

Bewerkersovereenkomst

Cito B.V.

Inleiding

Deze Bewerkersovereenkomst is een bijlage bij het Convenant Digitale Onderwijsmiddelen en Privacy, versie 2.0 (hierna: het “**Convenant**”) afgesloten tussen de PO-Raad, VO-raad en de brancheorganisaties van educatieve uitgeverij (GEU), distributeurs van leermiddelen (leden van sectie educatief van de Koninklijke Boekverkopersbond) en Cito B.V. (lid van de vereniging van digitale dienstverleners in het onderwijs, VDOD).

De uitgangspunten van deze “**Bewerkersovereenkomst**” sluiten aan bij de bepalingen in het Convenant, de Wet bescherming persoonsgegevens (hierna: Wbp), en de uitgangspunten zoals in jurisprudentie en de toezichthouder de Autoriteit Persoonsgegevens deze in richtsnoeren en uitspraken heeft aangegeven.

De Bewerkersovereenkomst versie 2.0 (juni 2016) is de opvolger van de Bewerkersovereenkomst versie 1.0 die in 2015 in het kader van het Convenant Digitale Onderwijsmiddelen en Privacy, leermiddelen en toetsen is opgesteld en in het najaar van 2015 door Cito in ondertekend. De versie 2.0 ziet naast het gebruik van leermiddelen en toetsen ook op School- en Leerlinginformatiemiddelen. Daarnaast is de overeenkomst op onderdelen bijgesteld naar aanleiding van recente ontwikkelingen in wet- en regelgeving, waaronder de wijziging van de Wbp in verband met de meldplicht datalekken.

De nieuwe Bewerkersovereenkomst versie 2.0 komt in de plaats van de Bewerkersovereenkomst uit 2015.

Deze Bewerkersovereenkomst bevat twee bijlagen:

1. In de Privacy Bijsluiter (Bijlage 1) wordt een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en onder welke doeleinden deze verwerkingen vallen.
2. In de Technische en Organisatorische Maatregelen (Bijlage 2) wordt omschreven welke beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continu punt van aandacht en zorg te blijven.

Informatie over het Convenant en de model Bewerkersovereenkomst is te vinden op de website <http://www.privacyconvenant.nl>. Meer informatie en antwoorden op vragen over privacy en de wettelijke rechten en verplichtingen voor Onderwijsinstellingen zijn te vinden op de websites van de sectorraden PO-Raad en VO-raad en bij Kennisnet.

Partijen:

Het bevoegd gezag van de school, geregistreerd onder een BRIN-nummer bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, hierna te noemen: “**Onderwijsinstelling**”.

en

de besloten vennootschap Cito B.V., gevestigd en kantoorhoudende aan de Amsterdamseweg 13, 6814CM te Arnhem, te dezen rechtsgeldig vertegenwoordigd door Michiel Colenbrander, Manager Business Onderwijs, hierna te noemen: “**Bewerker**”

hierna gezamenlijk te noemen: “**Partijen**”, of afzonderlijk: “**Partij**”

Overwegen het volgende:

- a) Onderwijsinstelling en Bewerker zijn een overeenkomst aangaan waarbij <concrete omschrijving van de door Bewerker in opdracht van Onderwijsinstelling te leveren producten/diensten>, (‘de Product- en Dienstenovereenkomst’). Deze Product- en Dienstenovereenkomst leidt ertoe dat Bewerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
- b) Partijen wensen, mede gelet op het bepaalde in artikel 14 Wet bescherming persoonsgegevens, in deze Bewerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

Komen het volgende overeen:

Artikel 1: Definities

In deze Bewerkersovereenkomst wordt verstaan onder:

- a. Betrokkene, Bewerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, en Verantwoordelijke: de begrippen zoals gedefinieerd in artikel 1 van de Wbp;
- b. Bewerkersovereenkomst: deze Bewerkersovereenkomst, inclusief Bijlagen;
- c. Bijlage: een bijlage bij deze Bewerkersovereenkomst, welke daarvan een onlosmakelijk deel uitmaakt;
- d. Convenant: het Convenant Digitale Onderwijsmiddelen en Privacy;
- e. Datalek: een inbreuk op de beveiliging, zoals bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstig nadelige gevolgen, dan wel ernstig nadelige gevolgen heeft voor de bescherming van persoonsgegevens, zoals bedoeld in artikel 34a, lid 1, Wbp;
- f. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
- g. Leermiddelen en Toetsen: digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens Onderwijsinstellingen;
- h. School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling administratiesysteem, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, een elektronische leeromgeving en een leerling volgsysteem;
- i. Privacy Bijsluiter: de privacy bijsluiter zoals opgenomen in Bijlage 1;
- j. Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Bewerker, zoals omschreven in overweging a;
- k. Model Bewerkersovereenkomst: het model voor een bewerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
- l. Subbewerker: de partij die door Bewerker wordt ingeschakeld als Bewerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Bewerkersovereenkomst en de Product- en Dienstenovereenkomst;
- m. Wbp: Wet bescherming persoonsgegevens.

