

Hoog-risico screening verwerkingen

Inhoud

Hoog-risico screening verwerkingen	1
Inleiding:	1
Procedure	1
Werkinstructie (wie-doet-wat)	2
Invulbaar screeningsformulier	4

Inleiding:

Dit document beschrijft één aanvullend proces dat naast bestaande procedures onderhouden dataregister en register van Verwerkingsovereenkomsten geldt. Het doel is vast te stellen of nieuwe of gewijzigde verwerkingen mogelijk een hoog risico opleveren voor de rechten en vrijheden van betrokkenen (AVG art. 35).

Het proces is uitgewerkt in drie vormen:

1. **Compacte procedure (± 1 A4)** – voor vaststelling
2. **Werkinstructie (wie-doet-wat)** – voor uitvoering
3. **Invulbaar screeningsformulier** – voor documentatie en bewijs

Procedure

Doel

Het tijdig, consistent en aantoonbaar bepalen of een nieuwe of gewijzigde verwerking mogelijk een hoog risico vormt voor de rechten en vrijheden van betrokkenen, en of een DPIA vereist is.

Reikwijdte

Deze procedure is van toepassing op **alle nieuwe én gewijzigde verwerkingen** van persoonsgegevens binnen de organisatie.

Onder een gewijzigde verwerking wordt onder andere verstaan:

- een nieuw of gewijzigd verwerkingsdoel;
- uitbreiding van soort of hoeveelheid persoonsgegevens;
- inzet van een nieuwe applicatie of leverancier;
- datadeling of koppelingen met derden;
- wijzigingen in (sub)verwerkersketen of doorgifte buiten de EER;
- wijziging in bewaartermijnen of beveiligingsniveau.

Proces in hoofdlijnen

1. **Startmelding**

De verantwoordelijke meldt een nieuwe of gewijzigde verwerking bij de Privacy- Security Officer.

2. **Hoog-risico screening**

De Privacy- Security Officer voert een vaste screening uit om te beoordelen of sprake kan zijn van een hoog risico.

3. **Besluit**

Op basis van de screening wordt vastgesteld of:

- een DPIA verplicht is;
- een DPIA wordt aanbevolen;
- een DPIA niet nodig is.

4. **Vastlegging**

De uitkomst en onderbouwing worden vastgelegd en opgenomen in het verwerkingsregister.

5. **Controle**

Bij de periodieke actualisatie van het verwerkingsregister wordt gecontroleerd of alle verwerkingen zijn gescreend.

Resultaat

- Voor elke verwerking is aantoonbaar vastgesteld of sprake is van (mogelijk) hoog risico.
- DPIA's worden uitgevoerd wanneer dit vereist is.
- Het verwerkingsregister bevat actuele en volledige informatie over hoog-risico-status en DPIA's.

Werkinstructie (wie-doet-wat)

Stap 1 – Signaleren

Wie: directeur, stafmedewerker, ICT, projectleider,

Wat: signaleert een nieuwe of gewijzigde verwerking

Resultaat: melding bij Privacy- Security Officer

Stap 2 – Startmelding

Wie: verantwoordelijke verwerking (bijv. Verwerker van softwareapplicatie)

Wat: levert korte beschrijving aan (doel, betrokkenen, applicatie, leverancier)

Resultaat: startregistratie (mail/formulier/ticket)

Stap 3 – Screening mogelijk hoog risico

Wie: Privacy- Security Officer

Wat: vult screeningformulier in op basis van vaste vragen

Resultaat: ingevulde screening met toelichting

Stap 4 – Besluit DPIA

Wie: Privacy- Security Officer (zo nodig in afstemming met FG)

Wat: bepaalt of sprake is van hoog risico en of een DPIA nodig is

Resultaat: besluit + motivatie

Stap 5 – Vastleggen

Wie: Privacy- Security Officer

Wat:

- slaat screening en besluit op;
- registreert uitkomst in het verwerkingsregister (hoog risico: ja/nee; DPIA: ja/nee/datum).

Stap 6 – Periodieke controle

Wie: Privacy- Security Officer

Wat: controleert bij periodieke actualisatie of alle verwerkingen een screening hebben

Resultaat: complete en actuele registratie

Invulbaar screeningsformulier

Bron: Werkdocument DPIA- Screeningsformulier

Algemene gegevens

- Naam verwerking:
- Verantwoordelijke:
- Datum screening:
- Nieuw of gewijzigd:
- Korte omschrijving verwerking:

Screening mogelijk hoog risico

Beantwoord onderstaande vragen met **ja/nee** en licht een *ja* kort toe.

1. Worden **leerlingen (kinderen)** verwerkt?
2. Betreft het **kwetsbare leerlingen** (zorg, OPP, jeugdhulp)?
3. Worden **bijzondere persoonsgegevens** verwerkt (gezondheid, gedrag, ontwikkeling)?
4. Is sprake van **grootschalige of structurele verwerking**?
5. Wordt **nieuwe of innovatieve technologie** ingezet?
6. Is er sprake van **monitoring, profilering of sturing**?
7. Worden gegevens **gedeeld met externe partijen**?
8. Is sprake van **doorgifte buiten de EU/EER**?
9. Kan misbruik of een datalek leiden tot **stigmatisering, uitsluiting of schade**?

Beoordeling

- Aantal 'ja' antwoorden:
- Conclusie mogelijk hoog risico:
 - ☐ Ja
 - ☐ Nee

Besluit

- DPIA verplicht:
 - ☐ Ja
 - ☐ Nee
- Motivatie (max. 5 regels):

Vastlegging

- Screening opgeslagen op locatie:
- Verwerkingsregister bijgewerkt (datum):
- Naam beoordelaar: