

DPIA LDOS

Bestemd voor het Bestuur van het SWV VO Westelijke mijnstreek, Maastricht Heuvelland en Parkstad (SWVVO3104-3105-3106)

Inleiding

Deze DPIA schetst de privacy risico's en beheersmaatregelen rond het gebruik van LDOS in een onderwijscontext. LDOS is een platform voor leer- en leerling gegevens. Binnen het SWV ligt de focus op gegevens benodigd voor de beoordeling de aangevraagde financiering bijzonder onderwijs. Hieronder valt ook een beperkte set gezondheidsgegevens van leerlingen.

Reikwijdte

- **Verwerkingsverantwoordelijke:** Bestuur van het SWV VO Westelijke mijnstreek, Maastricht Heuvelland en Parkstad (SWVVO3104-3105-3106)
- **Verwerkers:** LDOS-leverancier en eventuele hosting/cloudproviders.
- **Betrokkenen:** Leerlingen/studenten (voornamelijk minderjarigen), ouders/verzorgers, ondersteuningscoördinatoren/gedragswetenschappers van de scholen, VSV/BLD¹ en medewerkers van het SWV.
- **Doeleinden (hoog over):** Beoordeling financiering speciaal onderwijs, wettelijke verantwoording en rapportage en administratie omtrent zogenaamde thuiszitters.
- **Bijzonderheden:** Vanwege de taak van het SWV worden bijzondere persoonsgegevens verwerkt m.b.t. gezondheid/ondersteuningsbehoefte, minderjarige thuiszitters , grootschalige verwerking.

Beschrijving van de verwerking

Datastromen en systeemlandschap

- **LDOS-kern:** Vastleggen gegevens, normalisatie, opslag (datawarehouse/data lake), verrijking/analyse, visualisatie.
- **Uitgangen:** Overzicht voor beoordeling, resultaat beschikkingen, rapportages (inspectie/gemeente/kwaliteitszorg).

Geografische verwerkingen: Datacenterlocaties, back-ups, supporttoegang met name belegd bij leverancier LDOS.

¹ VSV staat voor Voortijdig Schoolverlaten, en BLD is het [Bureau InformatieDiensten](#) Nederland dat rapportages over VSV'ers maakt om vroegtijdig schoolverlaten te bestrijden.

Categorieën gegevens, doeleinden, grondslagen en bewaartermijnen

Categorie gegevens	Doel	Grondslag (AVG art. 6)	Bewaartermijn	Ontvangers
Identificatie (naam, nummer, school)	Identificatie en logistiek	Wettelijke taak van algemeen belang	Wettelijke bewaartermijnen worden gehanteerd	CvT, LDOS-verwerker
Gegevens t.b.v. aard van de aanvraag	Beoordeling, administratie	Wettelijke taak van algemeen belang	Wettelijke bewaartermijnen worden gehanteerd	CvT, LDOS-verwerker
Medische indicatie	Toekenning Passend onderwijs	Art. 9 lid 2 (bijzondere gegevens) – Wettelijke taak van algemeen belang	Zo kort mogelijk; periodieke review	CvT, LDOS-verwerker
Ondersteuningsbehoefte	Toekenning Passend onderwijs	Art. 9 lid 2 (bijzondere gegevens) – Wettelijke taak van algemeen belang	Strikt noodzakelijk; beperkte toegang	CvT, LDOS-verwerker
Gegevens thuiszitters	Stimulatie onderwijs-deelname	Taak van algemeen belang	Geaggregeerd zo lang als nodig; ruwe data kort	CvT, LDOS-verwerker, Leerplicht-ambtenaar, VSV/BLD

Vanuit kwaliteitsbewaking wordt de totale gegevensset ingezien en in analyses verwerkt om trends te volgen en rapportages te maken voor management en jaarverslagen.

Noodzaak en proportionaliteit

- **Doelbinding:** LDOS-inzet is gericht op bieden passend onderwijs, beperken thuisblijven en verantwoording toegang speciaal onderwijs. Gegevens worden niet gebruikt voor niet-verenigbare neven doelen.
- **Dataminimalisatie:**
 - Alleen de velden die nodig zijn per doel worden gevuld.
 - Gevoelige velden zijn gescheiden (bijzondere gegevens) logisch en technisch.
- **Transparantie:**
 - Duidelijke, doelgroepgerichte informatie voor school en ouders.
 - Er is beleid dat transparantie waarborgt.
- **Rechten van betrokkenen:**
 - Toegang, rectificatie, beperking, bezwaar via proces dat in lijn is met AVG-regels.
 - Geen of beperkte geautomatiseerde besluitvorming met rechts- of aanmerkelijke gevolgen; waar gebruikt, is menselijke tussenkomst geborgd en er is een bezwaarroute.
- **Bewaarbeperking:**
 - Er is een overzicht van concrete bewaartermijnen
 - Er wordt voldaan aan wettelijke plichten en er is een bezwaar- en klachtenprocedure.