Artikel 2: Onderwerp en opdracht Bewerkersovereenkomst

1. Deze Bewerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
2. De Onderwijsinstelling verstrekt aan de Bewerker de opdracht tot Verwerking van Persoonsgegevens ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst.

Artikel 3: Rolverdeling

1. Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verantwoordelijke. Bewerker is bewerker in de zin van de Wbp. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het doel en de middelen van de Verwerking van de Persoonsgegevens.
2. Bewerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Bewerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Bewerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie moet de Onderwijsinstelling in staat stellen een keuze te maken met betrekking tot de aangeboden diensten als zodanig, en daarnaast een afzonderlijke keuze te maken voor eventueel aangeboden optionele diensten.
3. De in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, moeten in de Privacy Bijsluiter bij deze Bewerkersovereenkomst in begrijpelijke taal zijn beschreven, waarna de Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en).
4. De Onderwijsinstelling kan verplicht zijn de Verwerking van de Persoonsgegevens te melden bij de Autoriteit Persoonsgegevens. De Onderwijsinstelling onderzoekt of zij hiervan is vrijgesteld en doet melding bij de Autoriteit Persoonsgegevens indien zij hiertoe verplicht is.
5. Onderwijsinstelling en Bewerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de relevante privacywet- en regelgeving mogelijk te maken.

Artikel 4: Privacy convenant

1. Partijen onderschrijven de bepalingen in het Convenant Digitale Onderwijsmiddelen en Privacy.

Artikel 5: Gebruik Persoonsgegevens

1. Bewerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Bewerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (mondeling, schriftelijk dan wel elektronisch) aan Bewerker zijn opgedragen. Deze verplichting geldt zowel gedurende de looptijd van deze overeenkomst als na afloop daarvan.
2. Een overzicht van de categorieën Persoonsgegevens en gebruik waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacy Bijsluiter bij deze Bewerkersovereenkomst.
3. De Bewerker dient in de Privacy Bijsluiter aan te geven of de Privacy Bijsluiter ziet op een Leermiddel en Toets en/of School- en Leerlinginformatiemiddel. Bewerker specificeert in de Privacy Bijsluiter voor welke (in het Convenant opgenomen) doeleinden persoonsgegevens worden verwerkt bij het gebruik zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt. Indien aangegeven in de toelichting in de Privacy Bijsluiter, dient de Bewerker tevens aan te geven onder welke van de in het Convenant omschreven doeleinden bij het gebruik van het product en/of de dienst de Verwerking van Persoonsgegevens plaatsvindt.
4. Bewerker onthoudt zich van verstrekking van Persoonsgegeven aan een Derde, tenzij deze uitwisseling plaatsvindt in opdracht van de Onderwijsinstelling of wanneer dit noodzakelijk is om te voldoen aan een op de Bewerker rustende wettelijke verplichting. In geval van een wettelijke verplichting, verifieert Bewerker voorafgaande de verstrekking de grondslag van het verzoek en de identiteit van de verzoeker. Daarnaast informeert Bewerker de Onderwijsinstelling – indien wettelijk toegestaan - onmiddellijk, zo mogelijk voorafgaand aan de verstrekking.
5. Partijen zullen jaarlijks de Bewerkersovereenkomst, de bijlagen Privacy Bijsluiter(s) en de bijlage Technische en Organisatorische Maatregelen actualiseren met betrekking tot de categorieën Persoonsgegevens, het gebruik daarvan in relatie tot de geleverde toetsproducten en/of diensten en beveiligingsmaatregelen.

