



## Bijlage 2: Beveiligingsbijlage Leerling in beeld

Behorende bij verwerkersovereenkomst van Cito B.V. en specifiek voor het product **Leerling in beeld primair en speciaal onderwijs op het Cito platform**

Versie: **12 juli 2022**

Cito B.V. heeft, overeenkomstig de AVG en artikel 7 en 8 van de Model Verwerkersovereenkomst passende technische en organisatorische maatregelen genomen om de verwerking van persoonsgegevens aantoonbaar te beveiligen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

### 1. Maatregelen die Cito B.V. heeft genomen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, wijziging, opslag, toegang of openbaarmaking.

- Een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;
- Een systeem van autorisatie waardoor enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie;
- Er is een coördinator informatiebeveiliging die de risico's omtrent de verwerking van persoonsgegevens inventariseert, het beveiligingsbewustzijn stimuleert, voorzieningen controleert en maatregelen treft die zien op naleving van het informatiebeveiligingsbeleid. Deze coördinator is bereikbaar op het volgende e-mailadres: [klantenservice@cito.nl](mailto:klantenservice@cito.nl).
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid;
- Er is een proces ingericht voor communicatie over informatiebeveiligingsincidenten;
- Met medewerkers worden geheimhoudingsverklaringen afgesloten en worden informatiebeveiligingsafspraken gemaakt;
- Het bewustzijn, opleiding en training ten aanzien van informatiebeveiliging wordt gestimuleerd.
- Cito B.V. heeft het internationale normenkader ISO27001 gebruikt als standaard voor het ISMS (Information Security Management System) en is ISO27001 gecertificeerd.

## 2. Maatregelen om de Persoonsgegevens te beveiligen en continuïteit van de middelen, het netwerk, de server en de applicatie te waarborgen.

Hieronder staat de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden, zoals beschreven in het Certificeringsschema informatiebeveiliging en privacy ROSA. Zie: [https://www.edustandaard.nl/standaard\\_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/](https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/).

|                          |                                                                                                                                                  |                   |               |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------|
| <b>Toetsvorm</b>         | Self assessment                                                                                                                                  |                   |               |
| <b>Uitvoerder toets</b>  | F. Nabuurs, informatiemanager – security officer, Cito                                                                                           |                   |               |
| <b>Inlogpagina</b>       | <a href="http://www.cito.nl/onderwijs/primair-onderwijs/lvs-leerling-in-beeld">www.cito.nl/onderwijs/primair-onderwijs/lvs-leerling-in-beeld</a> |                   |               |
| <b>BIV-classificatie</b> | Beschikbaarheid = H Integriteit = M Vertrouwelijkheid = M                                                                                        |                   |               |
| <b>Categorie</b>         | <b>Maatregelen</b>                                                                                                                               | <b>Compliance</b> | <b>Uitleg</b> |
| <b>Beschikbaarheid</b>   | Ontwerp                                                                                                                                          | voldaan           |               |
|                          | Capaciteit beheer                                                                                                                                | voldaan           |               |
|                          | Onderhoud                                                                                                                                        | voldaan           |               |
|                          | Testen                                                                                                                                           | voldaan           |               |
|                          | Monitoring                                                                                                                                       | voldaan           |               |
|                          | Herstel                                                                                                                                          | voldaan           |               |
| <b>Integriteit</b>       | Herleidbaarheid (gebruikers)                                                                                                                     | voldaan           |               |
|                          | Backup                                                                                                                                           | voldaan           |               |
|                          | Application controls                                                                                                                             | voldaan           |               |
|                          | Onweerlegbaarheid                                                                                                                                | voldaan           |               |
|                          | Herleidbaarheid (technisch beheer)                                                                                                               | voldaan           |               |
|                          | Controle integriteit                                                                                                                             | voldaan           |               |
| <b>Vertrouwelijkheid</b> | Onweerlegbaarheid (toepassing)                                                                                                                   | voldaan           |               |
|                          | Levenscyclus gegevens                                                                                                                            | voldaan           |               |
|                          | Logische toegang                                                                                                                                 | voldaan           |               |
|                          | Fysieke toegang                                                                                                                                  | voldaan           |               |
|                          | Netwerk toegang                                                                                                                                  | voldaan           |               |
|                          | Scheiding omgevingen                                                                                                                             | voldaan           |               |
|                          | Transport en fysieke opslag                                                                                                                      | voldaan           |               |
|                          | Logging                                                                                                                                          | voldaan           |               |
|                          | Omgaan met kwetsbaarheden                                                                                                                        | voldaan           |               |

### 3. Afspraken over het informeren over beveiligingsincidenten en/of Datalekken

Cito B.V. heeft een procedure voor de monitoring en identificatie van incidenten en het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging. In zo'n geval zullen wij de verwerkingsverantwoordelijke de volgende informatie ter hand stellen:

- De kenmerken van de inbreuk, zoals: datum en tijdstip ontdekken en duur inbreuk, samenvatting van de inbreuk waaronder de aard van de inbreuk en de aard en beschrijving van het beveiligingsincident (op wat voor onderdeel van de beveiliging gaat het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
- De oorzaak van de inbreuk;
- Hoe de inbreuk is ontdekt;
- De maatregelen die getroffen zijn om de inbreuk aan te pakken en eventuele (verdere en toekomstige) schade te voorkomen;
- Of de bij de inbreuk betrokken gegevens versleuteld, gehasht etc. waren;
- Benoemen van groep(en) Betrokkenen die gevolgen kunnen ondervinden van het incident, en de aantallen en omvang van de groep Betrokkenen;
- Wat de mogelijke gevolgen zijn van de inbreuk voor de Onderwijsinstelling en de Betrokkene(n), waaronder indien mogelijk een inschatting van het risico van de gevolgen voor betrokkene(n);
- De hoeveelheid en soort Persoonsgegevens betrokken bij de inbreuk (met name bijzondere gegevens zoals gegevens over gezondheid of godsdienst, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

In geval van een (vermoeden van) beveiligingsincident en/of Datalek zal onze coördinator informatiebeveiliging, in beginsel per e-mail contact opnemen met de contactpersoon van de Onderwijsinstelling die is vermeld in bijlage 4. De coördinator informatiebeveiliging is tevens aanspreekpunt voor het geval de Onderwijsinstelling contact wil opnemen over een beveiligingsincident en/of Datalek. De coördinator informatiebeveiliging is bereikbaar op het volgende e-mailadres: [klantenservice@cito.nl](mailto:klantenservice@cito.nl)

### Paraaf

Onderwijsinstelling

Verwerker

---

*Deze bijlage is opgezet volgens het branche-specifieke format van MEVW en vormt een integraal onderdeel van de bijbehorende verwerkersovereenkomst. Verwerkersovereenkomst en de bijlagen daarbij maken onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 4.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (MEVW, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <https://www.privacyconvenant.nl/>.*