Bewerkersovereenkomst mbo versie 2.0

REGIEGROEP IBP IN HET MBO

Kennisnet SURF saMBO-ICT

IBPDOC18

Verantwoording

Bronnen:

Model bewerkersovereenkomst (met bijlagen), behorend bij het convenant 'Digitale onderwijsmiddelen en privacy' versie 2.0, opgesteld door de PO-Raad, VO-raad, GEU, VDOD en KBb-e, in beheer bij Edu-K (www.edu-k.nl).
Maart/april 2016

Productie:

Kennisnet / saMBO-ICT
Mei 2016 versie 1.0
Mei 2017 versie 2.0

Bewerkers:

Leo Bakker (Kennisnet)
Ludo Cuijpers (Kennisnet en saMBO-ICT)
Axel Eissens (Kennisnet)
Job Vos (Kennisnet)
Mei 2017

Sommige rechten voorbehouden

Inhoudsopgave

1. Inleiding

1.1 Verplichting tot het sluiten van bewerkersovereenkomsten

In het geval dat een onderwijsinstelling persoonsgegevens van onderwijsdeelnemers gebruikt, en daarvoor een leverancier inschakelt, is het College van Bestuur wettelijk verplicht om afspraken te maken met de leverancier wat deze wel en niet mag doen met de gegevens. Daarbij worden er ook afspraken gemaakt over de beveiliging van de gegevens. Deze verplichting is ook opgenomen in:

- Statements 1.13 en 1.15 van het Normenkader informatiebeveiliging, IBPDOC2A;
- Beheersmaatregelen 1.13 en 1.15 Toetsingskader informatiebeveiliging, IBPDOC3;
- Statement P.10 van het Privacy compliance kader, IBPDOC2B;
- Beheersmaatregel P.10 van het Toetsingskader privacy (pluscluster 7), IBPDOC7.

Deze afspraken wordt opgenomen in een contract dat door de Wet bescherming persoonsgegevens (hierna: Wbp) **bewerkersovereenkomst** wordt genoemd. De wet geeft een opsomming welke zaken er in zo'n overeenkomst moeten worden geregeld, er is geen door de overheid of toezichthouder vastgesteld model.

De verantwoordelijke is verplicht om te zorgen dat er een bewerkersovereenkomst wordt afgesloten die voldoet aan de Wbp. Dat neemt niet weg dat een leverancier het initiatief mag en zal nemen om deze bewerkersovereenkomst op te stellen en toe te zenden aan de verantwoordelijke.

1.2 Bewerkersovereenkomst voor het po en vo

Voor het po en vo zijn er in 2014 gesprekken gestart tussen de sectorraden en de brancheorganisaties van leveranciers om afspraken te maken over de omgang met leerlinggegevens. Deze afspraken hebben geresulteerd in een convent 'digitale onderwijsmiddelen en privacy'(hierna: Convenant) dat zich richt op digitaal leermateriaal. In 2016 is dit Convenant uitgebreid met school- en leerlingadministratiesystemen. Het convenant 'Digitale Onderwijsmiddelen en Privacy 2.0' treedt op 6 juni 2016 in werking en wordt door scholen en leveranciers gebruikt. Het is de opvolger van versie 1.0

Om scholen en leverancier te helpen de juiste afspraken te maken, én om in het po en vo op de zelfde manier om te gaan met leerlinggegevens, is er een model bewerkersovereenkomst gemaakt. De uitgangspunten van deze model bewerkersovereenkomst sluiten aan bij de bepalingen in het convenant, de Wbp, en de uitgangspunten zoals in jurisprudentie en de toezichthouder de Autoriteit Persoonsgegevens deze in richtsnoeren en uitspraken heeft aangegeven.