Artikel 6: Geheimhouding

1. Bewerker zorgt er voor dat een ieder, waaronder haar werknemers, vertegenwoordigers en/of Subbewerkers, die betrokken zijn bij de Verwerking van de Persoonsgegevens deze gegevens als vertrouwelijk behandelt. Bewerker bewerkstelligt dat voor een ieder die betrokken is bij de Verwerking van de Persoonsgegevens een geheimhoudingsovereenkomst of –beding is gesloten.
2. De in dit artikel bedoelde geheimhoudingsplicht geldt niet voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken, indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Bewerker aan Onderwijsinstelling te verlenen diensten, of indien er een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te verstrekken.

Artikel 7: Beveiliging en controle

1. Bewerker zal, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige Verwerking. Deze maatregelen zullen, met inachtneming van de stand van de techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren, zulks met inachtneming van de risico's die het verwerken van Persoonsgegevens, en de aard daarvan, meebrengen.
2. De maatregelen zoals genoemd in artikel 7.1 omvatten in ieder geval:
 - a. maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Persoonsgegevens die in het kader van de Bewerkersovereenkomst worden verwerkt;
 - b. maatregelen om de Persoonsgegevens te beschermen tegen met name onopzettelijke of onrechtmatige vernietiging, verlies, onopzettelijke wijziging, onbevoegde of onrechtmatige opslag, toegang of openbaarmaking;
 - c. 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;
 - d. een passend informatiebeveiligingsbeleid voor de Verwerking van de Persoonsgegevens.
3. Bewerker zal de door haar getroffen informatiebeveiligingsmaatregelen evalueren en verscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.
4. In Bijlage 2 worden de afspraken tussen Partijen vastgelegd over de technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud en de frequentie van de rapportages die Bewerker aan de Onderwijsinstelling oplevert over de beveiligingsmaatregelen. Deze maatregelen liggen in het verlengde van de beveiligingsmaatregelen die de Onderwijsinstelling moet treffen.
5. De Bewerker stelt de Onderwijsinstelling in staat om te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Bewerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken. Naast rapportages door de Bewerker kan dat aan de hand van, maar niet beperkt tot, een geldige certificering of een gelijkwaardig controle- of bewijsmiddel.
6. In aanvulling op artikel 7, lid 4 heeft de Onderwijsinstelling te allen tijde het recht om, in overleg met de Bewerker en met inachtneming van een redelijke termijn, op eigen kosten, de door Bewerker genomen technische en organisatorische beveiligingsmaatregelen te laten toetsen door een onafhankelijke Register EDP auditor. Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een door Bewerker in te schakelen gecertificeerde en onafhankelijke auditor die een derden-verklaring (TPM) afgeeft. De Onderwijsinstelling wordt geïnformeerd over de uitkomsten van de audit.

Artikel 8: Datalekken

1. Bewerker heeft een passend beleid voor de omgang met Datalekken.
2. Indien Onderwijsinstelling dan wel Bewerker een Datalek vaststelt, dan zal deze de andere Partij onverwijld informeren. Bewerker verstrekt ingeval van een Datalek alle relevante informatie aan Verantwoordelijke met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Bewerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen. Aanvullend informeren Partijen elkaar onverwijld indien blijkt dat de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van Betrokkenen zoals bedoeld in artikel 34a, lid 2, Wbp.
3. Bewerker stelt bij een Datalek de Verantwoordelijke in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek. Bewerker dient hierbij aansluiting te zoeken bij de bestaande processen die Verantwoordelijke daartoe heeft ingericht. Partijen nemen zo spoedig mogelijk alle redelijkerwijs benodigde maatregelen om (verdere) schending of inbreuken betreffende de Verwerking van Persoonsgegevens, en meer in het bijzonder (verdere) schending van de Wbp of andere regelgeving betreffende de Verwerking van de Persoonsgegevens, te voorkomen of te beperken.
4. In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten. Partijen kunnen in onderling overleg bepalen of, en zo ja hoe, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten. Op verzoek van de Onderwijsinstelling kan Bewerker Onderwijsinstelling hierbij bijstaan en adviseren. De Onderwijsinstelling zal de Betrokkenen, indien wettelijk vereist, informeren over een dergelijke inbreuk. Partijen zullen te goeder trouw in onderling overleg afspraken maken over de redelijke verdeling van de eventuele kosten die verbonden zijn aan het voldoen aan de meldingsplichten.
5. Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub e, informeert de Bewerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9: Procedure rechten betrokkenen

1. Een klacht of verzoek van een Betrokkene met betrekking tot de Verwerking van de Persoonsgegevens wordt door de Bewerker onverwijld doorgestuurd naar de Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.
2. Bewerker verleent Onderwijsinstelling – voor zover redelijkerwijs mogelijk - volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Wbp, meer in het bijzonder de rechten van Betrokkenen zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens. Partijen zullen te goeder trouw overleggen over de redelijke verdeling van de eventuele kosten die hiermee gemoeid zijn.

