Bijlage 2 Technische en organisatorische beveiligingsmaatregelen

Cito B.V.

De Bewerker is overeenkomstig de WBP en artikel 7 Bewerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens.
In deze bijlage wordt omschreven welke beveiligingsmaatregelen er zijn getroffen. De beveiliging is een continu punt van aandacht en zorg.

Omschrijving van de maatregelen zoals bedoeld in artikel 7.2 Bewerkersovereenkomst

I. Toegang tot persoonsgegevens

Om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens hanteert Cito een autorisatiebeleid. Op grond van deze systematiek hebben medewerkers geen toegang tot meer gegevens dan strikt noodzakelijk is voor de uitoefening hun functie.

Medewerkers en gegevens	**Handelingen**
Medewerkers van klantenservice hebben toegang tot licentie- en verkoopinformatie. Zij kunnen onder meer zien welke school toegang heeft tot bepaalde toetsproducten en diensten en hoeveel (digitale) toetsen zijn afgenomen. De klantenservice heeft geen inzage in toets- of leerresultaten van leerlingen.	Administratieve handelingen in het kader van de toegang tot en (ver)werking van toetsproducten en –diensten. Ondersteuning van de klant bij vragen.
Medewerkers van de technische helpdesk (1e en 2e lijn) kunnen in het kader van een specifieke vraag of een probleem én met toestemming van de verantwoordelijke tijdelijk toegang krijgen tot de op het specifieke probleem betrekking hebbende leerlinggegevens en toets- of leerresultaten	Analyse van het specifieke probleem. Hulp bieden aan de eindgebruiker. Als het probleem is opgelost of de vraag is beantwoord, worden de betrokken gegevens verwijderd. Een globale omschrijving van het probleem wordt vastgelegd voor opvolging. Als het voor opvolging is vereist, worden de betrokken gegevens maximaal een half jaar bewaard.
Medewerkers van de logistieke afdeling hebben toegang tot ingestuurde antwoordformulieren (optisch leesbare formulieren).	Digitalisering (scannen) van antwoordformulieren om de gegevens geschikt te maken voor scoringsservice en rapportage of voor analyse en onderzoek.
Toetsdeskundigen en/of psychometristen hebben toegang tot geanonimiseerde (gepseudonimiseerde) sets van en toetsresultaten, leerling- en schoolkenmerken.	De geanonimiseerde (gepseudonimiseerde) afnamegegevens worden gebruikt voor onderzoeksdoeleinden om de toetsen van het Volgsysteem primair onderwijs en speciale leerlingen te kunnen verbeteren en verder te ontwikkelen.
IT- & databasebeheerders hebben toegang tot de centrale databases.	De handelingen van de IT- & databasebeheerders zijn gericht op beschikbaarheid, continuïteit en optimalisatie van ICT-systemen.

II. Maatregelen om persoonsgegevens te beschermen tegen misbruik

Organisatie van informatiebeveiliging en communicatieprocessen

- Cito heeft een coördinator voor informatiebeveiliging om risico's omtrent de verwerking van persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die toezien op naleving van het informatiebeveiligingsbeleid.
- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Cito heeft een proces ingericht en gedocumenteerd voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers (zowel intern als extern) worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Cito stimuleert bewustzijn, opleiding en training ten aanzien van privacy en informatiebeveiliging.
- Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

Fysieke beveiliging en continuïteit van de middelen

- Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf.
- Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.
- Er worden periodiek back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze back-ups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving.
- De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's.

Netwerk-, server- en applicatiebeveiliging en onderhoud

- De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord.
- De digitale omgevingen waarbinnen persoonsgegevens worden verwerkt komen tot stand op basis van systeemplanning, beveiligingscontrole en acceptatie. Wijzigingen in applicaties worden getest op kwetsbaarheden voordat deze in productie worden genomen.
- Op systemen worden periodiek de laatste (beveiligings-)patches geïnstalleerd op basis van patchmanagement.
- Penetratietests en vulnerability assessments worden periodiek uitgevoerd.
- Op wachtwoorden worden crypto grafische maatregelen toegepast om deze gegevens veilig op te slaan.
- Er wordt voor inlogprocessen gebruik gemaakt van versleutelde verbindingen.
- De uitwisseling van persoonsgegevens tussen de onderwijsinstelling en Cito vindt versleuteld. plaats. Dit is eveneens van toepassing op de communicatie tussen lokaal geïnstalleerde Cito producten en de Cito ICT omgeving.
- De uitwisseling van persoonsgegevens aan derden in opdracht van de onderwijsinstelling vindt eveneens versleuteld plaats.

III. Maatregelen om zwakke plekken te identificeren

De systemen van Cito worden periodiek gecontroleerd op veiligheid door Hoffmann B.V. Daarnaast voorziet het beveiligingsbeleid van Cito in interne processen om kwetsbaarheden te identificeren en op te lossen.

Informeren over datalekken en/of incidenten met betrekking tot beveiliging

De wijze waarop monitoring en identificatie van datalekken plaatsvindt:

Cito monitort 24/7 haar dienstverlening en heeft de in Bijlage 2 opgenomen maatregelen getroffen om ongeoorloofde of onrechtmatige toegang tot gegevens te voorkomen en te identificeren. Signalen die duiden op een datalek worden beoordeeld door de security officer van Cito, die analyseert of sprake kan zijn van een datalek.

De wijze waarop informatie wordt gedeeld:

Wanneer zich een datalek voordoet, wordt de verantwoordelijke onderwijsinstelling door of namens Cito in beginsel binnen 24 uur na ontdekking van het datalek per e-mail geïnformeerd. Afhankelijk van de situatie, kan ook informatie worden gedeeld via onze website en officiële sociale media kanalen en/of officiële distributeurs en/of handelsagenten.

Voor vervolgacties of vragen kan telefonisch of per e-mail contact worden opgenomen met onze helpdesk via de in de Privacy Bijsluiter opgenomen gegevens.

Cito deelt ten minste de volgende informatie wanneer zich een datalek voordoet:

- De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
- De oorzaak van het beveiligingsincident;
- De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
- Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
- De omvang van de groep betrokkenen;
- Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

Indien een concrete situatie zich daartoe leent, dan kan Cito een (eerste) melding van een datalek doen aan de Autoriteit Persoonsgegevens. De Onderwijsinstelling wordt hierover geïnformeerd en blijft ook in dit geval eindverantwoordelijk voor de melding.

Rapportage

Bewerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via http://www.cito.nl/over%20cito/privacyverklaring_website_cito

In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de Klantenservice van Cito, telefonisch bereikbaar via (026) 3521 11 11 of per mail via klantenservice@cito.nl.

Versie

Deze bijlage Technische en Organisatorische maatregelen is voor het laatst bijgewerkt op 13-11-2016.

Deze privacy bijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 2.0, een initiatief van de PO-Raad, VO-raad, de verschillende betrokken ketenpartijen (GEU, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: http://www.privacyconvenant.nl.