Het gebruik van dit model is verplicht voor alle partijen die aangesloten zijn bij het convenant (versie 1.0 en 2.0). Deze model bewerkersovereenkomst is een bijlage bij het convenant. Afwijken van de tekst van het model is alleen mogelijk op basis van 'past toe of leg uit': een leverancier die andere teksten gebruikt zal, in een bijlage bij de bewerkersovereenkomst, moeten uitleggen waarom de afgesproken tekst niet wordt aangehouden. Gezien het aantal bepalingen dat ofwel wettelijk is voorgeschreven, of waarvan de Autoriteit Persoonsgegevens aangeeft dat deze in de bewerkersovereenkomst moeten worden opgenomen, is de ruimte voor afwijking van de bepalingen in het model beperkt.

Overigens is de afspraak dat de bewerkersovereenkomst een apart document zal zijn: het opnemen van de bepalingen van de bewerkersovereenkomst in bijvoorbeeld de licentievoorwaarden, is niet toegestaan. De rolverdeling is immers anders: de onderwijsinstelling is bij de bewerkersovereenkomst niet een klant, maar de (eind)verantwoordelijke voor de deelnemer gegevens die de leverancier zal gaan gebruiken.

Voor het po en vo is afgesproken dat leveranciers het initiatief zullen nemen om deze bewerkersovereenkomst op te stellen. De onderwijsinstelling zal de bewerkersovereenkomst controleren, en bij akkoord, ondertekenen.

1.3 Bijlagen bij de model bewerkersovereenkomst

De model bewerkersovereenkomst voor het po en vo, 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. De afspraak is dat leveranciers zorgdragen voor het opstellen en invullen van deze privacybijsluiter aangezien zij precies weten wat hun product doet en welke gegevens er worden gebruikt.
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://ww.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, saMBO-ICT en bij Kennisnet.

1.4 Bewerkersovereenkomst voor het mbo

In het mbo bestaat er ook behoefte om op een eenduidige wijze afspraken te maken met leveranciers. Aangezien de MBO Raad niet is aangesloten bij de partijen die het Convenant hebben opgesteld, is er voor gekozen om een apart model voor het mbo te ontwikkelen. Aangezien veel leveranciers van mbo-instellingen ook werkzaam zijn in het vo, is er voor gekozen om de tekst van de model bewerkersovereenkomst voor het po en vo aan te houden. Hiertoe zijn voornamelijk de begrippen van het po- en vo-model aangepast aan de mbo-sector.

De tekst van de model bewerkersovereenkomst voor het mbo is opgenomen in hoofdstuk 2, de bij het model behorende bijlagen zitten in de bijlages bij hoofdstuk 2.

Bij het afsluiten van een bewerkersovereenkomst is het goed om te beseffen dat het College van Bestuur uiteindelijk de bewerkersovereenkomst zal moeten tekenen (deze bevoegdheid mag wel worden gedelegeerd). Dat betekent dat een bewerkersovereenkomst geldt voor alle onderwijsinstellingen en onderwijslocaties die onder dit CvB vallen. Er hoeven dus per locatie geen aparte overeenkomsten te worden gesloten.

