HANDLEIDING GEB[1]

Dit document dient als handleiding om uit te maken of voorafgaand aan de beoogde verwerking al dan niet een gegevensbeschermingseffectbeoordeling (GEB) moet worden uitgevoerd.

Het betreft niet de verwerkingsverantwoordelijken die gehouden zijn tot naleving van de titels 2 en 3 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (gerechtelijke autoriteiten, politiediensten, algemene inspectie van de federale politie en de lokale politie, Cel voor Financiële Informatieverwerking, de algemene administratie der Douane en accijnzen, de Passagiersinformatie-eenheid, de veiligheids- en inlichtingendiensten,…).

Wanneer u tot vaststelling komt dat u een GEB moet uitvoeren voor uw geplande verwerking met hoog risico en u hebt een functionaris voor gegevensbescherming dan kunt u zijn advies vragen en hem bij de uitvoering daarvan betrekken. Dit advies voegt u bij uw interne documentatie over uw verwerking met hoog risico.

Indien uw geplande gegevensverwerking met hoog residueel risico een grensoverschrijdend karakter vertoont, dient u de vragen a tot g en 26 van het formulier te beantwoorden teneinde uit te maken of de Belgische GBA bevoegd is om een advies te verstrekken over uw geplande verwerking.

In deze handleiding komt ook de vraag aan bod wanneer de verwerkingsverantwoordelijken het advies van een Gegevensbeschermingsautoriteit (GBA) moeten vragen aangaande de bedoelde verwerking.

Voor verdere uitleg, kunt u de richtsnoeren raadplegen van de werkgroep "artikel 29" over de bescherming van gegevens (Groep 29) betreffende de GEB en op welke manier wordt bepaald of een verwerking eventueel een verhoogd risico inhoudt als bedoeld in de AVG, goedgekeurd op 4 oktober 2017 (WP 248 rev. 01)[2] alsook de Aanbeveling uit eigen beweging van de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) nr. 01/2018 van 28 februari met betrekking tot de gegevensbeschermingseffectbeoordeling en de voorafgaande raadpleging[3].

[1] Gegevensbeschermingseffectbeoordeling.
[2] Beschikbaar op dit adres: https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/wp248%20rev.01_nl.pdf
[3] Beschikbaar op: https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2018.pdf

1. MOET IK EEN GEGEVENSBESCHERMINGSEFFECTBEOORDELING VERRICHTEN VOORALEER IK START MET MIJN GEGEVENSVERWERKING?

Artikel 35 van de AVG verplicht elke verwerkingsverantwoordelijke die een verwerking wil verrichten die mogelijks een verhoogd risico inhoudt voor de rechten en vrijheden van natuurlijke personen, daarop een gegevensbeschermingseffectbeoordeling uit te voeren.

Deze verplichting heeft dus uitsluitend betrekking op de verwerkingen met hoog risico en alleen als het gaat om nieuwe verwerkingen met deze kenmerken en dit vanaf 25/05/201, of op bestaande verwerkingen die een verandering hebben ondergaan (gewijzigde technologie, inzamelingsmethode van de gegevens, omvang van de verzamelde gegevens of categorieën verzamelde gegevens, ...) die een verhoogd risico inhoudt voor de rechten en vrijheden van de betrokkenen.

Er bestaan lijsten met verwerkingen die een hoog risico inhouden en een lijst met criteria waarmee kan worden bepaald of een verwerking een hoog risico inhoudt.

Het is verplicht om voor de geplande verwerkingen, opgesomd onder artikel 35.3 van de AVG (punt a) hieronder), een GEB uit te voeren vooraleer met de verwerking te starten.

> De lijst met verwerkingen waarvan de GBA meent dat ze een hoog risico inhouden en als bijlage 2 is gevoegd bij haar voormelde Aanbeveling 01/2018, wordt in deze handleiding niet vermeld aangezien deze ontwerplijst nog ter advies dient te worden voorgelegd aan het Europees Comité voor gegevensbescherming alvorens zij door de GBA kan worden goedgekeurd en bindende kracht krijgt.
>
> Omdat de ontwerplijst met verwerkingen zonder hoog risico, als bijlage 3 gevoegd bij de Aanbeveling 01/2018, hetzelfde statuut heeft, wordt ook deze niet vermeld in de handleiding.

Wanneer een geplande verwerking niet voorkomt in de lijst met verwerkingen als bedoeld in artikel 35.3 van de AVG (**punt a)** hierna), moet er toch een voorafgaande GEB worden uitgevoerd als die beantwoordt aan de criteria als uitgevaardigd door de Groep 29 ter bepaling of een verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen **(punt b)** hierna).

a. Lijsten van persoonsgegevensverwerkingen waarvoor een voorafgaande GEB verplicht is.

