**Gegevensbeschermingseffectbeoordeling (GEB/DPIA)**

**sjabloon**

<NAAM GEB>

Bron: Dit sjabloon werd opgesteld door de [Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens](https://overheid.vlaanderen.be/vlaamse-toezichtcommissie" \t "_blank) en is afgeleid van het model van het d.pia.lab van de VUB: Brussel, 2020., licentie: CC BY SA 4.0.  
<https://researchportal.vub.be/files/53602836/dpialab_pb2020_1_final.pdf>  Zie ook [www.dpialab.org](http://www.dpialab.org/) [dpialab@vub.ac.be](mailto:dpialab@vub.ac.be)

# Inhoudstafel

[Inhoudstafel 2](#_Toc87943352)

[<naam GEB> 3](#_Toc87943353)

[0. Algemene omschrijving van de verwerking 4](#_Toc87943354)

[1. Projectstructuur 5](#_Toc87943355)

[1.1 Deelnemers aan GEB 5](#_Toc87943356)

[1.2 Projectwerking bij het opzetten van GEB 5](#_Toc87943357)

[1.3 Middelen voor het uitvoeren van de GEB 5](#_Toc87943358)

[1.4 (Her)evaluatie van GEB tijdens de verwerking 5](#_Toc87943359)

[2. Bronnen voor het opstellen van de GEB 6](#_Toc87943360)

[2.1 Algemeen overzicht 6](#_Toc87943361)

[2.2 Overzicht toepasselijkheid AVG 6](#_Toc87943362)

[3. Systematische beschrijving (verplicht) 8](#_Toc87943363)

[3.1 De scope van de GEB (in functie van de verwerkingsdoelen) 8](#_Toc87943364)

[3.2 Systematische beschrijving van de verwerkingen (en verwerkingsdoelen) 8](#_Toc87943365)

[3.3 Beschrijving van de context van de verwerkingen 8](#_Toc87943366)

[3.4 Beschrijving van de betrokkenen en andere actoren 8](#_Toc87943367)

[4. Noodzakelijkheid en evenredigheid (verplicht) 9](#_Toc87943368)

[4.1 De rechtmatigheid van de verwerking 9](#_Toc87943369)

[4.2 De basisbeginselen van de verwerking 9](#_Toc87943370)

[4.3 Beoordeel de noodzakelijkheid en evenredigheid (sensu strictu) 11](#_Toc87943371)

[5. Methode voor beoordeling risico’s op rechten en vrijheden van betrokkenen 12](#_Toc87943372)

[5.1 Aanvaardbaarheidscriteria van negatieve effecten 12](#_Toc87943373)

[5.2 Risicoanalyse, -evaluatie en opvolging 12](#_Toc87943374)

[6. Beoordeling risico’s op rechten en vrijheden van betrokkenen (verplicht) 13](#_Toc87943375)

[7. Beoogde maatregelen om risico’s aan te pakken (verplicht) 14](#_Toc87943376)

[8. Mening betrokkenen/vertegenwoordigers over de verwerking (verplicht) 15](#_Toc87943377)

[9. Adviezen betreffende de GEB (verplicht onder voorwaarden) 16](#_Toc87943378)

[9.1 Advies functionaris voor gegevensbescherming (verplicht indien aangesteld) 16](#_Toc87943379)

[9.2 Voorafgaande raadpleging bij de toezichthouder (verplicht bij hoog restrisico) 16](#_Toc87943380)

[10. Besluit van de verwerkingsverantwoordelijke (verplicht) 17](#_Toc87943381)

# <naam GEB>

|  |  |
| --- | --- |
| **Naam/referentie van het initiatief:** |  |
| **Naam, contactinformatie en andere identificatiegegevens van:** |  |
| **Verwerkingsverantwoordelijke(n) en hun vertegenwoordigers:** |  |
| **Verantwoordelijke(n) voor het project (business owner):** |  |
| **Functionaris(sen) voor gegevensbescherming (DPO)1:** |  |
| **Versie van GEB:** |  |
| **Referentie naar pre-GEB:** |  |
| **Classificatie:** |  Publiek   Vertrouwelijk   Informatieklasse [1/2/3/4/5] ... |

1 Alle Vlaamse bestuursinstanties moeten een functionaris aangesteld hebben en hun verwerkers ook.

2 De Vlaamse Toezichtcommissie voor de Vlaamse bestuursinstanties.

# Algemene omschrijving van de verwerking

<Beschrijf in algemene woorden de verwerking en de verwerkingsdoelen (max 1 A4) >

# Projectstructuur

## Deelnemers aan GEB

<Benoem interne en externe experten, betrokken partijen>

## Projectwerking bij het opzetten van GEB

### 1.2.1 Projectfasen en planning

<Geef aan op welke manier de GEB tot stand is gekomen, de projectfasen en de planning.>

### 1.2.1 Projectfasen en planning

<Geef aan op welke manier de projectstructuur garandeert dat de GEB plaats zal vinden voorafgaandelijk aan de verwerking.>

## Middelen voor het uitvoeren van de GEB

<Welke middelen – tijd, kosten, knowhow, … worden ingezet?>

## (Her)evaluatie van GEB tijdens de verwerking

<Geef aan of en op welke manier en wanneer de GEB gemonitord zal worden. Als een dergelijke monitoring niet wordt voorzien, dien je dit te verantwoorden.

Beschrijf hoe je een wijziging in het risico zal detecteren en op welke manier en wanneer je zal toetsen:

* Of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd
* Of er sprake is van een veranderend risico gerelateerd aan de verwerking

Bespreek hoe je zal omgaan met eventuele wijzigingen van het risico. Geef daarnaast aan welke procedure/stappen worden gevolgd wanneer uit de beoordeling van de GEB blijkt dat de verwerking niet wordt uitgevoerd volgens de bepalingen en principes zoals beschreven in de GEB>

# Bronnen voor het opstellen van de GEB

Hieronder worden de bronnen opgelijst die worden gebruikt bij het opstellen van de GEB. De lijst kan worden uitgebreid, hieronder is reeds een eerste onderverdeling terug te vinden. Zorg ervoor dat voldoende wordt toegelicht op welke manier de bron relevant is voor de beoogde verwerking(en).

## Wet- en regelgeving

<Beschrijf de algemene en specifieke wetgeving die op de verwerking van toepassing is en specifieer voor elke regelgeving waarom deze van toepassing is. De AVG kan een onderdeel zijn (met dan verwijzing naar specifieke elementen uit AVG, zoals bijvoorbeeld een verwijzing naar specifieke verwerkingssituaties zoals beschreven in artikels 85-91 AVG>

## Aanbevelingen van EDPB/EDPS

<Welke aanbevelingen van de EDPB/EDPS zijn relevant in de context van de beoogde verwerking(en)? >

## Aanbevelingen en standpunten van toezichthouders

<Zijn er standpunten van toezichthouders (Vlaamse Toezichtcommissie of andere (Europese) toezichthouders?>

## Aanbevelingen en standpunten van rechtbanken

<Zijn er standpunten van toezichthouders (Vlaamse Toezichtcommissie of andere (Europese) toezichthouders?>

# Systematische beschrijving (verplicht)

## De scope van de GEB (in functie van de verwerkingsdoelen)

<Beschrijf welke verwerkingen worden meegenomen in de GEB en welke verwerkingen eventueel uitgesloten zijn. Als verwerkingen worden uitgesloten, dient een verantwoording te worden gegeven waarom (en vooral: waarom dat dit de beoordeling niet beïnvloedt)>

## Beschrijving van de context van de verwerkingen

<Verwerkingen vinden steeds plaats in een bepaalde context. Beschrijf deze context.>

## Systematische beschrijving van de verwerkingen (en verwerkingsdoelen)

<Beschrijf op een systematische wijze de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd (indien van toepassing). Deel hierbij de verwerkingen in volgens doeleinde en nummer of label elk van de verwerkingen

Naast de systematische beschrijving wordt er bij voorkeur ook gebruik gemaakt van schema’s om de verwerking verder toe te lichten. Minimaal worden hier volgende schema's verwacht:

* **Architectuur** van de verwerking: een visualisatie van de verwerking in logische stappen, inclusief de aanduiding van enkele belangrijke architecturale eigenschappen (zoals encryptie of het gebruik van een encryptiesleutel, data transfer, aanduiding van een beveiligingsmaatregel, ...
* **Datamodel**: een visualisatie van de datastromen in functie van de verwerkingen en indien relevant, de verwijzing naar de betrokkenen. Op dit schema wordt zichtbaar gemaakt welke (categorieën) persoonsgegevens in welke fase van het verwerkingsproces worden verwerkt

In functie van de leesbaarheid van deze schema's kunnen deze worden opgesplitst in meerdere schema's. De doelstelling van de schema's is de lezer toe te laten een beter begrip te laten krijgen van de verwerking. Het doel is niet de verwerking tot in het detail te documenteren.>

## Beschrijving van de betrokkenen en andere actoren

<Lijst alle betrokken actoren op (minimaal alle type van betrokkenen) en hun mate van betrokkenheid/rol in de verwerking of hun belang daarin>

# Noodzakelijkheid en evenredigheid (verplicht)

<Beoordeel de noodzaak en evenredigheid van de verwerkingen met betrekking tot de doeleinden op basis van de beginselen>

## De rechtmatigheid van de verwerking

<Bespreek per verwerkingsdoel de rechtmatigheid van de verwerking (artikel 6 AVG) en, indien van toepassing, de voorwaarde waaraan is voldaan om het verwerkingsverbod zoals beschreven in artikel 9 op te heffen.