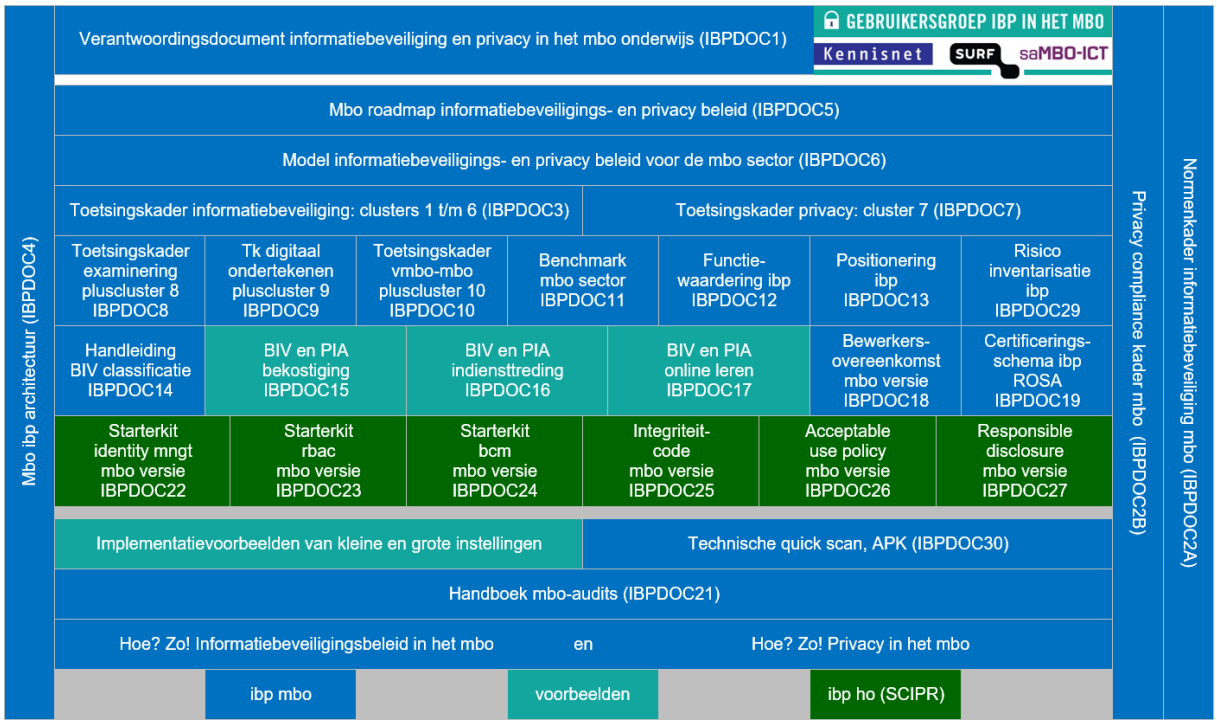
Overigens is er in opdracht van de MBO Raad een project gestart waarbij wordt onderzocht of het mogelijk is om voor de gehele mbo-sector afspraken te maken met leverancier (vergelijkbaar met de afspraken die in het convenant zijn opgenomen). Dat betekent dat deze model bewerkersovereenkomst versie mbo vervangen kan worden door een nieuw, specifiek voor het mbo met de leveranciers afgestemd, model. *Daarom is er in de model bewerkersovereenkomst een nieuw artikel 13 lid 6 opgenomen dat voorziet in de mogelijkheid om de bestaande bewerkersovereenkomst te vervangen door een nieuwe bewerkersovereenkomst als er in de mbo-sector gewerkt zal (gaan) worden met een convenant of een door de sector vastgestelde model bewerkersovereenkomst (vergelijkbaar met de model bewerkersovereenkomst zoals die in de po- en vo-sector wordt gebruikt.*

Overigens is er in het model een verwijzing opgenomen naar het convenant zoals dat geldt voor de po- en vo-sector. Leveranciers en mbo-instellingen kunnen er vrijwillig voor kiezen om zich te conformeren aan het convenant dat in die sectoren geldt. Voor mbo-instellingen die ook een vo-opleiding bieden, geldt dat voor hen (en hun leverancier) het convenant al van toepassing is (en dit artikel kan dus blijven staan).

De integrale tekst van de model bewerkersovereenkomst met bijlagen is opgenomen in hoofdstuk 2. Deze kan (bijvoorbeeld door middel van knippen en plakken) 1-op-1 overgenomen worden.

1.5 Framework informatiebeveiliging en privacy in het mbo

Het gebruik van de model bewerkersovereenkomst past binnen de maatregelen die een onderwijsinstelling moet nemen in het kader van het framework informatiebeveiliging en privacy voor het mbo. Schematisch weergegeven:



2. Model Bewerkersovereenkomst, versie mbo

Partijen:

1. Het bevoegd gezag van **<naam + rechtsvorm onderwijsinstelling>**, geregistreerd onder BRIN-nummer **<brin>** bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, gevestigd en kantoorhoudende aan **<adres>,** te **(<post-code>) <plaats>**, te dezen rechtsgeldig vertegenwoordigd door **<functie + naam>,** hierna te noemen: "**Onderwijsinstelling**".

