Hieronder vindt u het **toetsingskader** voor het **format DPIA-rapportage DGC**. Het toetsingskader wordt gebruikt door de onafhankelijke experts bij het beoordelen van de DPIA's.

Toetsingskader voor Format DPIA-rapportage DGC

1. Inleiding en context DPIA

[Beoordeeld aan de hand van onderdelen A1, A3, A4, A5 en A11 Format DPIA-rapportage DGC]

**Doel:** Beoordelen of de aanleiding, context en scope van de DPIA helder en volledig zijn beschreven.

**Toetsingscriteria:**

* De aanleiding voor de DPIA is helder omschreven.
* Er is een duidelijke beschrijving van de verwerking, het doel en de beoogde veranderingen.
* De scope van de DPIA is afgebakend (wat is wel/niet in scope).

**Beoordelingsvragen:**

* Is duidelijk waarom deze DPIA is uitgevoerd?
* Zijn de verwerkingsactiviteiten goed omschreven?
* Is de betrokken context van de verwerking toegelicht (juridisch, organisatorisch, technisch)?

**Oordeel**

**[ ]** Akkoord

*DPIA voldoet op dit punt aan de minimale vereisten.*

**[ ]** Niet akkoord

*De DPIA voldoet op dit punt niet aan de minimale vereisten.*

**Toelichting**

2. Betrokken partijen en rollen

[Beoordeeld aan de hand van onderdelen A6 en A7 Format DPIA-rapportage DGC]

**Doel:** Controleren of de verantwoordelijkheden en betrokken actoren goed in beeld zijn.

**Toetsingscriteria:**

* De verwerkingsverantwoordelijke is duidelijk benoemd.
* De eventuele verwerker(s) is/zijn geïdentificeerd.

**Beoordelingsvragen:**

* Zijn alle relevante actoren bij de verwerking benoemd, inclusief de verwerkingsverantwoordelijke, verwerker(s), Functionaris Gegevensbescherming, Chief Information Officer (CIO) en overige betrokken rollen, met een toelichting op hun betrokkenheid?

**Oordeel**

**[ ]** Akkoord

*DPIA voldoet op dit punt aan de minimale vereisten.*

**[ ]** Niet akkoord

*De DPIA voldoet op dit punt niet aan de minimale vereisten.*

**Toelichting**

3. Beschrijving gegevensverwerking

[Beoordeeld aan de hand van onderdelen A2, A4, A5, A8, A9, A10, B11, B12 en B13 Format DPIA-rapportage DGC]

**Doel:** Nagaan of de gegevensverwerking correct en volledig is beschreven.

**Toetsingscriteria:**

* Soorten persoonsgegevens zijn gespecificeerd.
* Doeleinden van verwerking zijn duidelijk omschreven.
* Verwerkingsgrondslag is benoemd en onderbouwd.
* Duur van de verwerking en bewaartermijnen zijn vermeld.
* Verwerkingslocaties zijn benoemd
* Ontvangers en doorgiften aan derde landen zijn benoemd.

**Beoordelingsvragen:**

* Zijn de doeleinden van de verwerking expliciet en specifiek omschreven?
* Zijn de bewaartermijnen en bewaardoeleinden per gegevenscategorie duidelijk omschreven?
* Is de verwerking begrijpelijk uitgelegd voor een niet-technisch publiek?
* Is de gekozen verwerkingsgrondslag benoemd én onderbouwd in relatie tot het doel?
* Zijn alle gegevenscategorieën opgenomen?

**Oordeel**

**[ ]** Akkoord

*DPIA voldoet op dit punt aan de minimale vereisten.*

**[ ]** Niet akkoord

*De DPIA voldoet op dit punt niet aan de minimale vereisten.*

**Toelichting**

4. Beoordeling van de noodzaak en evenredigheid

[Beoordeeld aan de hand van onderdeel B14 Format DPIA-rapportage DGC]

**Doel:** Toetsen of de verwerking noodzakelijk is en of er geen minder ingrijpende alternatieven zijn.

**Toetsingscriteria:**

* Er is een expliciete afweging gemaakt van noodzakelijkheid.
* Proportionaliteit wordt gewogen t.o.v. de inbreuk op de persoonlijke levenssfeer.
* Alternatieven zijn onderzocht en besproken (Subsidiariteit).

