Bijlage II GEGEVENSBESCHERMINGS-EFFECTBEOORDELINGEN

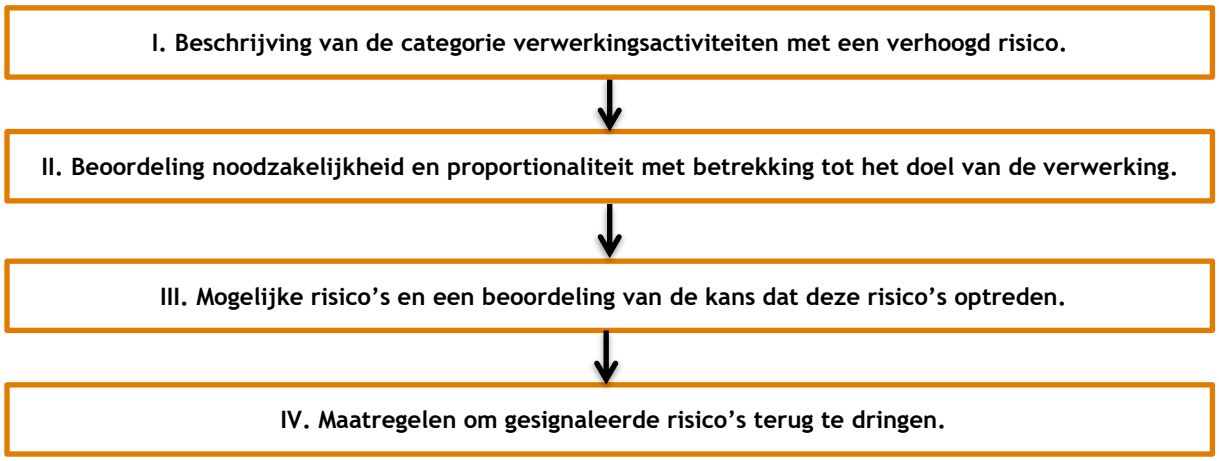
Calvijn College

Uitgevoerd door: […]
Datum: […]
[Gevalideerd door: …]

1. Inleiding

Dit rapport voorziet conform artikel 3.5 van het Privacyreglement en artikel 35 van de AVG in een gegevensbeschermingseffectbeoordeling (GEB of DPIA) van die verwerkingsactiviteiten die het bevoegd gezag van de Stichting kwalificeert als verwerking met een waarschijnlijk verhoogd risico voor de rechten en vrijheden van betrokkenen.

In het rapport komt achtereenvolgens en gecategoriseerd op gelijksoortige verwerkingen met vergelijkbare risico's, het volgende aan de orde:



2. Effectbeoordelingen

Verwerkingsactiviteit:	
I. Beschrijving	
II. Noodzakelijkheid/ proportionaliteit	
III. Risico's	
IV. Maatregelen	
Advies FG	

Verwerkingsactiviteit:	
I. Beschrijving	
II. Noodzakelijkheid/ proportionaliteit	
III. Risico's	
IV. Maatregelen	
Advies FG	

Verwerkingsactiviteit:	
I. Beschrijving	
II. Noodzakelijkheid/ proportionaliteit	
III. Risico's	
IV. Maatregelen	
Advies FG	

3. Evaluatie

Het bevoegd gezag toetst de verwerkingsactiviteiten van persoonsgegevens binnen haar Stichting periodiek op nakoming van de uitkomsten van de gegevensbeschermingseffectbeoordelingen. Deze toetsing vindt ook plaats wanneer risico's veranderen, bijvoorbeeld wanneer wordt overgestapt naar een andere digitale applicatie- of verwerkingsomgeving en/of aanbieder. Van deze evaluatie wordt een schriftelijk verslag opgesteld en als bijlage bij deze rapportage gevoegd.

Wanneer de Stichting besluit meer en/of andere persoonsgegevens te verzamelen, andere verwerkingen toepast (denk aan profilering met gegevens die reeds worden verzameld) of uit het register van verwerkingsactiviteiten blijkt dat de doelen voor gegevensververwerkingen zijn gewijzigd, voert zij vóór deze verwerking – indien ingevolge artikel 35 AVG noodzakelijk - een beoordeling uit conform het in paragraaf 2 aangehouden model.