Wanneer u de hierna volgende persoonsgegevensverwerkingen wil verwezenlijken, moet u daarvan, krachtens artikel 35.3 van de AVG, het effect beoordelen op de rechten en vrijheden van de betrokkenen en dit vooraleer met de verwerking te starten:

- Een systematische en uitgebreide beoordeling van *persoonlijke aspecten van natuurlijke personen*, die gebaseerd is 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;

- *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
- *stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.*[4]

b. Criteria ter bepaling van een hoog risico bij een persoonsgegevensverwerking

De Groep 29 identificeerde **negen criteria** die verwerkingsverantwoordelijken in overweging moeten nemen bij hun analyse of een voorgenomen verwerking al dan niet een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Deze criteria zijn opgenomen in de onderstaande lijst.

Over het algemeen, 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. In de meeste gevallen kan een verwerkingsverantwoordelijke ervan uitgaan dat voor een verwerking die aan **twee criteria** voldoet een gegevensbeschermingseffectbeoordeling moet worden uitgevoerd. In sommige gevallen kan een verwerkingsverantwoordelijke echter oordelen dat een verwerking die aan slechts één van deze criteria voldoet een gegevensbeschermingseffectbeoordeling vereist.[5]

Dit zijn de 9 criteria:

☐ 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[6].

☐ Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg voor de betrokkene[7].

[4] Voor een interpretatie van de in deze opsomming bedoelde verwerkingen, cf.de overwegingen 23 tot 27 van de voormelde Aanbeveling 01/2018.

[5] Voor bijkomende voorbeelden van toepassing van deze criteria, zie Groep 29, Richtsnoeren GEB, p. 13-14, beschikbaar op volgend adres http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[6] Zie ook overwegingen (71), (75) en (91) van de 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.

[7] Voor meer uitleg over deze begrippen wordt verwezen naar de richtsnoeren van de Groep 29 over de geautomatiseerde individuele besluitvorming en de profilering in de zin van de AVG (WP 251.rev01), beschikbaar op volgend adres http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826

☐ Stelselmatige monitoring: dit criterium omvat verwerkingen om betrokkenen te observeren, te monitoren of te controleren, met inbegrip van gegevensinzameling via netwerken en de stelselmatige monitoring van openbaar toegankelijke ruimten. Dit is een criterium dat uitgaat van een vermoedelijke verwerking met hoog risico omdat de persoonsgegevens kunnen worden verzameld onder omstandigheden waarin de betrokkenen niet weten wie hun gegevens verzamelt en hoe die gegevens zullen worden gebruikt. Bovendien kan het voor natuurlijke personen onmogelijk zijn om te voorkomen dat ze aan een dergelijke verwerking in een openbare (of openbaar toegankelijke) ruimte worden onderworpen[8].

☐ Gevoelige gegevens of gegevens van zeer persoonlijke aard: Dit criterium is vervuld voor de bijzondere categorieën persoonsgegevens bedoeld in artikel 9 (gegevens betreffende ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond, alsook de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid) en artikel 10 van de AVG (persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daaraan gekoppelde veiligheidsmaatregelen) bedoeld onder artikel 10. 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 zware gevolgen zou hebben voor het dagelijkse leven van de betrokkene (zoals bijvoorbeeld financiële gegevens die kunnen worden gebruikt voor betalingsfraude)[9].

☐ 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;

[8] Voor voorbeelden van activiteiten die een regelmatig en systematisch observeren van de betrokken kunnen betekenen, wordt verwezen naar punt 2.1.4 van de Richtsnoeren van de Groep 29 over de afgevaardigde voor gegevensbescherming die in verschillende talen beschikbaar zijn op volgend adres http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48137

[9] Dit criterium kan ook betrekking hebben op gegevens zoals persoonlijke documenten, e-mails, dagboeken, notities uit e-readers met notitiefuncties, en zeer persoonlijke informatie opgeslagen 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.

- de geografische omvang van de verwerkingsactiviteit[10].

☐ 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 zouden overschrijden[11].

☐ Gegevens met betrekking tot kwetsbare personen, zoals bijvoorbeeld kinderen, werknemers, geesteszieken, asielzoekers, bejaarden, patiënten en andere meest kwetsbare segmenten van de bevolking die speciale bescherming behoeven.[12] 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.

☐ Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen, zoals het gecombineerd gebruik van herkenningssystemen zoals 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[13].

☐ Wanneer, ingevolgde de verwerking zelf, de betrokkenen geen recht kunnen uitoefenen of genieten van een dienst of een overeenkomst. Dit omvat de verrichtingen met het oog op het toestaan, wijzigen of weigeren van de toegang door de betrokkenen tot een dienst of de mogelijkheid voor deze personen om een contract af te sluiten[14].