Artikel 10: Verwerking buiten de Europese Economische Ruimte

1. Partijen zien er op toe dat voor zover Persoonsgegevens buiten de Europese Economische Ruimte (verder: EER) worden Verwerkt, dit alleen plaatsvindt conform wettelijke voorschriften, en eventuele verplichtingen die in dit verband op Onderwijsinstellingen rusten. Indien gegevens buiten de EER worden verwerkt wordt dit in Bijlage 1 aangegeven, inclusief een opgave van de landen waar de gegevens worden verwerkt.

Artikel 11: Inschakeling Subbewerker

1. Bewerker kan een Subbewerker inschakelen, van wie de identiteit en vestigingsgegevens zullen worden opgenomen in de Privacy Bijsluiter.
2. Bewerker verplicht iedere Subbewerker contractueel de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen na te leven met betrekking tot de Verwerking van Persoonsgegevens welke verplichtingen en maatregelen minimaal dienen te voldoen aan het bepaalde in deze Bewerkersovereenkomst.
3. Bewerker verplicht iedere Subbewerker contractueel om Persoonsgegevens niet verder te verwerken anders dan in het kader van deze Bewerkersovereenkomst is overeengekomen.

Artikel 12: Bewaartermijnen en vernietiging Persoonsgegevens

1. Onderwijsinstelling zal Bewerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Bewerker. Bewerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen.
2. Onderwijsinstelling verplicht Bewerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Bewerkersovereenkomst te (doen) vernietigen, tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van (wettelijke) verplichtingen, dan wel op verzoek van de Onderwijsinstelling. De Onderwijsinstelling kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden.
3. Bewerker zal Onderwijsinstelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.
4. Bewerker zal alle Subbewerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Bewerkersovereenkomst en zal waarborgen dat alle Subbewerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13: Tegenstrijdigheid en wijziging Bewerkersovereenkomst

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Bewerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, dan zullen de bepalingen van deze Bewerkersovereenkomst leidend zijn.
2. Indien Partijen van de artikelen in de Model Bewerkersovereenkomst door omstandigheden moeten afwijken, of deze willen aanvullen, dan zullen deze wijzigingen en/of aanvullingen door Partijen worden beschreven en gemotiveerd in een overzicht dat als Bijlage 3 aan deze Bewerkersovereenkomst zal worden gehecht. Het bepaalde in dit lid geldt niet voor aanvullingen en/of wijzigingen van de Bijlagen 1 en 2.
3. Bij belangrijke wijzigingen in het product en/of de (aanvullende) diensten die van invloed zijn op de Verwerking van de Persoonsgegevens wordt, alvorens de Onderwijsinstelling de keuze hiertoe aanvaardt, de Onderwijsinstelling in begrijpelijke taal geïnformeerd over de consequenties van deze wijzigingen. Onder belangrijke wijzigingen wordt in ieder geval verstaan: de toevoeging of wijziging van een functionaliteit die leidt tot een uitbreiding ten aanzien van de te Verwerken Persoonsgegevens, de doeleinden waaronder de Persoonsgegevens worden Verwerkt en het inschakelen van een (andere) Subbewerker. De wijzigingen zullen in Bijlage 1 worden opgenomen.
4. Wijzigingen in de artikelen van de Bewerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.
5. In het geval enige bepaling van deze Bewerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Bewerkersovereenkomst volledig van kracht. Partijen zullen in dat geval met elkaar in overleg treden om de nietige, vernietigbare of anderszins niet afdwingbare bepaling te vervangen door een uitvoerbare alternatieve bepaling. Daarbij zullen partijen zoveel mogelijk rekening houden met het doel en de strekking van de nietige, vernietigde of anderszins niet afdwingbare bepaling.

Artikel 14: Duur en beëindiging

1. De looptijd van deze Bewerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.
2. Deze Bewerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Bewerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Bewerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren.