 36 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)*;

Gelet op het verslag van Willem Debeuckelaere;

Brengt op [datum] de volgende aanbeveling uit:

Inhoudstafel:

1. Inleiding

1. Op 24 mei 2016 is de Algemene Verordening Gegevensbescherming ("AVG")[3] in werking getreden. De AVG zal van toepassing zijn vanaf 25 mei 2018.[4]

2. De AVG voorziet in een aantal nieuwe verplichtingen voor de verwerkingsverantwoordelijke[5], waaronder de verplichting om, in bepaalde gevallen, over te gaan tot een gegevensbeschermingseffectbeoordeling ("GEB"). Een GEB is een proces dat ertoe strekt om risico's te evalueren in verband met de rechten en vrijheden van natuurlijke personen, die ontstaan of dreigen te ontstaan naar aanleiding van de verwerking van persoonsgegevens, evenals om de mogelijkheden tot beheersing van deze risico's te evalueren.[6]

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

(1) de essentiële onderdelen van een GEB (punt 3);
(2) de omstandigheden wanneer een GEB verplicht is (punt 4);
(3) de omstandigheden waarin een voorafgaande raadpleging verplicht is (punt 5);
(4) de actoren die bij een GEB betrokken dienen te zijn (punt 6); en
(5) een aantal bijzondere bepalingen (punt 7).

4. Vooraleer op voormelde aspecten in te gaan, is het nuttig om eerst de juridische context van de verplichting tot het uitvoeren van een GEB schetsen, teneinde een goed begrip van de *ratio legis* te bevorderen.

2. Juridische context: de verantwoordingsplicht en de risico-gebaseerde aanpak

5. De verplichting tot het uitvoeren 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.

---

[3] Verordening (EU) 2016/79 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), O.J. 4 mei 2016, L 119/1.

[4] Artikel 99(2) AVG.

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

[6] Het begrip "gegevensbeschermingseffectbeoordeling" wordt niet als dusdanig gedefinieerd in de AVG, maar wordt in overweging (84) 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.*"

6. 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.

7. Het beginsel van de verantwoordingsplicht van de verwerkingsverantwoordelijke gaat gepaard met een risico-gebaseerde aanpak (zgn. "***risk-based approach***")[8]. Artikel 24(1) AVG bepaalt dat de verwerkingsverantwoordelijke "*passende technische en organisatorische maatregelen*" moet nemen *om te waarborgen (…) dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd*, "*[r]ekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende* ***risico's*** *voor de rechten en vrijheden van natuurlijke personen*".

8. De risico-gebaseerde aanpak van de AVG heeft als doel om een "**schaalbare en proportionele aanpak**"[9] te bevorderen, zonder daarmee om de gegevensbeschermingsbeginselen of de rechten van de betrokkenen op de helling te plaatsen.[10] Dit betekent dat men voor verwerkingen met een hoog risico meer beschermingsmaatregelen zal dienen te nemen dan bij verwerkingen met een laag risico.

9. De verplichting tot het uitvoeren van een GEB is ontwikkeld tegen de achtergrond van richtlijn 95/46, 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 de persoonsgegevens te verbeteren.[11] Het nieuwe systeem legt daarom het accent op de verplichting van de verwerkingsverantwoordelijke om een voorafgaande GEB uit te voeren voor verwerkingen die een "waarschijnlijk hoog risico" met zich meebrengen en op de maatregelen die kunnen worden genomen om deze risico's te verminderen.

---

[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] In het Engels: "*a scalable and proportionate approach to compliance*". (Ibid, p. 2).

[10] 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.)

[11] Overweging (89) AVG.