Omgekeerd is het mogelijk dat een verwerkingsverantwoordelijke een verwerking, die overeenstemt met sommige van de bovenvermelde criteria, toch niet beschouwt als een verwerking die "waarschijnlijk een hoog risico inhoudt". In dergelijke gevallen dient de verwerkingsverantwoordelijke de redenen te motiveren en te documenteren waarom geen enkele gegevensbeschermingseffectbeoordeling werd uitgevoerd en dient hij deze in documentatie op te nemen/te registreren alsook de adviezen van de

[10] Zie ook overweging (75) en (91) van de AVG. Zie ook Groep 29, Richtlijnen voor functionarissen voor gegevensbescherming, p. 9.
[11] Zie verder ook de toelichting in het WP29-advies inzake doelbinding (WP 203), p. 24.
[12] Zie ook overweging (75) van de AVG.
[13] Of een technologie al dan niet als “nieuw” beschouwd dient te worden dient "conform het bereikte niveau van technologische kennis” ingevuld te worden.
[14] 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.

functionaris voor gegevensbescherming (indien hij over een dergelijke functionaris beschikt) ter zake om deze op eenvoudige vraag ter beschikking te kunnen stellen van de Gegevensbeschermingsautoriteit

c. Vrijstelling van de verplichting tot het uitvoeren van een voorafgaande GEB?

Artikel 35.10 van de AVG stelt sommige verwerkingsverantwoordelijken vrij van de verplichting om een GEB uit te voeren voorafgaand aan sommige gegevensverwerkingen met een hoog risico. Het gaat om de verwerkingen uitgevoerd in toepassing van artikel 6.1.c (verwerkingen die noodzakelijk zijn om een wettelijke verplichting na te leven waaraan de verwerkingsverantwoordelijke onderworpen is) of 6.1.e van de AVG (verwerkingen die nodig zijn om een opdracht te vervullen van algemeen belang die aan de verwerkingsverantwoordelijke werd toevertrouwd.

Evenwel, krachtens artikel 23 van de voormelde wet van 30 juli 2018 heeft de Belgische wetgever gebruik gemaakt van de mogelijkheid die hem geboden wordt door dit artikel 35.10 van de AVG om te besluiten dat niettemin vóór de verwerkingsactiviteit een specifieke gegevensbeschermingseffectbeoordeling door de betrokken verwerkingsverantwoordelijken dient te worden verricht, ook al werd reeds een algemene gegevensbeschermingseffectbeoordeling uitgevoerd in het kader van de vaststelling van de wettelijke grondslag.

2. WANNEER MOET IK HET ADVIES VAN DE GBA INWINNEN OVER DE GEPLANDE VERWERKING?

Niet alle verwerkingen waarvoor een voorafgaande GEB moet worden uitgevoerd dienen voorafgaandelijk voor advies aan de gegevensbeschermingsautoriteit te worden voorgelegd.

Enkel deze die nog een hoog residueel risico vertonen ondanks de door de verwerkingsverantwoordelijke genomen risico-beperkende maatregelen dienen voorafgaandelijk voor advies te worden voorgelegd aan de gegevensbeschermingsautoriteit.

De verplichte voorafgaande raadpleging van de GBA, bepaald in artikel 36 van de AVG is immers enkel van toepassing voor verwerkingen met een hoog risico voor de rechten en vrijheden van de betrokkenen. Een verwerking die een die nog een hoog residueel risico vertoont betekent dat die een hoog risico vertoont ondanks de door de verwerkingsverantwoordelijke genomen maatregelen om dit risico te beperken.

Daarom dient de informatie die moet worden ingevuld op het formulier voor raadpleging van de Gegevensbeschermingsautoriteit of in de bijlagen enkel betrekking te hebben op deze verwerking met hoog residueel risico.

3. TOT WELKE GEGEVENSBESCHERMINGSAUTORITEIT KAN IK MIJ WENDEN INGEVAL VAN GEPLANDE GEGEVENSVERWERKING MET HOOG RESIDUEEL RISICO EN GRENSOVERSCHRIJDEND KARAKTER?

Artikel 4, § 23 van de Algemene Verordening Gegevensbescherming definieert een grensoverschrijdende verwerking als een:

"*verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd;*

of

een verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden".

Indien uw geplande verwerking beantwoordt aan deze definitie en een hoog residueel risico inhoudt, dient u zich te wenden tot de leidende gegevensbeschermingsautoriteit om hierover een voorafgaand advies te verkrijgen.

Teneinde te kunnen uitmaken wie in uw situatie deze leidende autoriteit is, dient u de vragen a tot g alsook vraag 26 van het formulier voor aanvraag van het advies GEB in te vullen.

Weet dat indien de Belgische gegevensbeschermingsautoriteit op basis van de door u meegedeelde informatie besluit dat zij de leidende autoriteit is voor de bedoelde verwerking, deze aanwijzing evenwel niet mag worden beschouwd als definitief of vaststaand. Deze beslissing kan immers desgevallend later worden ongedaan gemaakt door het Europees Comité voor gegevensbescherming, onder meer ingevolge bezwaren die eventueel kunnen worden geformuleerd door andere gegevensbeschermingsautoriteiten over haar aanwijzing als leidende autoriteit.

Indien dit het geval is zou uw aanvraagformulier voor het bekomen van een advies over uw verwerking met hoog residueel risico, kunnen worden meegedeeld aan andere bevoegde Europese gegevensbeschermingsautoriteiten.

****