Bijlage 1 Evaluatieverslagen

Periodieke evaluatie van verwerkingsactiviteit: [vul in] **Datum:** [vul in] **Door:** [vul in]	
Stand van zaken	
Bevindingen	
Risico's	
Conclusie en maatregelen	

Periodieke evaluatie van verwerkingsactiviteit: [vul in] **Datum:** [vul in] **Door:** [vul in]	
Stand van zaken	
Bevindingen	
Risico's	
Conclusie en maatregelen	

Periodieke evaluatie van verwerkingsactiviteit: [vul in] **Datum:** [vul in] **Door:** [vul in]	
Stand van zaken	
Bevindingen	
Risico's	
Conclusie en maatregelen	

Toelichting

Per 25 mei 2018 is de verwerkingsverantwoordelijke (in dit verband: het bevoegd gezag) verplicht om vooraf na te denken over privacy-risico's van bepaalde gegevensverwerkingen en deze risico's zoveel mogelijk te beperken door in een vroeg stadium na te denken over eventueel te nemen maatregelen. Deze verplichting geldt met name wanneer gebruik wordt gemaakt van nieuwe technologieën voor gegevensverwerking. Het instrument dat hiervoor volgens artikel 35 van de AVG moet worden gebruikt is de 'Gegevensbeschermingseffectbeoordeling' (verder: GEB). Deze bijlage voorziet in een model om de GEB op een gestructureerde en gestandaardiseerde wijze uit te voeren en te documenteren. Het eindproduct is een GEB-rapportage van de Stichting waarin de GEB´s die zijn uitgevoerd zijn geregistreerd. Ook registreert de verwerkingsverantwoordelijk in dit rapport de periodieke evaluaties die moeten worden uitgevoerd. Het model gebruikt u aan de hand van de volgende drie stappen.

Stap 1: is een GEB verplicht?

De eerste stap bestaat uit het bepalen of een GEB is verplicht. Niet voor iedere gegevensverwerking is een GEB nodig, alleen voor de verwerkingen die mogelijk een groot privacy-risico met zich meebrengen voor betrokkene(n). Bijvoorbeeld door de aard van de verwerking, de omvang of het doel van de verwerking.

Daarvan is in ieder geval - maar niet uitsluitend - sprake als het gaat om:
- de (grootschalige) verwerking van bijzondere of gevoelige persoonsgegevens van leerlingen [1];
- ziekteverzuim en re-integratie van personeel.

Wanneer verwerkingen gelijksoortig zijn en vergelijkbare risico's kennen, kunnen de verwerkingen in één GEB worden behandeld. Het is in dat geval niet nodig om voor elke verwerking een afzonderlijke GEB uit te voeren. Als gegevens worden verwerkt onder een gedragscode ligt het minder voor de hand dat een verwerking binnen die gedragscode onaanvaardbare hoge risico's zal opleveren.

In de volgende gevallen is een GEB verplicht.
De gegevensverwerking:
1. valt onder de reikwijdte van gegevensverwerkingen als beschreven in artikel 35 AVG;
2. staat op de 'zwarte' lijst van de Autoriteit Persoonsgegevens (AP); of
3. voldoet aan twéé of meer criteria van de criterialijst die door de werkgroep van Europese Privacytoezichthouders (WP29) is vastgesteld.

Overigens kan het ook in gevallen dat een GEB wellicht niet verplicht is, raadzaam zijn om toch een GEB uit te voeren. Het is een handig instrument om de risico's te inventariseren en passende maatregelen te treffen.