3. Essentiële onderdelen van een GEB zoals vereist door artikel 35 AVG

A) Overzicht

10. 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) Inventaris van de beoogde verwerkingen en de verwerkingsdoeleinden

11. Artikel 35(7) AVG vereist in eerste instantie dat de GEB een *systematische* beschrijving van de beoogde verwerkingen en verwerkingsdoeleinden omvat. Het is daarbij belangrijk dat zowel de verwerkingen als de beoogde doeleinden op een volledige, consistente en duidelijke wijze worden omschreven. Bij de omschrijving van verwerkingen verwacht de Commissie dat de verwerkingsverantwoordelijke rekening houdt met de verplichting tot het bijhouden van een register van verwerkingsactiviteiten vervat artikel 30 AVG. Naast een omschrijving van de verwerkingsdoeleinden, voorziet deze bepaling ook dat de verwerkingsverantwoordelijke o.m. volgende informatie bijhoudt:

- *een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;*
- *de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;*
- *indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen; en*

- *indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist.*

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") dient vermeden te worden.[12] 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.

C) Proportionaliteitstoets

12. Een GEB moet de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden beoordelen. De verwerkingsverantwoordelijke moet dan ook uitdrukkelijk aangeven (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. Indien verschillende verwerkingen of verwerkingsmiddelen aangewend zouden kunnen worden om de beoogde doeleinde(n) te bereiken, dan verwacht de Commissie dat de verwerkingsverantwoordelijke uitdrukkelijk aangeeft waarom de gekozen verwerkingsmiddelen minder ingrijpend zijn dan de alternatieven.

13. 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?). Tot slot dient de verwerkingsverantwoordelijke er ook over te waken dat een passend evenwicht tussen de relevante belangen behouden blijft.[13]

D) Risicobeoordeling

- *Het begrip "risico"*

14. Het begrip "risico" kan op verschillende wijzen worden geïnterpreteerd. In de literatuur omschrijft men het begrip "risico" doorgaans als de **kans** ("waarschijnlijkheid") dat een bepaalde bedreiging zich voordoet, met een welbepaalde **impact** ("ernst") tot gevolg.[14]

---

[12] Zie ook Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", 2 april 2013, p. 15-16.

[13] 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 (cf. *infra*; nrs. 25-26).

[14] Zie bijv. I. Naumann (ed.), "Privacy and Security Risks when Authenticating on the Internet with European eID Cards", ENISA, 26 november 2009. Zie ook ISO, "Risk management – Vocabulary", ISO Guide 73:2009 ("*un risque est souvent exprimé en*

- *Het begrip "risicobeoordeling"*

15. Het begrip "risicobeoordeling" verwijst naar het geheel van procedures dat er toe strekt om risico's te (1) identificeren, (2) analyseren en (3) beoordelen.[15] **Identificatie** van risico's verwijst naar het proces dat ertoe strekt om risico's te onderzoeken, erkennen en beschrijven.[16] 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.[17] 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.[18]

16. 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. 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).[19]

- *Om welke risico's gaat het?*

17. Artikel 35(1) AVG verwijst naar een bijzonder categorie van risico's, m.n. de *risico's voor de rechten en vrijheden van natuurlijke personen.* Volgens de Groep 29 hebben de woorden "*voor de rechten en vrijheden van natuurlijke personen*" in de GDPR[20] voornamelijk betrekking op het recht op privacy, maar zij kunnen ook betrekking hebben op andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, vrijheid van gedachte, geweten en godsdienst, het verbod op discriminatie en het recht op vrijheid van beweging.[21]

---

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*").

[15] 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*").

[16] *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.*)

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

[18] *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*")

[19] Zie ook ISO, "Risk management – Vocabulary", ISO Guide 73:2009, die "risque résiduel" omschrijft als "*risque subsistant après le traitement du risque*") (vrij vertaling : "*risico dat overblijft na de behandeling van het risico*").

[20] Zie de overwegingen (74) tot en met (77) AVG.

[21] Article 29 Data Protection Working Party, "Statement on the role of a risk-based approach in data protection legal frameworks", WP218, 30 mei 2014, p. 4.

18. Verschillende gegevensverwerkingen kunnen verschillende (inherente) risico's inhouden voor de rechten en vrijheden van natuurlijke personen. Overweging (75) van de AVG lijst, bij wijze van voorbeeld, een aantal omstandigheden op waarin de verwerking aanleiding geven tot risico's voor de rechten en vrijheden van natuurlijke personen, m.n.:

- *waar de verwerking kan leiden tot discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, ongeoorloofde ongedaanmaking van pseudonimisering, of enig ander aanzienlijk economisch of maatschappelijk nadeel;*
- *wanneer de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen;*
- *wanneer persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, en bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen;*
- *wanneer persoonlijke aspecten worden geëvalueerd, om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken;*
- *wanneer persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt; of*
- *wanneer de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen*.

- *Nood aan een contextuele analyse*

19. De Commissie onderstreept dat een risicobeoordeling steeds dient plaats te vinden in functie van het geheel van bijzondere omstandigheden van elke verwerking (of groep van vergelijkbare verwerkingen[22]). 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*."

[22] Overeenkomstig artikel 35(1) AVG kan één GEB een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden (zie verder *infra*; nr. 33).

Het is dus in functie van het geheel van bijzondere omstandigheden van elke verwerking dat de verwerkingsverantwoordelijke de risico's voor het privéleven en voor de rechten en vrijheden van personen moet inschatten en de passende maatregelen moet nemen om de toepassing van de bepalingen van de verordening te waarborgen.

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

20. In de regel beslist de verwerkingsverantwoordelijke vrij over de methodologie die hij wenst te hanteren, op voorwaarde dat deze beantwoordt aan een aantal minimumkenmerken van betrouwbaarheid en objectiviteit[23] , en rekening houdt met de minimale elementen die de AVG voorschrijft. Het is aan de verwerkingsverantwoordelijke om een methodologie te hanteren die hem in staat stelt om de vereisten van de AVG na te leven.

21. De Commissie acht het bovendien belangrijk dat iedere verwerkingsverantwoordelijke die een GEB onderneemt, een methodologie hanteert die aangepast is aan de noden en context van haar eigen onderneming.

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

23. Bovendien raadt de Commissie ten stelligste aan dat de verwerkingsverantwoordelijke zich baseert op reeds bestaande methodologieën inzake risicobeheer. Het gebruik van internationale standaarden, zoals deze ontwikkeld door de Internationale Organisatie voor Standaarden (ISO)[24], alsook gedragscodes ontwikkeld of erkend op Europees niveau, is hierbij van bijzonder belang.[25]

24. Ongeacht welke methodologie uiteindelijk door de verwerkingsverantwoordelijke weerhouden wordt, acht de Commissie het onontbeerlijk dat de verwerkingsverantwoordelijke uitdrukkelijk aangeeft welke methodologie gekozen werd en dat deze op een consistente wijze wordt toegepast doorheen heel het proces van de GEB.

---

[23] 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.*"

[24] In het bijzonder ISO 31000 (Risk management) en ISO 27005 (Information security risk management).

[25] Zie ook ENISA, "ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31, 2010", July 2010, p. 6, raadpleegbaar via https://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia. Wat betreft gedragscodes erkend of ontwikkeld op Europees niveau zie ook infra; nr. 60 e.v.

E) Beoogde maatregelen

25. Een GEB omvat niet enkel een beoordeling van risico's, maar bevat tevens 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. Pas nadat de beoogde beschermingsmaatregelen in rekening worden gebracht, is men in staat om het residuele risico van de voorgenomen verwerking in te schatten.

26. 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.[26]

4. Omstandigheden waarin het uitvoeren van een GEB verplicht is

27. De AVG vereist niet dat de verwerkingsverantwoordelijke een GEB uitvoert voor iedere verwerking van persoonsgegevens. In de 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.[27] 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 bieden artikel 35(4) en artikel 35(5) AVG aan nationale toezichthouders de mogelijkheid om lijsten op te stellen van het soort verwerkingen waarvoor een GEB wel of niet vereist is.

A) Een "waarschijnlijk hoog risico" voor de rechten en vrijheden van natuurlijke personen

28. Artikel 35(1) AVG bepaalt dat :

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

29. Het begrip "waarschijnlijk hoog risico" wordt door de AVG niet nader omschreven. De Commissie is zich er van bewust dat verschillende organisaties verschillende schalen en methodologieën hanteren

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

[27] Artikel 35(1) AVG.