**Beoordelingsvragen:**

* Is onderbouwd waarom deze verwerking noodzakelijk is voor het doel?
* Worden de minst ingrijpende middelen ingezet?

**Oordeel**

**[ ]** Akkoord

*DPIA voldoet op dit punt aan de minimale vereisten.*

**[ ]** Niet akkoord

*De DPIA voldoet op dit punt niet aan de minimale vereisten.*

**Toelichting**

5. Beoordeling van de waarborging van de rechten van betrokkenen

[Beoordeeld aan de hand van onderdeel B15 Format DPIA-rapportage DGC]

**Doel:** Nagaan of betrokkenen hun privacyrechten, indien van toepassing, daadwerkelijk kunnen uitoefenen en of passende procedures zijn ingericht om deze rechten te respecteren en faciliteren.

**Toetsingscriteria:**

* De registratiehouder heeft onderbouwd welke rechten van betrokkenen van toepassing zijn (en welke evt. niet) en hoe invulling gegeven wordt aan de rechten van betrokkenen.
* De registratiehouder heeft, waar nodig, procedures hiervoor ingericht.

**Oordeel**

**[ ]** Akkoord

*DPIA voldoet op dit punt aan de minimale vereisten.*

**[ ]** Niet akkoord

*De DPIA voldoet op dit punt niet aan de minimale vereisten.*

**Toelichting**

6. Beoordeling van de risico’s voor betrokkenen

[Beoordeeld aan de hand van onderdeel C16 Format DPIA-rapportage DGC]

**Doel:** Beoordelen of de risico’s voor de rechten en vrijheden van betrokkenen goed zijn geanalyseerd.

**Toetsingscriteria:**

* De DPIA bevat een risicoanalyse m.b.t. privacy-impact.
* Verschillende risico’s (bijv. identiteitsdiefstal, verlies controle) zijn geclassificeerd naar waarschijnlijkheid en impact.
* Er wordt onderscheid gemaakt tussen individueel en collectief risico.

**Beoordelingsvragen:**

* Zijn de risico’s concreet en herkenbaar omschreven?
* Is er sprake van een systematische aanpak bij risico-inschatting?
* Zijn de risico’s geclassificeerd naar waarschijnlijkheid en impact, en is deze classificatie onderbouwd?

**Oordeel**

**[ ]** Akkoord

*DPIA voldoet op dit punt aan de minimale vereisten.*

**[ ]** Niet akkoord

*De DPIA voldoet op dit punt niet aan de minimale vereisten.*

**Toelichting**

7. Maatregelen ter beperking van risico’s

[Beoordeeld aan de hand van onderdeel D17 Format DPIA-rapportage DGC]

**Doel:** Controleren of passende technische en organisatorische maatregelen zijn voorgesteld en onderbouwd.

**Toetsingscriteria:**

* Specifieke maatregelen (bijv. pseudonimisering, encryptie, logging) zijn benoemd.
* Er is aangegeven welk risico door welke maatregel wordt verminderd.
* De effectiviteit van maatregelen is geëvalueerd.

**Beoordelingsvragen:**

* Zijn de voorgestelde maatregelen concreet en specifiek benoemd (technisch en organisatorisch)?
* Zijn de voorgestelde maatregelen realistisch en uitvoerbaar binnen de context van de organisatie?
* Zijn de risico’s geclassificeerd naar waarschijnlijkheid en impact, en is deze classificatie onderbouwd?
* Is de effectiviteit van de voorgestelde maatregelen onderbouwd of geëvalueerd (bijv. via een rest-risicoanalyse)?”

