Kwaliteitskaart Wijs! – ICT– Verwerkingsovereenkomsten en DPIA

Kaart	**Kwaliteitskaart Wijs! – Verwerkingsovereenkomsten en DPIA**
Eigenaar	**Staffunctionaris H&F**
Versie	**juli 2025, jaarlijks evalueren**

Doel

Deze kaart heeft als doel het systematisch identificeren, beoordelen en beheren van risico's bij de verwerking van persoonsgegevens, zodat de privacy van betrokkenen wordt gewaarborgd en naleving van relevante wet- en regelgeving (zoals de AVG) wordt gegarandeerd.

Toepassingsgebied

Deze kwaliteitskaart beschrijft het proces voor de beoordeling en afhandeling van verwerkersovereenkomsten bij aanschaf van digitale (leer)middelen. Het zou moeten worden beschouwd als een aanvulling op het inkoop- en aanbestedingsbeleid van Wijs!.
Voor elke software digitale tool die voor het onderwijs of voor communicatie wordt gebruikt en persoonsgegevens van ouders, leerlingen of medewerkers bevat (bijvoorbeeld apps, softwarepakketten etc.) moet door Wijs! een gebruikersovereenkomst worden afgesloten. Het is niet toegestaan om producten te installeren of te gebruiken zonder dat deze overeenkomst beschikbaar is.
Aanwijzingen van medewerkers van de ICT-afdeling ten aanzien van virusbestrijding of versie-updates dienen te worden opgevolgd.

Het Bestuur is verantwoordelijk voor de gegevensbescherming. Dat betekent dat alleen een bestuurder bevoegd is om de (model)verwerkersovereenkomst en de bijlagen te tekenen. Het bevoegd gezag kan iemand mandateren (Bij Wijs! is de Privacy Officer gemandateerd) om namens het bestuur akkoord te geven op verwerkersovereenkomsten, maar de bestuurder blijft daar eindverantwoordelijk voor.
Na ondertekening kan het digitale product door alle scholen, die vallen onder het bestuur dat getekend heeft, gebruikt worden. Vooropgesteld dat ook de eventuele licentie voor al de scholen is aangeschaft.

Scholen hebben altijd voordat een digitaal systeem (waarin persoonsgegevens worden gebruikt) aangeschaft wordt, contact hebben met de PO en de verwerkersovereenkomst (inclusief motivatie) aanleveren. De Privacy Officer (PO) beoordeelt de verwerkersovereenkomst en stelt deze vast (indien van toepassing wordt een DPIA opgestart).
De verwerkersovereenkomst wordt opgenomen in het verwerkersregister.
Bij wijzigingen in de verwerking moet er een nieuwe verwerkersovereenkomst vastgesteld worden en het verwerkersregister geupdate worden.