Risicoanalyse

Risico	Oorzaak	Impact voor betrokkene	Kans	Huidige beheersing
Ongeautoriseerde toegang	Te ruime rollen, zwakke authenticatie	Blootstelling zorgdata, reputatie- en emotionele schade	Klein	Beperkte toegang inclusief MFA beveiliging
Functievermenging doelafwijking	Hergebruik data zonder toetsing	Profilering, vertrouwensbreuk	Klein	Beleid; Beperkte toegang
Bias in analyses	Onvolledige/vertekenende data	Onterechte afwijzing ongelijke behandeling	Klein-Middel	Validatie; meerdere mensen-in-de-lus, bezwaar-procedure
Overmatige monitoring	Fijnmazige tracking thuiszitters	Druk op welzijn, tegenwerking	Middel	Beperking in proces, drempels gegevensvastlegging
Datalek/incident	Softwarefout, phishing, exportfouten	Identiteitsfraude, schade	Klein-Middel	Encryptie, DLP, IRP
Onvoldoende transparantie	Onduidelijke communicatie	Onzekerheid, klachten, verlies vertrouwen	Klein	Privacy-informatie, Beleid
Derde-land overdracht	Cloud buiten EER zonder passende waarborgen	Onrechtmatige toegang, minder bescherming	Klein	Bindende afspraken leverancier, verwerkers-overeenkomst



Beperkende maatregelen

Governance en proces

- **Rollen en verantwoordelijkheden:** Er is een proceseigenaar LDOS, een FG; en taken en bevoegdheden zijn vastgelegd.
- **DPIA-levend document:** Herzie bij scopewijzigingen, nieuwe datasets, algoritmereleases.
- **DPIA/Change gate: Verwerkingsregister:** up-to-date; **DPIA-check:** voorafgaand aan uitbreidingen.

Juridisch en contractueel

Onderstaande is voorzien en de omgang met LDOS:

- **Verwerkersovereenkomst:** Doelbinding, subverwerkers, auditrechten, supporttoegang, incidentmeldingstermijnen.
- **Bijzondere gegevens:** Specifieke rechtmatigheid (art. 9), strikte noodzaak, gescheiden opslag en toegangsregimes.

Toegangs- en identiteitsbeheer

- **RBAC en least privilege:** Rollen per functie; periodieke herijking FG.
- **Sterke authenticatie:** MFA voor alle personeel voor gevoelige datasets.
- **Logging en monitoring:** Onweerlegbare auditlogs, anomalie meldingen, periodieke logreviews.

Dataminimalisatie en ontwerp

- **Scheiding van omgevingen:** Productie/acceptatie/test strikt gescheiden; geen productie-PII in test.
- **Pseudonimiseren/aggregatie:** Werk met pseudoniemen in analytics; toon op dashboards wat nodig is per rol.
- **Privacy by default:** Conservatieve standaardinstellingen; opt-ins voor optionele features.

Beveiliging

- **Encryptie:** Rustend (AES-256) en in transit (TLS 1.2+); sleutelbeheer gescheiden van data.
- **Hardening en patching:** Beheer lifecycle; SBOM; kwetsbaarheidsscans en pentests.
- **Data Loss Prevention:** Beperk exports; watermarking; goedkeuringsflows voor gevoelige exports.
- **Back-ups & DR:** Versleuteld, getest, RTO/RPO afgestemd op onderwijscontinuïteit.

Rechten en transparantie

- **Uitlegbaarheid analytics:** Publiceer modeldoelen, gebruikte variabelen, validatie, en beperkingen.
- **Minderjarigen:** Ouders/verzorgers waar van toepassing; kindvriendelijke communicatie.

Incidentrespons en training

- **IRP:** Duidelijke stappen, meldingscriteria AP/betrokkenen, oefencycli.
- **Awareness:** Bewustzijn borgen bij gebruikers over data-inzichten, bias, en exportveiligheid.
- **Third-party risk:** Security due diligence, certificeringen, jaarlijkse assurance (bijv. ISAE/SOC).

Rest-risico, besluit en opvolging

- **Rest-risico-inschatting:** Na implementatie van bovenstaande maatregelen is de verwachting van de restrisico's "Klein" voor de meeste risico's; bias en overmatig monitoren blijven aandachtspunten (mogelijk "middel").
- **Besluit:** Verwerking is proportioneel.
 - **Aanbeveling:** dataminimalisatie heroverwegen en eventueel proces aanpassen.
- **AP-consultatie:** Vereist indien na maatregelen een "hoog" restrisico blijft (bijv. grootschalige profilering met aanmerkelijke gevolgen zonder adequate mitigatie). Documenteer motivatie. Vooralsnog niet van toepassing.
- **Actieplan:**
 - **Korte termijn (0–3 mnd):** Vaststelling deze DPIA.
 - **Midden (3–6 mnd):** Actueel houden beleid en processen. Opvolgen aanbeveling.
 - **Doorlopend:** jaarlijkse DPIA-herziening.

Benodigde details aanwezig waarmee dit document gefinaliseerd kan worden.

- **LDOS-specificaties:** SaaS, datalocaties, subverwerkers (leverancier heeft de gegevens en dit ligt vast in verwerkersovereenkomst).
- **Datascope:** Exacte datasets/velden, inclusief eventuele bijzondere gegevens liggen vast in het ontwerp van LDOS (leverancier heeft de gegevens).
- **Functionaliteit:** Gebruikte analyses/algoritmen, automatische signalering, risicoscores.
- **Grondslagen:** Wettelijke kaders onderwijs en toekenning financiering speciaal onderwijs.
- **Bewaarbeleid:** Wettelijke termijnen worden gehanteerd.

Vaststelling

Ondergetekende verklaart dit document (Data Protection Impact Assessment) te hebben vastgesteld.

Plaats: Heerlen

Datum: 22-9-25

Handtekening: 

Naam: **Maaïke Vos**

Functie: **Directeur** Samenwerkingsverbanden VO Westelijke Mijnstreek 31.04, Maastricht-Heuvelland 31.05 en Parkstad 31.06. **Gemandateerd door de Besturen** van de genoemde samenwerkingsverbanden.