**Oordeel**

**[ ]** Akkoord

*DPIA voldoet op dit punt aan de minimale vereisten.*

**[ ]** Niet akkoord

*De DPIA voldoet op dit punt niet aan de minimale vereisten.*

**Toelichting**

8. Resultaten en conclusies

[Algemeen oordeel]

**Doel:** Toetsen of de uiteindelijke beoordeling helder en navolgbaar is.

**Toetsingscriteria:**

* De uitkomst van de DPIA is duidelijk samengevat.
* Eventuele resterende risico’s zijn benoemd.
* Er is aangegeven of aanpassing van het project nodig is.

**Beoordelingsvragen:**

* Is de eindconclusie van de DPIA duidelijk en kernachtig samengevat?
* Is de conclusie in lijn met de voorafgaande analyse en bevindingen?
* Zijn resterende risico’s expliciet benoemd en gewogen?
* Wordt duidelijk of de gegevensverwerking kan worden voortgezet, aangepast of gestopt?
* Is het besluit over de voortgang van de gegevensverwerking onderbouwd op basis van de DPIA-resultaten?

**Oordeel**

**[ ]** Akkoord

*DPIA voldoet op dit punt aan de minimale vereisten.*

**[ ]** Niet akkoord

*De DPIA voldoet op dit punt niet aan de minimale vereisten.*

**Toelichting**

9. Proces en documentatie

[Algemeen oordeel]

**Doel:** Beoordelen of het DPIA-proces transparant en herleidbaar is.

**Toetsingscriteria:**

* Het tijdstip van uitvoering (tijdig vóór besluitvorming) is aangegeven.
* De DPIA is afgestemd met de Functionaris Gegevensbescherming.
* Er is documentatie van consultaties (intern/extern).

**Beoordelingsvragen:**

* Is de DPIA uitgevoerd vóórdat met de verwerking gestart werd? (Zo nee verklaar waarom niet)
* Is het gehele DPIA-proces (besluiten, versies, adviezen) goed gedocumenteerd en traceerbaar?
* Zijn consultaties met interne en/of externe partijen gedocumenteerd (zoals IT, juridische afdeling, externe verwerker, FG)?
* Is de Functionaris Gegevensbescherming (FG) tijdig en aantoonbaar betrokken bij de DPIA?
* Eventueel: Zijn adviezen van de FG vastgelegd en verwerkt in het proces?

**Oordeel**

**[ ]** Akkoord

*DPIA voldoet op dit punt aan de minimale vereisten.*

**[ ]** Niet akkoord

*De DPIA voldoet op dit punt niet aan de minimale vereisten.*

**Toelichting**

**Eindbeoordeling DPIA:**

[ ] **[ ]**  Akkoord

Uit de DPIA blijkt dat de verwerking van persoonsgegevens geen onaanvaardbare (rest)risico’s oplevert voor de rechten en vrijheden van natuurlijke personen.

[ ] **[ ]** Niet akkoord

Uit de DPIA blijkt dat de verwerking van persoonsgegevens onaanvaardbare (rest)risico’s met zich brengt voor de rechten en vrijheden van natuurlijke personen.

**Toelichting bij het oordeel/samenvatting van de bevindingen:**

Graag ontvangen wij van u als beoordelaar een rapportage over de door u beoordeelde DPIA. In deze rapportage verwachten wij:

* een heldere conclusie of er sprake is van (on)aanvaardbare restrisico’s voor de rechten en vrijheden van betrokkenen;
* indien er sprake is van onaanvaardbare restrisico’s een korte onderbouwing hoe deze restrisico’s zich verhouden tot het toetsingskader;
* indien van toepassing: aanbevelingen voor aanvullende maatregelen.

De rapportage dient de eindbeoordeling van de DPIA (akkoord | niet akkoord) te onderbouwen en dit wordt gedeeld met de registratiehouder.