   EN

2. De besloten vennootschap **<Naam> B.V., gevestigd en kantoorhoudende aan <adres>,** te **(<postcode>) <plaats>**, te dezen rechtsgeldig vertegenwoordigd door **<functie + naam>,** hierna te noemen: "**Bewerker**" .

   Hierna gezamenlijk te noemen: "**Partijen**", of afzonderlijk: "**Partij**"

Overwegen het volgende:

1. Onderwijsinstelling en Bewerker zijn een overeenkomst aangegaan 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.
2. 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:

1.1 Betrokkene, Bewerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, en Verantwoordelijke: de begrippen zoals gedefinieerd in artikel 1 van de Wbp;
1.2 Bewerkersovereenkomst: deze Bewerkersovereenkomst, inclusief Bijlagen;
1.3 Bijlage: een bijlage bij deze Bewerkersovereenkomst, welke daarvan een onlosmakelijk deel uitmaakt;
1.4 Convenant: de meest recente versie van het *Convenant Digitale Onderwijsmiddelen en Privacy*, zoals gepubliceerd op www.privacyconvenant.nl;
1.5 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;
1.6 Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
1.7 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;
1.8 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 (zoals bijvoorbeeld een LAS, LVS, SIS of KRS);
1.9 Privacy Bijsluiter: de privacy bijsluiter zoals opgenomen in Bijlage 1;
1.10 Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Bewerker, zoals omschreven in overweging a;
1.11 Model Bewerkersovereenkomst: het model voor een bewerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;

1.12 Sub bewerker: 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;
1.13 Wbp: Wet bescherming persoonsgegevens.

Artikel 2: Onderwerp en opdracht Bewerkersovereenkomst

1.1 Deze Bewerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
1.2 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

3.1 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.
3.2 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.
3.3 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).
3.4 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.
3.5 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

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

Artikel 5: Gebruik Persoonsgegevens

5.1 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.
5.2 Een overzicht van de categorieën Persoonsgegevens en gebruik waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacy Bijsluiter bij deze Bewerkersovereenkomst.
5.3 De Bewerker dient in de Privacy Bijsluiter aan te geven of de Privacy Bijsluiter toeziet op een Leermiddel en Toets en/of School- en Leerlinginformatiemiddelen. 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.
5.4 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.

[1] Het betreft hier het Convenant Digitale Onderwijsmiddelen en Privacy dat tussen PO Raad, VO Raad en leveranciersorganisaties GEU, KBb-E en VDOD is afgesloten. Dit convenant is nog niet met de MBO Raad afgesloten. Maar een mbo instelling kan het convenant als zodanig wel hanteren.

5.5 *SPECIFIEKE BEPALING IN GEVAL VAN UITWISSELING VAN EEN ONDERWIJSKUNDIG RAPPORT, OVERSTAPDOSSIER OF DIGITAAL ONDERWIJS DOSSIER: In aanvulling op het bepaalde in lid 4, geldt dat indien Bewerker wordt verzocht Persoonsgegevens te verstrekken aan een door Onderwijsinstelling aangewezen en geselecteerde Derde, zijnde een andere onderwijsinstelling, de Bewerker slechts tot die verstrekking zal overgaan nadat deze onderwijsinstelling zijn administratieve onderwijsidentiteit (bijvoorbeeld BRIN of OiN), voor zover hij daarover beschikt, kenbaar heeft gemaakt.*

5.6 *SPECIFIEKE BEPALING IN GEVAL VAN DISTRIBUTIE VAN LEERMIDDELEN: Partijen zullen jaarlijks bij het opstellen van de leermiddelenlijsten voor het eerstvolgende schooljaar, welke leermiddelenlijsten ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst worden opgesteld, de Privacy Bijsluiter aanvullen en/of wijzigen door het opnemen van de categorieën Persoonsgegevens en het gebruik dat van deze Persoonsgegevens wordt gemaakt, met betrekking tot de (digitale) leermiddelen die op de desbetreffende leermiddelenlijsten worden opgenomen.]*

Artikel 6: Geheimhouding

6.1 Bewerker zorgt er voor dat een ieder, waaronder haar werknemers, vertegenwoordigers en/of sub bewerkers, 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.

