Bijlage 2 Beveiligingsbijlage

Cito B.V.

Dit is de branchespecifieke beveiligingsbijlage van de Vereniging Digitale Onderwijs Dienstverleners (VDOD). Deze bijlage is gebaseerd op bijlage 2 bij de model verwerkersovereenkomst behorende bij het Convenant. Dit model is afgestemd door de Initiatiefnemers van het Convenant en is gepubliceerd op de website https://www.privacyconvenant.nl/.

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 Model Verwerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens, en om die maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen.

Aantoonbaarheid beveiligingsmaatregelen

Verwerker is verplicht om aan Onderwijsinstelling aan te tonen of en op welke wijze passende technische en organisatorische maatregelen zijn genomen om te waarborgen en te kunnen aantonen dat de verwerking plaatsvindt in overeenstemming met de AVG en de Model Verwerkersovereenkomst.

In het kader van het organiseren en aantonen van deze voornoemde maatregelen, maakt Verwerker gebruik van (de meest recente versie van) het in het onderwijs ontwikkelde 'Certificeringsschema informatiebeveiliging en privacy ROSA'[1]. Dat schema voorziet in een baseline van (beveiligings)maatregelen waarmee organisaties dit aantoonbaar kunnen maken. Cito B.V. voldoet conform classificatie aan de normen en uitgangspunten zoals genoemd in het certificeringsschema. De actuele rapportage van het Certificeringsschema voor Cito B.V. is in te zien via http://www.cito.nl/contact/privacyverklaring_website_cito.

Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst

I. Toegang Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

Verwerker hanteert een autorisatiebeleid om te bepalen wie toegang moet hebben tot welke Persoonsgegevens. Medewerkers hebben op grond van deze systematiek geen toegang tot meer data dan strikt noodzakelijk is voor de uitoefening van hun functie. Logische toegang wordt beschermd door een wachtwoordbeleid. Dit beleid wordt technisch afgedwongen. Multifactor authenticatie voor medewerkers maakt hiervan deel uit. Daarnaast hanteert Cito B.V. een streng beleid voor fysieke toegang tot haar kantoor.

Hieronder wordt uitgewerkt welke (groepen) medewerkers van de Verwerker toegang hebben tot welke Persoonsgegevens, inclusief een omschrijving van handelingen die deze medewerkers uit mogen voeren met de Persoonsgegevens.

Medewerkers en gegevens	Handelingen
Medewerkers van Klantenservice hebben toegang tot licentie- en verkoopinformatie. Zij kunnen onder meer zien welke Onderwijsinstelling 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 Onderwijsinstelling bij vragen.

[1] https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa/

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 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. Omschrijving van de maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, Verwerking, toegang of openbaarmaking.

Organisatie van informatiebeveiliging en communicatieprocessen

- Cito B.V. 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 B.V. heeft een proces ingericht en gedocumenteerd voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers (zowel intern als extern) worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Cito B.V. 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 cryptografische 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. Omschrijving van de maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

De systemen van Cito worden periodiek gecontroleerd op veiligheid door een extern bedrijf, dat gespecialiseerd is in cybersecurity. Daarnaast voorziet het beveiligingsbeleid van Cito in interne processen om kwetsbaarheden te identificeren en op te lossen.

IV. Omschrijving van de procedures en processen met betrekking tot vastlegging (logging) van gebeurtenissen die (onregelmatige) gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren.

Handelingen van medewerkers worden gelogd en zijn traceerbaar naar individuele personen. Logging is enkel toegankelijk voor bevoegde personen. Logging wordt regelmatig (geautomatiseerd) gecontroleerd op rechtmatigheid van toegang en gebruik.

Rapportage

Verwerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om Persoonsgegevens te beschermen tegen misbruik via http://www.cito.nl/contact/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.

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 deze bijlage 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 B.V., 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 B.V. 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 Privacybijsluiter opgenomen gegevens.

Cito B.V. 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 daartoe aanleiding geeft, dan kan Cito B.V. 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.

Versie

Deze Beveiligingsbijlage is voor het laatst bijgewerkt op 17 april 2018.