[1] Kennisnet heeft een gegevensbeschermingseffectbeoordeling (PIA) uitgevoerd voor online educatieve content (https://www.sambo-ict.nl/wp-content/uploads/2017/09/IBPDOC27-Responsible-Disclosure-versie-2.0.docx)

Ad 1. De gegevensverwerking valt onder de reikwijdte van artikel 35 AVG

Voor een aantal gegevensverwerkingen is in de AVG vastgesteld dat een GEB noodzakelijk is, namelijk wanneer het gaat om:

- de geautomatiseerde beoordeling van personen (denk aan profilering of een verzekeraar die automatisch claims laat beoordelen);
- grootschalige verwerking van bijzondere gegevens; of
- het grootschalig monitoren van openbare ruimtes (denk aan beveiligingscamera's en het volgen van smartphones voor marketingdoeleinden).

Ad 2. De gegevensverwerking staat op de 'zwarte' lijst van de AP

De AP heeft de bevoegdheid om een 'zwarte' lijst op te stellen (artikel 35 lid 4 AVG). De zwarte lijst bevat gegevensverwerkingen waarvoor een GEB altijd verplicht is. Naar verwachting verschijnt deze lijst in de loop van 2018.

De AP heeft als tegenhanger van de 'zwarte' lijst, ook de bevoegdheid om een 'witte' lijst op te stellen (artikel 35 lid 4 AVG). Op de witte lijst kan de AP gegevensverwerkingen vaststellen waarvoor nooit een GEB hoeft te worden uitgevoerd.

Ad 3. De gegevensverwerking voldoet aan twéé of meer criteria van de criterialijst die door de werkgroep van Europese toezichthouders (WP29) is vastgesteld

Valt de verwerking niet onder de reikwijdte van gegevensverwerkingen als beschreven in art. 35 AVG en bieden ook de 'witte' en 'zwarte' lijsten geen uitkomst, dan kan het bevoegd gezag negen criteria langslopen die door WP29 zijn opgesteld. Voldoet de verwerking aan méér dan twee van de criteria? Dan raadt de AP aan om een GEB uit te voeren.

Criterialijst WP29:

- ✓ Beoordelen van mensen op basis van persoonskenmerken (profilering, prognoses);
- ✓ Geautomatiseerde beslissingen;
- ✓ Stelselmatige en grootschalige monitoring;
- ✓ Gevoelige gegevens;
- ✓ Grootschalige gegevensverwerkingen;
- ✓ Gekoppelde databases;
- ✓ Gegevens over kwetsbare personen;
- ✓ Gebruik van nieuwe technologieën;
- ✓ Blokkering van een recht, dienst of contract.

Uitzondering: Voor gegevensverwerkingen met als grondslag een wettelijke plicht of algemeen belang dan wel openbaar gezag (artikel 6 lid 1c en e AVG) geldt dat een GEB niet nodig is als de wet die dit regelt specifiek is over de verwerking en er al een privacy-afweging heeft plaatsgevonden. Dit kan bijvoorbeeld blijken uit de parlementaire geschiedenis.

Stap 2: uitvoeren van de GEB

De tweede stap is het uitvoeren van de GEB conform het model zoals opgenomen in paragraaf 2 van het modelrapport. In de rapportage komt achtereenvolgens aan bod:

a) een beschrijving van de verwerkingsactiviteit of geheel aan samengevoegde verwerkingsactiviteiten en verwerkingsdoeleinden;
b) een beoordeling van de noodzaak en evenredigheid van de verwerkingen met het oog op de doelen;
c) een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;
d) de beoogde maatregelen om de gesignaleerde risico's aan te pakken; en
e) het advies van de FG.

Bij de uitvoering van de effectbeoordeling kan het wenselijk zijn om betrokkenen of hun vertegenwoordigers (MR) te vragen om hun mening over de voorgenomen verwerking. Ook is de verwerkingsverantwoordelijke verplicht om de FG om advies te vragen. De FG kan adviseren over het al dan niet uitvoeren van de GEB, de onderzoeksmethode, de vraag of misschien een gespecialiseerd bureau moet worden ingeschakeld, de waarborgen die nodig zijn om de risico's voor betrokkenen te beperken en de vraag of de uitkomsten van de GEB in overeenstemming zijn met de wet.