6.2 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

7.1 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.

7.2 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.

7.3 Bewerker zal de door haar getroffen informatiebeveiligingsmaatregelen evalueren en verscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.

7.4 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.

7.5 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.

7.6 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 derdenverklaring (TPM) afgeeft. De Onderwijsinstelling wordt geïnformeerd over de uitkomsten van de audit.

Artikel 8: Datalekken

8.1 Bewerker heeft een passend beleid voor de omgang met Datalekken.

8.2 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 Betrokken zoals bedoeld in artikel 34a, lid 2, Wbp.

8.3 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 de 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.

8.4 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.

8.5 Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub b, informeert de Bewerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9: Procedure rechten betrokkenen

9.1 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.

9.2 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

10.1 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

11.1 Bewerker kan een Subbewerker inschakelen, van wie de identiteit en vestigingsgegevens zullen worden opgenomen in de Privacy Bijsluiter.

11.2 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.

11.3 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

12.1 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.

12.2 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.

12.3 Bewerker zal Onderwijsinstelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.

12.4 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

13.1 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.

13.2 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 dan 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.

13.3 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.

13.4 Wijzigingen in de artikelen van de Bewerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.

13.5 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.

13.6 Partijen zijn verplicht hun medewerking te verlenen aan het wijzigen of vervangen van deze bewerkersovereenkomst in geval dat:

- Ontwikkelingen in wetgeving of jurisprudentie aanpassing vereisen;
- Er wijzigingen zin in de model bewerkersovereenkomst (IBPDOC18) zoals die is opgenomen in het Framework ibp in het mbo
- Er voor de onderwijsinstellingen in de mbo-sector een afsprakenstelsel of convenant van toepassing is of wordt verklaard waarbij een modelbewerkersovereenkomst hoort

Artikel 14: Duur en beëindiging

14.1 Op deze Bewerkersovereenkomst is Nederlands recht van toepassing.

14.2 De looptijd van deze Bewerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.

14.3 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.

BIJLAGE 1: PRIVACY BIJSLUITER [naam product/dienst]

Onderwijsinstellingen maken in toenemende mate gebruik van digitale toepassingen binnen het onderwijs. Bij het gebruik en levering van deze producten en diensten zijn gegevens nodig die te herleiden zijn tot personen (zoals leerlingen). Onderwijsinstellingen moeten daarom met Bewerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiter geeft onderwijsinstellingen informatie over de dienstverlening die Bewerker verleent en welke persoonsgegevens de Bewerker daarbij verwerkt. Alles bij elkaar eigenlijk over de vraag "wie, wat, waar, waarom en hoe" wordt omgegaan met de privacy van de betrokken personen wiens gegevens worden uitgewisseld.

Het gebruik van deze Privacy Bijsluiter helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld. In het kader van de herkenbaarheid is het wenselijk dat Bewerkers zo veel mogelijk op uniforme wijze gebruik maken van de Privacy Bijsluiter. Afwijkingen van dit model zijn weliswaar mogelijk, maar dienen bij voorkeur beperkt te blijven. Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in separate Bijlage(n), welke als volgt genummerd worden: "Bijlage 1A", "Bijlage 1B", etc.. Deze Bijlagen worden aan de Bewerkersovereenkomst gehecht.