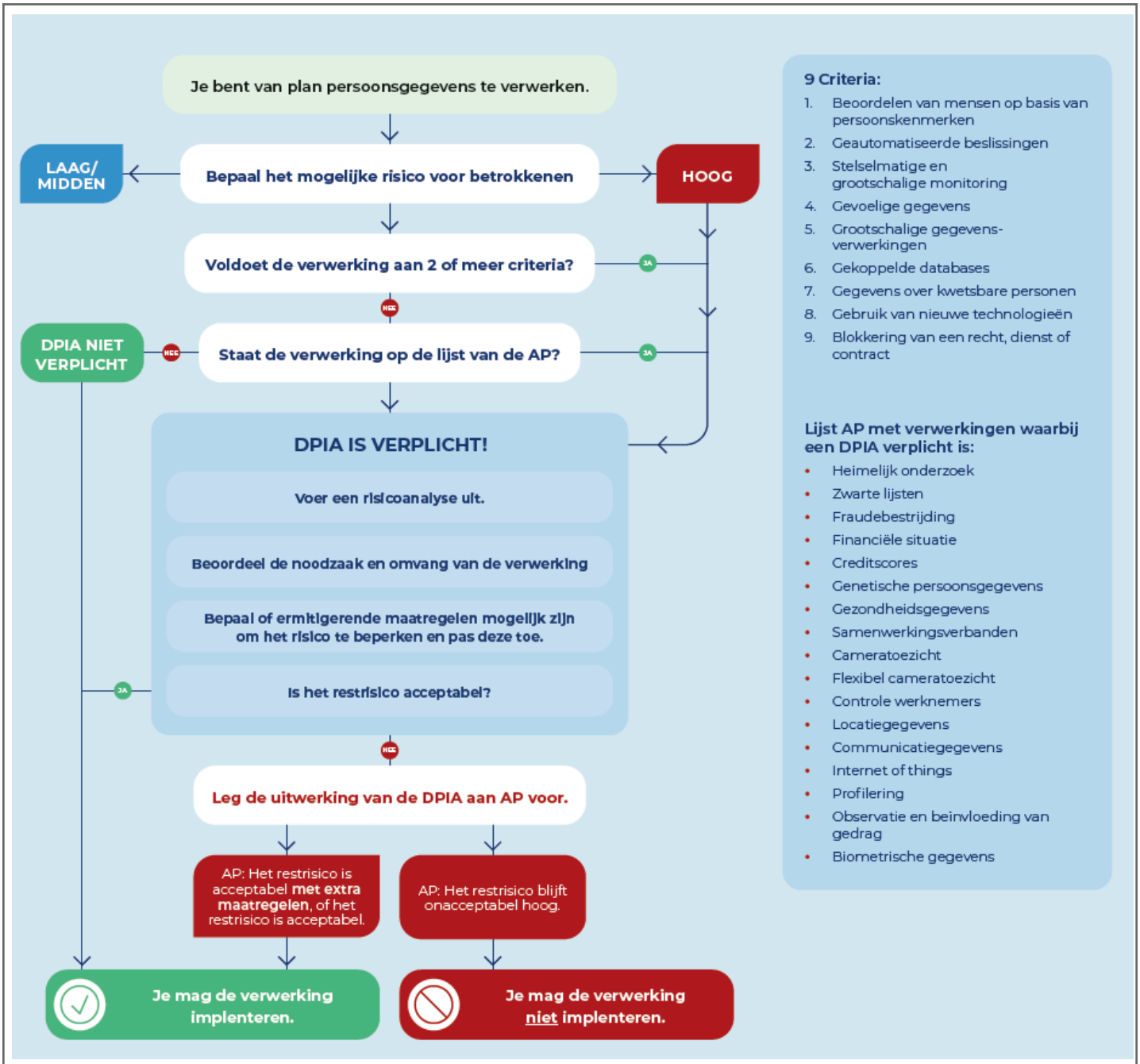
Als verwerkingsverantwoordelijke van privacy gevoelige gegevens moet er een risico-analyse worden uitgevoerd (Data Protection Impact Assessment (DPIA)) wanneer de gegevensverwerking **waarschijnlijk een hoog privacyrisico** oplevert. (Zie bijgevoegd stroomschema)

De Autoriteit Persoonsgegevens (AP) heeft een lijst gepubliceerd van verwerkingen die mogelijk een hoog risico opleveren voor de privacy van betrokkenen. De relevante thema's voor Wijs! staan hieronder dikgedrukt, hiervoor is een DPIA verplicht:

1. **Gezondheidsgegevens**
2. **Samenwerkingsverbanden**
3. Cameratoezicht
4. **Controle werknemers**
5. **Communicatiegegevens**
6. Internet of things
7. Profilering
8. **Observatie en beïnvloeding van gedrag**
9. Biometrische gegevens

Is er geen sprake van de bovenstaande verwerkingen, dan moet worden beoordeeld of de verwerking van gegevens waarschijnlijk een hoog privacyrisico oplevert, dat moet worden beoordeeld op basis van de onderstaande criteria. Als er twee of meer van deze criteria een 'ja' scoren is een DPIA verplicht.

1. Beoordelen van mensen op basis van persoonskenmerken (bv. LOVS en HR systeem)
2. Geautomatiseerde beslissingen
3. Stelselmatige grootschalige monitoring
4. Gevoelige gegevens
5. Grootschalige gegevensverwerking
6. Gekoppelde databases
7. Gegevens over kwetsbare personen
8. Gebruik van nieuwe technologieën
9. Blokkering van een recht, dienst of contract.



bron: poster Privacy op School

Een DPIA is een speciale risicoanalyse gericht op het voorkomen van privacyschending.

Pré DPIA

Om te beoordelen of er een DPIA nodig is, wordt een vooronderzoek uitgevoerd, een pre-DPIA, middels de Pre-DPIA Vragenlijst:

1. Beschrijving van het gegevensverwerkende proces
2. Verwerkte persoonsgegevens
3. Verwerkingsdoeleinden
4. Betrokken partijen

5. Bewaartermijnen
6. Beoordeling van de rechtmatigheid
7. Globale beoordeling van de risico's
8. Beveiligingsmaatregelen

De pre-DPIA wordt uitgevoerd door de Privacy Officer (PO) in samenwerking met procesverantwoordelijken.

Wijs! kiest altijd voor het gebruik van standaardinstelling van de systemen, met een minimale gegevensverwerking en niet meer verzamelt dan strikt noodzakelijk is (Privacy bij default). Daarbij wordt er gebruikgemaakt van geautoriseerd toegangsbeheer (alleen medewerkers die gebruikmaken van een programma ontvangen daarvoor inloggegevens en bepaalde rechten). Daarnaast maken we alleen gebruik van systemen die de gegevens binnen de EER opslaan.
Wijs! maakt altijd gebruik van de inrichtingsadviezen van Sivon.

Afname DPIA

De uitvoering van een DPIA valt onder de verantwoordelijkheid van de bestuurder. De uitvoering wordt bij Wijs! gedaan door de PO in teamverband (FG, IBP team en collega's die bij het werkproces betrokken zijn).
Voor de DPIA wordt gebruik gemaakt van standaard DPIA's opgesteld door Sivon (coöperatie van schoolbesturen in PO en VO- expertise en kennisdeling m.b.t. ICT producten en diensten voor scholen). In 2025 zal een DPIA Groenendijk Visma en Jamf door Sivon worden opgeleverd. Daarna zal Wijs! deze DPIA's voor de eigen organisatie beoordelen/afnemen.

Risico-identificatie

Inventarisatie van gegevensverwerkingen

- Identificeer alle processen waarin persoonsgegevens worden verwerkt.
- Bepaal de aard, omvang, context en doeleinden van de verwerking.

2. **Identificatie van risico's**
   - Breng potentiële risico's in kaart, zoals ongeautoriseerde toegang, verlies, wijziging of openbaarmaking van persoonsgegevens.
   - Overweeg interne en externe dreigingen.

Risico-beoordeling

1. **Beoordelingscriteria**
   De beoordeling van risico's gebeurt op basis van:
   a. **Impact:** De potentiële schade voor betrokkenen (bijv. financiële schade, reputatieschade, juridische gevolgen).
   b. **Waarschijnlijkheid:** De kans dat het risico zich voordoet.
2. **Classificatie van risico's**
   a. **Lage risico's:** Kleine impact en/of lage waarschijnlijkheid.
   b. **Middelgrote risico's:** Matige impact en/of matige waarschijnlijkheid.

c. **Hoge risico's:** Grote impact en/of hoge waarschijnlijkheid.

Risico-beheer

1. **Beheersmaatregelen**
   Op basis van de risicoanalyse worden passende maatregelen getroffen:
   a. **Lage risico's:** Basisbeveiligingsmaatregelen, zoals wachtwoordbeleid en toegangsbeheer.
   b. **Middelgrote risico's:** Aanvullende maatregelen, zoals encryptie, periodieke controles en bewustwordingscampagnes.
   c. **Hoge risico's:** Strenge beveiligingsmaatregelen, zoals Data Protection Impact Assessments (DPIA), pseudonimisering en regelmatige audits.
2. **Monitoring en evaluatie**
   a. Voer periodieke risico-evaluaties uit.
   b. Pas maatregelen aan bij veranderende omstandigheden.
   c. Rapporteer incidenten en leer van eerdere risico's.

Tot slot

Door een gestructureerde aanpak te hanteren voor het identificeren, beoordelen en beheren van risico's bij de verwerking van persoonsgegevens, wordt de privacybescherming gewaarborgd en wordt voldaan aan wet- en regelgeving.

Literatuur of verder lezen?

- Privacy bij design en default:
- https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht
- https://normenkaderibp.kennisnet.nl/groeipad/fase-4/deelproject-4-4-privacy-by-design-en-privacy-by-default-toepassen/
- https://www.privacyconvenant.nl/over/