Als de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, beschrijf dan de gerechtvaardigde belangen die de verwerkingsverantwoordelijke behartigt.>

## De basisbeginselen van de verwerking

<Beschrijf per verwerkingsdoel op welke wijze de beginselen die op de verwerking van persoonsgegevens van toepassing zijn, zoals beschreven in artikel 5 AVG, werden geïmplementeerd. Volgende tabel kan helpen bij de verdere uitwerking. Als dezelfde beginselen van toepassing zijn op verschillende verwerkingsdoelen, wordt dit toegelicht.>

|  |  |  |
| --- | --- | --- |
| Eerlijkheid (beschrijf hoe je er voor zorgt dat de beoogde verwerking geen andere doelen heeft dan deze die beschreven zijn) | 5(1)(a) | ... |
| Transparantie (Hoe worden de betrokkenen goed geïnformeerd en hoe worden hun vragen behandeld?) | … |

|  |  |  |  |
| --- | --- | --- | --- |
| Beperking van het doel | Welbepaalde | 5(1)(b) | … |
| Uitdrukkelijk omschreven | … |
| Gerechtvaardigde doelen | ... |
| Niet verder verwerkt | … |
| *(Uitzonderingen)* | 89(1) | … |
| Gegevens-minimalisering | Toereikend | 5(1)(c) | ... |
| Ter zake dienend |
| Beperkt |
| Nauwkeurig-heid | Nauwkeurig | 5(1)(d) | ... |
| Up-to-date | ... |
| Opslag-beperking | Noodzakelijk | 5(1)(e) | … |
| (*Uitzonderingen*) | 89(1) | … |
| Gegevens-beveiliging | Integriteit en vertrouwelijkheid | 5(1)(f) | .. |
| Veiligheid van de verwerking | 32 |
| Gegevensbescherming door ontwerp | | 25(1) | … |
| Gegevensbescherming als standaard instelling | | 25(2) | ... |

## Beoordeel de noodzakelijkheid en evenredigheid (sensu strictu)

### Noodzaak

<Beschrijf en beoordeel van de noodzaak van de verwerkingen met betrekking tot de doeleinden. Waarom is (zijn) de beoogde verwerking(en) noodzakelijk in functie van het beoogde doel? >

### Evenredigheid

<Beschrijf en beoordeel van de evenredigheid van de verwerkingen met betrekking tot de doeleinden. Waarom is (zijn) de beoogde verwerking(en) evenredig is met het beoogde doel? Geef aan of er alternatieven zijn voor de beoogde verwerking die het doel op vergelijkbare wijze zouden kunnen bereiken, en waarom deze alternatieven niet worden aangewend>

# Methode voor beoordeling risico’s op rechten en vrijheden van betrokkenen

## Aanvaardbaarheidscriteria van negatieve effecten

<De verwerkingsverantwoordelijke bepaalt en motiveert de criteria voor de aanvaardbaarheid van negatieve effecten>

## Risicoanalyse, -evaluatie en opvolging

<Geef aan hoe je de risicomatrix opbouwt, met aandacht voor de risico-identificatie (methode), de impact en de kans en de manier waarop het risico wordt geëvalueerd. Bespreek op welke manier de risico’s nadien worden behandeld, met inbegrip van de risico’s die via maatregelen zullen worden gereduceerd. Geef aan hoe de beslissing over risico-acceptatie zal plaatsvinden, inclusief de verwerking van de adviezen van de functionaris voor de gegevensbescherming en eventueel voorafgaande raadpleging van de autoriteit>

# Beoordeling risico’s op rechten en vrijheden van betrokkenen (verplicht)

<Beoordeel de risico’s op rechten en vrijheden vanuit het standpunt van de betrokkenen (niet vanuit het standpunt van de verantwoordelijke, of vanuit de gehanteerde systemen of procedures). Geef aan welke risico’s zich kunnen manifesteren, wat de kans en impact is van het eventueel voorkomen en hoe deze moeten worden ingeschaald.>

# Beoogde maatregelen om risico’s aan te pakken (verplicht)

<Koppel aan elk geïdentificeerd risico minstens één maatregel, of geef aan wanneer er geen enkele maatregel mogelijk is, en schat nadien het restrisico in>

# Mening betrokkenen/vertegenwoordigers over de verwerking (verplicht)

<Zoals vermeld in artikel 35 lid 9 vraagt de verwerkingsverantwoordelijke in beginsel de betrokkenen of vertegenwoordigers naar hun mening over de voorgenomen verwerking>

# Adviezen betreffende de GEB (verplicht)

## Advies functionaris voor gegevensbescherming

<Wat is het advies van de functionaris voor de gegevensbescherming? Voeg het advies van de functionaris als een bijlage toe aan dit document.>

## Voorafgaande raadpleging bij de toezichthouder (verplicht bij hoog restrisico)

<Wat is de reactie van de toezichthouder betreffende de verwerking? Voeg de reactie toe in bijlage indien deze schriftelijk werd verstrekt.>

## Overzicht van de acties die de verwerkingsverantwoordelijke neemt naaar aanleiding van het advies van de functionaris en de raapleging van de toezichthouder

<Beschrijf op welke manier de verschillende elementen uit de adviezen en aandachtspunten werd gereageerd. Zorg ervoor dat op alle elementen uit de adviezen een reactie wordt geformuleerd, inclusief een verantwoording van de beoogde actie in functie van het risico. Een goeie werkmethode kan er in bestaan dat de adviezen en aanbevelingen in vorige punten worden genummerd.>

# Besluit van de verwerkingsverantwoordelijke (verplicht)

<Wat is het besluit van de verwerkingsverantwoordelijke?>