A. Algemene informatie

Naam product en/of dienst	:
Naam Bewerker en vestigingsgegevens	:
Beknopte uitleg en werking product en dienst	:
Link naar leverancier en/of productpagina	:
Doelgroep (zoals PO/VO/MBO, onderbouw/bovenbouw)	:
Gebruikers	: studenten/ouders/verzorgers/docenten

B. De specifieke diensten

Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen

1. Verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst.

a. [….]
b. [….]

2. Omschrijving van de optionele Verwerkingen die de bewerker aanbiedt

Toelichting: Het gaat hier om aanvullende diensten en bijhorende Verwerkingen die geen onlosmakelijk onderdeel vormen van de aangeboden dienst. Dit zijn bijvoorbeeld optionele diensten voor de Onderwijsinstelling die behulpzaam kunnen zijn voor de Onderwijsinstelling t.b.v. het primaire (leer)proces en administratieve werkzaamheden
De Onderwijsinstelling dient een keuze te maken (opdracht te geven) voor het afnemen van deze diensten. Dat kan door de keuze schriftelijk aan te geven in deze bijlage (bijvoorbeeld door het aanvinken van een tick-box☑).
Instemming kan ook plaatsvinden doordat de Onderwijsinstelling in de praktijk de dienst activeert, bijvoorbeeld door een product of dienst aan of uit zetten. De Onderwijsinstelling die op deze wijze de keuze maakt, dient dit op basis van eerder verstrekte informatie (zoals bijvoorbeeld opgenomen in deze bijsluiter) te kunnen doen.

a. [….]
b. [….]
[….]

C. Doeleinden voor het verwerken van gegevens

De Bewerker dient in deze Bijsluiter expliciet aan te geven of deze:

☐ I. leverancier is van een digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen, of
☐ II. (tevens) leverancier is van een School- en Leerlinginformatiemiddel.

Ad I. Indien de Bewerker leverancier is van een digitaal product en/of digitale dienst bestaande uit Leermiddelen en Toetsen, dan zijn de mogelijke doelstellingen van deze producten en diensten uitputtend omschreven in het daarop betrekking hebbende onderdeel van artikel 5 lid 1 van het Convenant Digitale Onderwijsmiddelen en Privacy 2.0. Deze hoeven in deze Bijsluiter verder niet benoemd te worden.

Ad II. (Alleen) indien de bewerker (tevens) leverancier is van een digitaal product en/of digitale dienst bestaande uit een School- en Leerlinginformatiemiddel dan dient in deze Privacy Bijsluiter expliciet te worden aangegeven voor welke doeleinden er Persoonsgegevens worden verwerkt bij het gebruik van het product en/of de dienst. De Bewerker dient hierbij zo veel mogelijk aansluiting te zoeken bij de in artikel 5 lid 2 van het Convenant Digitale Onderwijsmiddelen en Privacy 2.0 opgenomen lijst met doeleinden.

D. Categorieën en soorten persoonsgegevens

Omschrijving en opsomming categorieën Persoonsgegevens die gebruikt worden:
Eventuele optionele Persoonsgegevens (die worden niet standaard gevraagd en opgeslagen):
Soorten van gegevens (zoals bijzondere gegevens, of financiële gegevens):

Functie(groep)	(Categorie) Persoonsgegevens	Type verwerking

E. Algemene informatie over getroffen beveiligingsmaatregelen:

Voor de genomen veiligheidsmaatregelen wordt kortheidshalve verwezen naar Bijlage 2 bij de Bewerkersovereenkomst.
Specifieke beveiligingsmaatregelen voor deze dienst/product [indien van toepassing]:
Eventuele certificeringen:
Audits/derden-verklaringen:
Plaats/Land van opslag en Verwerking van de Persoonsgegevens:

F. Subbewerkers

Bewerker maakt voor dienst/product gebruik van de volgende Subbewerkers:
[partijnaam, beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt Verwerkt door deze Subbewerker]
Plaats/Land van opslag en Verwerking van de Persoonsgegevens (indien de Persoonsgegevens buiten de EER worden verwerkt wordt apart opgave gedaan van de landen waar de Persoonsgegevens worden verwerkt).

Naam organisatie: **<Naam>**
Korte omschrijving dienstverlening: <invullen>
Mate van verwerking Persoonsgegevens: <invullen>
Plaats/Land van verwerking gegevens: <invullen>

Naam organisatie: **<Naam>**
Korte omschrijving dienstverlening: <invullen>

Mate van verwerking Persoonsgegevens: <invullen>
Plaats/Land van verwerking gegevens: <invullen>

G. Contactgegevens

Voor vragen of opmerkingen over deze bijsluiter of de werking van dit product of deze dienst, kunt u terecht bij: [contactgegevens].

H. Versie

[versie nummer en datum laatste aanpassing]

.

BIJLAGE 2: Technische en organisatorische beveiligingsmaatregelen

De Bewerker is overeenkomstig de Wbp en artikel 7 Bewerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens. Deze maatregelen worden in deze bijlage nader (op hoofdlijnen) ingevuld.

Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in separate Bijlage(n), welke als volgt genummerd worden: "Bijlage 2A", "Bijlage 2B", etc.. Deze Bijlagen worden aan de Bewerkersovereenkomst gehecht.

Omschrijving van de maatregelen zoals bedoeld in artikel 7.2 Bewerkersovereenkomst

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

Meer in het bijzonder de uitwerking welke (groepen) medewerkers van de Bewerker toegang hebben tot welke Persoonsgegevens, inclusief een omschrijving van handelingen die deze medewerkers uit mogen voeren met de persoonsgegevens.

a. (groepen van) medewerkers die toegang hebben tot welke Persoonsgegevens:

b. handelingen die deze medewerkers uitvoeren met de Persoonsgegevens:

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.

Meer in het bijzonder de uitwerking van de door Bewerker getroffen technische en organisatorische (beveiligings-)maatregelen en de daarbij gehanteerde beveiligingsnorm.

[beschrijving beveiliging applicatie/platform]

[beschrijving wijze van identificatie/authenticatie/autorisatie en beveiliging daarvan]

[beschrijving beveiliging van wijze van uitwisseling/transport van gegevens]

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.

[zoals een periodieke analyse van (security) incidenten, het periodiek uitvoeren van een extern/intern kwetsbaarhedenonderzoek (ethical hack) of het periodiek uitvoeren van controles op beveiliging van systemen]

Rapportage (artikel 7.4 van de Bewerkersovereenkomst

Bewerker rapporteert periodiek met een frequentie van […] maal per jaar, uiterlijk op […] aan Verantwoordelijke over de door Bewerker genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin. Beveiligingsincidenten en datalekken wordt door Bewerker direct gemeld aan de contactpersoon van de Onderwijsinstelling.

[contactgegevens helpdesk/servicedesk voor beveiligingsincidenten]

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

Afspraken over het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging, met name over

- De wijze waarop monitoring en identificatie van incidenten plaatsvindt,
- De wijze waarop informatie wordt gedeeld:
  - Op welke manier (via e-mail, telefoon);
  - Aan wie gericht (contactpersonen en contactgegevens);
  - Met wie kan (bij vervolgacties) contact worden opgenomen.
- Informatie die in ieder geval over een incident gedeeld moet worden
  - 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).
- Eventuele afspraken of, en zo ja hoe, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie

[versie nummer en datum laatste aanpassing]

3. Varianten model bewerkersovereenkomst versie mbo

Mogelijk bestaat de behoefte om af te wijken van de model bewerkersovereenkomst. Indien er geen samenhang is met producten of diensten gericht op de po- en vo-sector, kan er voor gekozen worden om in overleg met de leverancier af te wijken van de model bewerkersovereenkomst versie mbo.