Ad a) een beschrijving van de verwerkingsactiviteiten

De rapportage vangt aan met een beschrijving van de verwerkingsactiviteit waarvoor een GEB wordt uitgevoerd. Hierbij moet ook worden vermeld met welke doeleinden de gegevens worden verwerkt en als het gaat om een gegevensverwerkingen onder de grondslag van een gerechtvaardigd belang (artikel 6 lid 1f AVG), om welk belang dit gaat. Raadpleeg hiervoor het register van verwerkingsactiviteiten (bijlage I bij het Privacyreglement).

Ad b) een beoordeling van de noodzaak en evenredigheid

Na de verwerkingsactiviteit(en) en de bijbehorende doeleinden te hebben beschreven moet de verwerking worden beoordeeld op noodzakelijkheid en evenredigheid (proportionaliteit) met het oog op het doel van de verwerking. Is de verwerking op deze manier nodig om het doel te bereiken? Is een eventuele inbreuk op de privacy van betrokkene niet onevenredig in verhouding tot dit doel?

Ad c) een beoordeling van de risico's

Stel vervolgens potentiële privacy risico's vast. Neem daarbij in ogenschouw welke negatieve gevolgen een (hypothetische) situatie waarin persoonsgegevens verloren gaan of onrechtmatig worden verwerkt met zich meebrengt voor de rechten en vrijheden van betrokkene(n). Ook is het nuttig om in kaart te brengen hoe groot de kans is dat deze gevolgen intreden en hoe groot de impact is op de betrokkene(n) en de organisatie als geheel als zich problemen of incidenten voordoen. Denk bijvoorbeeld aan de impact op de organisatie wanneer een incident leidt tot negatieve publiciteit.

De ‘handreiking Privacy Impact Assessment’ (de Engelse AVG benaming voor gegevensbeschermings-effectbeoordeling) uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland, kan behulpzaam zijn bij een systematische uitvoering van dit onderdeel. Deze handreiking voorziet onder meer in een vragenlijst aan de hand waarvan privacyrisico’s in kaart kunnen worden gebracht en is te raadplegen via https://www.norea.nl/download/?id=522. Ook het in september 2017 gepubliceerde model gegevensbeschermingseffectbeoordeling rijksdienst (PIA) kan dienen als handleiding bij de uitvoering van de GEB´s:
https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia

Ad d) de beoogde maatregelen

Op basis van de inschatting van de risico’s moet worden nagegaan óf en op welke manier risico’s vermeden of verkleind kunnen worden. Als blijkt dat aanvullende maatregelen nodig zijn, maak dit dan concreet en beschrijf deze in het rapport.

Ad e) advies FG

Neem tot slot een korte beschrijving op van het advies van de FG en wat daarmee is gedaan.

Verplicht advies AP: Wanneer uit een GEB volgt dat de verwerking een hoog risico oplevert en beoogde maatregelen dit risico onvoldoende kunnen beperken, is het bevoegd gezag verplicht voorafgaand aan de verwerking advies te vragen aan de AP (artikel 36 AVG). Tot de AP het onderzoek heeft afgerond en – binnen acht weken - advies heeft gegeven, mag het bevoegd gezag de verwerking niet uitvoeren.

Stap 3: periodieke evaluatie

Tot slot de derde en laatste stap: de evaluatie. De verwerkingsverantwoordelijke dient de verwerkingsactiviteiten waarvoor een GEB is uitgevoerd indien nodig – maar bij voorkeur periodiek – te toetsen op nakoming van de uitkomsten. Ook dient een nieuwe GEB te worden uitgevoerd als risico’s veranderen. Bijvoorbeeld door technologische ontwikkelingen, voortschrijdend inzicht of nieuwe informatie over zwakke plekken in de beveiliging.

Tot slot

Kennisnet werkt aan een set met sector-brede gegevensbeschermingseffectbeoordelingen voor de verwerkingen met een hoog risico die binnen vrijwel alle onderwijsorganisaties plaatsvinden. Als deze beoordelingen gepubliceerd zijn door Kennisnet, kunt u deze verwerken in uw eigen beoordelingen en bij deze rapportage voegen.