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 methodologie. Het begrip "waarschijnlijk hoog risico" in de zin van AVG stemt echter niet noodzakelijk overeen met het begrip "waarschijnlijk hoog risico" zoals men dat terugvindt in andere risico-beheersingsmodellen.

30. De Commissie meent dat het begrip "waarschijnlijk hoog risico" in eerste instantie verwijst naar de gegevensverwerkingen waarvan het *aannemelijk* is dat zij *aanzienlijke nadelige gevolgen* kunnen hebben voor de fundamentele rechten en vrijheden van natuurlijke personen indien men niet voorziet in passende beschermingsmaatregelen. Een "aanzienlijk 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. Dit is bijvoorbeeld het geval wanneer het aannemelijk is dat de verwerking aanleiding kan geven tot de nadelige gevolgen die worden opgesomd in overweging (75) AVG.[28]

31. In tegenstelling tot artikel 36 AVG, heeft het "waarschijnlijk hoog risico" dat aanleiding geeft tot de verplichting tot het uitvoeren van een GEB betrekking op het "inherente" risico van de voorgenomen gegevensverwerking. Het "residuele risico" speelt pas bij de toepassing van de verplichting om over te gaan tot voorafgaande raadpleging van de toezichthoudende autoriteit (cf. *infra*; nr. 40 e.v.).[29]

B) <u>Situaties omschreven in artikel 35(3) AVG</u>

32. 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*.[30]

In die gevallen zal in de regel steeds een voorafgaande GEB uitgevoerd moeten worden. Overweging (91) van de AVG preciseert dat de verplichting tot het uitvoeren van een voorafgaande

[28] Zie supra; nr. 18.

[29] Wat betreft het onderscheid tussen "inherente" en "residuele" risico's zie supra; nr. 16.

[30] Voor de invulling van de begrippen "systematisch", "stelselmatig" en "grootschalig" verwijst de Commissie naar de richtsnoeren van de Groep 29 met betrekking tot de functionaris voor gegevensbescherming (Article 29 Data Protection Working Party, "Guidelines on Data Protection Officers", WP 243, 13 december 2016, p. 7-8). 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.

effectbeoordeling niet van toepassing is als het gaat om de verwerking van persoonsgegevens van patiënten of cliënten door een arts, een andere zorgprofessional of door een advocaat. In die gevallen mag de verwerking niet als een grootschalige verwerking worden beschouwd.

33. Onder bepaalde omstandigheden kan het redelijk en nuttig kan 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.[31] 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. 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, …) wanneer ieder van deze verwerkingsverantwoordelijken een reeks vergelijkbare verwerkingen beogen die vergelijkbare hoge risico's inhouden.

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

34. 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.

35. 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.

36. De Commissie wenst te benadrukken dat voormelde lijsten geen enkele afbreuk doen aan de algemene verplichting van verwerkingsverantwoordelijke om, overeenkomstig artikel 24(1) AVG, steeds te voorzien in passende technische en organisatorische maatregelen om te waarborgen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd, rekening houdend met o.a. de risico’s voor de rechten en vrijheden van natuurlijke personen. Deze algemene verplichting tot risicobeoordeling en risicobeheersing geldt onverminderd het bestaan van een lijst van bijzondere

[31] Overweging (92) AVG.

verwerkingen waarvoor het uitvoeren van een GEB verplicht is (of het bestaan van een lijst van verwerkingen waarvoor het uitvoeren GEB niet verplicht is).

37. Bovendien zijn de lijsten geenszins exhaustief: het uitvoeren van een GEB is steeds vereist van zodra de toepassingsvoorwaarden bepaald bij artikel 35 AVG voldaan zijn.

38. 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.

39. 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.

5. Omstandigheden waarin voorafgaande raadpleging verplicht is

40. 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."*

41. Uit de bewoording van artikel 36(1) AVG blijkt duidelijk dat een voorafgaande raadpleging slechts verplicht is wanneer het residuele risico hoog is. Enkel wanneer blijkt dat de voorgenomen verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen doeltreffende risico-beperkende maatregelen zou nemen, dient de verwerking voorafgaandelijk te worden voorgelegd aan de toezichthoudende autoriteit. Indien het risico afdoende beperkt kan worden aan de hand van passende technische en organisatorische maatregelen, dient er géén voorafgaande raadpleging plaats te vinden.[32]

42. Indien de toezichthoudende autoriteit van mening is dat de beoogde verwerking niet conform de verordening 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 bedoelde bevoegdheden uitoefenen. Die termijn van 8 weken kan met zes bijkomende

[32] De Commissie benadrukt dat het begrip "organisatorische" maatregelen niet enkel verwijst naar de communicatie en hiërarchie binnen een onderneming. Procedures en richtlijnen voor personeel zijn in dit verband ook essentieel.

weken worden verlengd.[33] 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).

43. 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 deze verordening;

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

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

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

6. De betrokken actoren

A) <u>De verwerkingsverantwoordelijke</u>

44. 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 de uitvoering van een GEB overeenkomstig artikel 35 AVG verplicht is.

45.De Commissie acht het onontbeerlijk dat de verwerkingsverantwoordelijke ervoor zorgt dat de juiste personen binnen de onderneming betrokken worden bij het risico-beoordelingsproces. 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 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, zij die strategische

[33] 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.

beslissingen inzake projectontwikkeling nemen en de personeelsleden (of hun vertegenwoordigers) die gebruik zullen maken van de persoonsgegevens in kwestie bij de uitoefening van hun taken.

46. Bovendien raadt de Commissie ook aan dat het hoogste orgaan binnen de organisatie van de verwerkingsverantwoordelijke afdoende betrokken wordt bij het risico-beoordelingsproces. De risicobeoordeling (met of zonder GEB), 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 kunnen worden voorgelegd.

B) De verwerker

47. 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*".[34]

48. Overweging (95) bevestigt verder 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.

49. In het licht van voormelde bepalingen zal de toezichthoudende autoriteit bij de beoordeling van de bijstandsplicht van de verwerker rekening houden met (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

50. De Commissie acht het vanzelfsprekend dat de functionaris voor gegevensbescherming, wanneer die is aangeduid, de verwerkingsverantwoordelijke bijstaat en adviseert bij het uitvoeren een GEB. Artikel 35(2) AVG bevestigt uitdrukkelijk dat wanneer een functionaris voor gegevensbescherming is

[34] Artikel 28(3)f AVG.

aangewezen, de verwerkingsverantwoordelijke bij het uitvoeren van een GEB diens advies zal inwinnen.

51. 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. De Commissie acht het dan ook onwenselijk dat de functionaris voor gegevensbescherming geheel op eigen houtje, zonder inbreng van de relevante actoren, een GEB opstelt.

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

52. 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.*".

53. De Commissie merkt op dat het afzonderlijk lezen van de Engelstalige, Franstalige en Nederlandstalige versies van artikel 35(9) 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*".

54.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. Zijn beslissing is evenwel onderhevig is aan een marginale controle vanwege de toezichthoudende autoriteit, gelet op diens algemene handhavingsbevoegdheid. Het is voor de verwerkingsverantwoordelijke met andere woorden dus niet geheel vrijblijvend of de betrokkenen of hun vertegenwoordigers worden geraadpleegd. 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 acht de Commissie het nodig dat dergelijke raadpleging ook daadwerkelijk plaatsvindt.

E) <u>De toezichthoudende autoriteit</u>

55. 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.

56. 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.

57. De Commissie is van mening dat de toelichting vervat in deze aanbeveling, alsook de richtsnoeren uitgevaardigd op Europees niveau (in het bijzonder door de Artikel 29 Werkgroep en ENISA), samen met de relevante internationale standaarden, in zeer hoge mate houvast bieden aan de verwerkingsverantwoordelijke om op een correcte manier aan risicobeheersing te doen.

7. Bijzondere bepalingen

A) <u>Verwerking op grond van een wettelijke verplichting of algemeen belang</u>

58. 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.[35]

[35] Overweging (93) 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.*"

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.[36]

59. 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.[37] 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.

B) <u>Gedragscodes</u>

60. 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.*"

61. 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.[38]

---

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

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

[38] Artikel 40(9) AVG.

C) Nazicht

62. De verwerkingsverantwoordelijke is gehouden om, waar nodig, na te gaan 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.[39]

63. Gelet op de vaststelling dat risico's doorgaans evolueren met de tijd, acht de Commissie het opportuun dat de verwerkingsverantwoordelijke zelf een periodiek nazicht van de uitgevoerde GEB inbouwt. In het kader van een goed risicobeheer verwacht de Commissie dat de verwerkingsverantwoordelijke minstens om de 2 jaar een nazicht inbouwt. De Commissie raadt ook aan dat de uitkomst van het nazicht formeel ter goedkeuring van de directie- of kaderleden van de organisatie van de verwerkingsverantwoordelijke wordt voorgelegd.[40]

64.Tot slot wijst de Commissie er op dat er ook andere omstandigheden zijn die aanleiding kunnen geven tot het herzien van een eerder uitgevoerde GEB, 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.[41]

De Wnd. Administrateur, De Voorzitter,

An Machtens Willem Debeuckelaere

[39] Artikel 35 (11) AVG.

[40] Zie ook supra; nr. 46.

[41] 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.

8. Bijlage 1 : Minimale kenmerken van een behoorlijk risicobeheer

In de regel beslist de verwerkingsverantwoordelijke vrij over de procedure en methodologie die 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.[42]

Om te vermijden dat er een situatie van rechtsonzekerheid zou ontstaan bij gebrek aan objectieve elementen waaraan de kwaliteit van een bepaalde methodologie getoetst kan worden, formuleert de Commissie hieronder een aantal **minimale kenmerken**. Deze elementen zijn niet nieuw, maar reeds elders gedocumenteerd.[43] 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 methodologieën inzake risicobeheer. Internationale standaarden, zoals deze ontwikkeld door de Internationale Organisatie voor Standaarden (ISO)[44], alsook gedragscodes ontwikkeld of erkend op Europees niveau, zijn hierbij van bijzonder belang.[45]

De verwerkingsverantwoordelijke dient uitdrukkelijk aan te geven welke methodologie gekozen werd en dient erover te waken dat deze op een consistente wijze wordt toegepast doorheen heel het proces van de GEB.

2. Gestructureerd

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

---

[42] Overweging (76) 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: "*De waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkene moeten worden bepaald onder verwijzing naar de aard, het toepassingsgebied, de context en de doeleinden van de verwerking. 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.*"

[43] Zie ISACA, "Privacy Audit - Methodology and Related Considerations, *Isaca Journal* 2014, Volume 1, raadpleegbaar op http://www.isaca.org/Journal/archives/2014/Volume-1/Documents/Privacy-Audit-Methodology-and-Related-Considerations_joa_Eng_0114.pdf; ENISA, "ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31, 2010", July 2010, p. 6-9, raadpleegbaar via https://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia en OECD, "Digital Security Risk Management for Economic and Social Prosperity", OECD Recommendation and Companion Document, 2015, raadpleegbaar op http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.

[44] In het bijzonder ISO 31000 (Risk management) en ISO 27005 (Information security risk management).

[45] Zie ook ENISA, "ENISA Position on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications of March 31, 2010", July 2010, p. 6.

- definitie van de relevante context (bestaande uit de externe en interne parameters die in rekening gebracht dienen te worden bij de beheersing van risico's);
- definitie van maatstaven om de risico's voor de rechten en vrijheden van natuurlijke personen in te schatten;
- identificatie en analyse van risico's (inclusief de identificatie van kwetsbaarheden, bedreigingen, en de toekenning van een risicowaarde);
- definitie van aanvaardbare risicowaarden (inclusief een bepaling van welke risicowaarden onaanvaardbaar zijn); en
- identificatie van passende risico-beperkende maatregelen (i.e. de technische en organisatorische maatregelen die noodzakelijk zijn om het risico tot een aanvaardbaar niveau te herleiden).