3.1 Afwijking artikel 4 (toepasselijkheid convenant)

Tot het moment dat daar meer duidelijkheid over is, kunnen onderwijsinstellingen en leveranciers er voor kiezen om de bepalingen van het Convenant voor het po en vo vrijwillig na te komen. Dat wordt geregeld in artikel 4 van de model bewerkersovereenkomst versie mbo. Zeker voor mbo-instellingen die ook een vo-onderwijs bieden, zal dit vanzelfspreken zijn omdat vo-instellingen en vo-leveranciers gebonden zijn aan het Convenant. Er kan desalniettemin voor gekozen worden om artikel 4 niet van toepassing te verklaren en uit de bewerkersovereenkomst te verwijderen.

3.2 Afwijking artikel 7.6 (toetsing beveiligingsmaatregelen)

Mogelijk bestaat de behoefte voor de onderwijsinstelling om afspraken te maken over toetsing van de beveiligingsmaatregelen die de leverancier heeft genomen. In het kader van standaardisering van afspraken rondom beveiliging, wordt er binnen Edustandaard gesproken over een baseline informatiebeveiliging. Dit is uitgewerkt in het certificeringsschema (voor meer toelichting: https://www.edustandaard.nl/standaarden/afspraken/afspraak/certificeringsschema-rosa-1/2.0/)

In het geval dat de onderwijsinstelling zelf afspraken wenst te maken over toetsing van de door de leverancier genomen maatregelen, kan artikel 7.6 vervallen en worden vervangen worden door de volgende toevoegingen:

7.6 Bewerker is verplicht periodiek of op verzoek een door haar aan te wijzen onafhankelijke IT-auditor of deskundige een onderzoek te laten uitvoeren ten aanzien van de organisatie van Bewerker, teneinde te doen vaststellen dat Bewerker aan het bepaalde met betrekking tot de bescherming van de vertrouwelijkheid, integriteit, beschikbaarheid en beveiliging van Persoonsgegevens en vertrouwelijke gegevens zoals omschreven in de Overeenkomst en Bewerkersovereenkomst voldoet. De frequentie van het onderzoek is een keer per twee jaar met uitzondering van Verwerkingen met een hoog risico waarbij een jaarlijks onderzoek van Bewerker gevraagd wordt. Er is in ieder geval sprake van een hoog risico indien Bijzondere persoonsgegevens in de zin van de Wbp worden verwerkt. Indien er enkel publieke Persoonsgegevens worden verwerkt, is er sprake van een laag risico en geldt er geen verplichting tot het doen van een periodiek onderzoek.

7.7 Bewerker is verplicht de bevindingen van de IT-auditor of deskundige, in de vorm van een Third Party Memorandum, na een verzoek ter zake aan Verantwoordelijke ter beschikking te stellen.

7.8 Bewerker verzorgt een regelmatige, minimaal eenmaal per kwartaal na aanvang van de opvolgende kalendermaand, een rapportage over beveiligingsbeheer waarbij minimaal de volgende onderdelen zijn opgenomen:

- *Aantal, status, voortgang en analyse van incidenten;*
- *Maatregelen genomen op het gebied van beveiligingsbeheer naar aanleiding van incidenten;*
- *Algemene maatregelen genomen op het gebied van gegevensbeveiliging.*

7.9 De kosten van de periodieke audit komen voor rekening van de Bewerker. De kosten van de audit op verzoek komen voor rekening van de Verantwoordelijke, tenzij uit de bevindingen van de audit blijkt dat de Bewerker de bepalingen uit de Bewerkersovereenkomst niet is nagekomen. In dat geval komen de kosten voor rekening van Bewerker. Deze bepaling laat de overige rechten van de Verantwoordelijke, waaronder die op schadevergoeding, onverlet.

7.10 Wanneer tijdens een audit wordt vastgesteld dat Bewerker niet aan het bepaalde in de Overeenkomst en de Bewerkersovereenkomst voldoet, zal Bewerker alle redelijkerwijs noodzakelijke maatregelen nemen om te zorgen dat zij hieraan alsnog voldoet.