3. Op maat

Een risicobeoordeling is steeds maatwerk. 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.[46]

5. Voldoende genuanceerd

Een risicobeoordeling dient voldoende schalen te bevatten teneinde een genuanceerde evaluatie van geïdentificeerde risico mogelijk te maken[47]. Het voorzien van slechts drie schalen (laag, medium en hoog) om risico's te beoordelen is doorgaans onvoldoende om tot een correcte appreciatie te leiden.

---

[46] 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.

[47] Zie bijvoorbeeld ISACA, privacy Audit-Methodology and Related Considerations, Isaca Journal, Volume 1, 2014, http://www.isaca.org/Journal/archives/2014/Volume-1/Documents/Privacy-Audit-Methodology-and-Related-Considerations_joa_Eng_0114.pdf

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 aan de functionaris voor de gegevensbescherming en/of veiligheidsconsulent, maar ook de ontwikkelaars van nieuwe toepassingen, zij die strategische beslissingen inzake projectontwikkeling nemen en de personeelsleden (of hun vertegenwoordigers) die gebruik zullen maken van de persoonsgegevens in kwestie bij de uitoefening van hun taken.

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. In het kader van een goed risicobeheer verwacht de Commissie dat de verwerkingsverantwoordelijke minstens om de 2 jaar een nazicht inbouwt. 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.

9. Bijlage 2: Lijst van het soort verwerking waarvoor een GEB verplicht is (art. 35(4) AVG)

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).

De Commissie wenst te benadrukken dat het bestaan van een lijst van bijzondere 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. Bovendien is de onderstaande lijst geenszins exhaustief: het uitvoeren van een GEB is steeds vereist van zodra de toepassingsvoorwaarden bepaald bij artikel 35 AVG voldaan zijn. 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(2) 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 biometrie ter identificatie van betrokkenen;
2. wanneer de verwerking gebruik maakt van genetische gegevens;
3. wanneer persoonsgegevens ingezameld worden bij derden om vervolgens in aanmerking te worden genomen bij de beslissing om een dienstverlening te weigeren of stop te zetten;
4. wanneer de verwerking dient om de financiële solvabiliteit van de betrokkene te beoordelen of om enig ander risico-profiel van betrokkene te genereren dat in aanmerking genomen wordt bij dienstverlening aan de betrokkene (of bij de beslissing om een dienstverlening te weigeren of stop te zetten);
5. wanneer de verwerking van die aard is dat een inbreuk op persoonsgegevens de fysieke gezondheid van de betrokkene in het gedrang zou kunnen brengen;
6. wanneer de verwerking financiële of gevoelige persoonsgegevens betreft die (her)gebruikt worden voor (een) doeleinde(n) andere dan degene waarvoor ze werden ingezameld, behoudens wanneer de verwerking hetzij is gebaseerd is op de toestemming van de betrokkene, hetzij noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
7. wanneer de verwerking aanleiding geeft tot een mededeling of ter beschikking stelling aan het publiek van persoonsgegevens die betrekking hebben op een groot aantal betrokkenen;

8. wanneer persoonlijke aspecten worden geëvalueerd, om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen;
9. wanneer er op grote schaal profielen van natuurlijke personen worden opgesteld;
10. ingeval van grootschalige verwerking van persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, voor (een) doeleinde(n) andere dan degene waarvoor ze werden ingezameld;
11. wanneer meerdere verwerkingsverantwoordelijken van plan zijn een gemeenschappelijke applicatie- of verwerkingsomgeving in te voeren voor een hele sector, of een segment daarvan, of voor een gangbare horizontale activiteit en waarbij gebruik gemaakt wordt van gevoelige gegevens;
12. wanneer de verwerking ertoe strekt om de kennis, prestaties, vaardigheden of mentale gezondheidstoestand van leerlingen te registeren en de evolutie ervan op te volgen, met name aan de hand van leerlingvolgsystemen, ongeacht of deze leerlingen zich in het primair, secundair, tertiair of universitair onderwijs bevinden.

10. Bijlage 3: 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. 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 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;

2. 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 gevoelige of gerechtelijke gegevens in de zin van de artikelen 9 en 10 van de 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;

3. 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;

4. 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;

5. 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;

6. 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;

7. 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.