Zermelo Verwerkersovereenkomst 3.0

Dit document bevat:

- De modelovereenkomst zoals opgesteld vanuit het privacyconvenant
- Bijlage 1: Privacybijsluiter
- Bijlage 2: Beveiligingsbijlage
- Bijlage 2b: Certificeringsschema ROSA
- Bijlage 3: Afwijkingen van de modelovereenkomst

Deze overeenkomst is afgesloten op: <datum + tijd van afsluiten> door <functie + naam>, <naam + rechtsvorm onderwijsinstelling>

Modelovereenkomst

Deze Model Verwerkersovereenkomst is een bijlage bij het *Convenant Digitale Onderwijsmiddelen en Privacy* (hierna: het Convenant).

> Dit is de ongewijzigde tekst van de modelovereenkomst. Bijlage 3 bevat de punten waarop Zermelo afwijkt van het model.

De nieuwe Model Verwerkersovereenkomst 3.0 komt in de plaats van eerdere Model verwerkersovereenkomsten uit 2015 en 2016. De uitgangspunten van deze Model Verwerkersovereenkomst 3.0 sluiten aan bij de bepalingen in het Convenant, geven invulling aan verplichtingen op grond van de Europese Algemene Verordening Gegevensbescherming (hierna: AVG), en de uitgangspunten zoals onder andere in (inter) nationale beveiligingsnormen, jurisprudentie en richtsnoeren van de toezichthouder zijn aangegeven.

Reeds afgesloten Verwerkersovereenkomsten op basis van de modellen uit 2015 en 2016 blijven hun gelding houden totdat deze verwerkersovereenkomsten door partijen worden beëindigd. Het uitgangspunt is dat met ingang van 25 mei 2018, het moment waarop de AVG van toepassing wordt, Onderwijsinstellingen en Leveranciers bij het aangaan van een verwerkersovereenkomst of bij vernieuwing van een bestaande verwerkersovereenkomst, de Model Verwerkersovereenkomst 3.0. gebruiken.

In het Convenant is afgesproken dat Onderwijsinstellingen en Leveranciers het actuele model gebruiken bij het maken van afspraken. Van de actuele Model Verwerkersovereenkomst kan alleen gemotiveerd en schriftelijk worden afgeweken.
Deze Model Verwerkersovereenkomst 3.0 bevat twee bijlagen:

1. In de Privacybijsluiter (Bijlage 1) wordt met name een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en voor welke doeleinden.
2. In de Beveiligingsbijlage (Bijlage 2) wordt omschreven welke technische en organisatorische beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continu punt van aandacht en zorg te blijven

Informatie over het Convenant en de model Verwerkersovereenkomst is te vinden op de website 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, VO-raad, MBO Raad (saMBO-ICT) en bij Kennisnet.

Maart 2018

Partijen:

1. Het bevoegd gezag van <naam + rechtsvorm onderwijsinstelling>, geregistreerd onder BRIN-nummer(s) <brin> bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, gevestigd en kantoorhoudende aan <adres>, te (<postcode>) <plaats>, te dezen rechtsgeldig vertegenwoordigd door <functie + naam>, hierna te noemen: "**Onderwijsinstelling**".
   en
2. De besloten vennootschap Zermelo Software B.V., gevestigd en kantoorhoudende aan Schuttersveld 9, te Leiden, te dezen rechtsgeldig vertegenwoordigd door G.C.M. van Rijn, directie, hierna te noemen: "**Verwerker**"

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

Overwegen het volgende:

1. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij Verwerker (rooster)software ter beschikking stelt en/of werkzaamheden verricht op het gebied van roosters en schoolorganisatie, ('de Product- en Dienstenovereenkomst'). Deze Product- en Dienstenovereenkomst leidt ertoe dat Verwerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
2. Partijen wensen, mede gelet op het bepaalde in artikel 28 lid 3 Algemene Verordening Gegevensbescherming, in deze Verwerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

Komen het volgende overeen:

Artikel 1: Definities

In deze Verwerkersovereenkomst wordt verstaan onder:

1. Betrokkene, Verwerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens en Verwerkingsverantwoordelijke: de begrippen zoals gedefinieerd in de AVG;
2. Bijlage(n): bijlage(n) bij het Convenant of de Verwerkersovereenkomst;
3. Convenant: het Convenant Digitale Onderwijsmiddelen en Privacy 3.0;
4. Convenantpartij: een tot het Convenant toegetreden Onderwijsinstelling of Leverancier;
5. Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG;
6. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
7. Initiatiefnemers: partijen die de initiatiefnemers zijn van het Convenant als opgenomen in de aanhef van het Convenant;
8. Instructies: geschreven of elektronisch gestuurde aanwijzing van de Verwerkingsverantwoordelijke aan de Verwerker in het kader van haar bevoegdheden zoals geformuleerd in deze Verwerkersovereenkomst of in de Product- en Dienstenovereenkomst. Instructies worden verstrekt door en aan de contactpersonen van partijen zoals die zijn opgenomen in de Bijlage(n);
9. Keten iD: een pseudoniem van een persoonsgebonden nummer van een Onderwijsdeelnemer dat de Onderwijsdeelnemer niet langer direct identificeerbaar maakt. Hierna wordt dat pseudoniem opnieuw versleuteld tot het Keten iD, dat voor identificatiedoeleinden gebruikt wordt voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen. Het Keten iD wordt ook ECK iD genoemd;
10. 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;
11. Leverancier: leverancier van een Digitaal Onderwijsmiddel, zoals een distributeur, uitgever of leverancier van een administratiesysteem;
12. Model Verwerkersovereenkomst: het model voor een verwerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
13. Onderwijsdeelnemer: onderwijsdeelnemer in het primair onderwijs, voortgezet onderwijs of middelbaar beroepsonderwijs;
14. Platform: het platform als bedoeld in artikel 8 van het Convenant, thans bekend als Edu-K;
15. Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Verwerker, zoals omschreven in overweging a met inbegrip van een op basis van die overeenkomst gesloten overeenkomst tussen een Onderwijsdeelnemer en Leverancier voor het betreffende product of dienst;
16. Privacybijsluiter: één of meerdere privacybijsluiter(s) zoals opgenomen in de Bijlage(n) die van toepassing zijn op de aangeboden Digitale Onderwijsmiddelen;
17. Reglement: het reglement als bedoeld in artikel 8 lid 4 van het Convenant;
18. School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling-administratiesysteem, kernregistratiesysteem, studentinformatiesysteem, deelnemersadministratie, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, dashboards en kwaliteitsmanagementsystemen voor zover zij Persoonsgegevens van Onderwijsdeelnemers bevatten, een elektronische leeromgeving en een leerling volgsysteem;
19. Standaardattributenset: de door het Platform vastgestelde aanvullende gestandaardiseerde Persoonsgegevens van Onderwijsdeelnemers die naast het Keten iD gebruikt kunnen worden voor de toegang tot en het gebruik van Digitale Onderwijsmiddelen (zoals gepubliceerd op de website van het Platform);
20. Subverwerker: de partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van de Model Verwerkersovereenkomst en de Product- en Dienstenovereenkomst;
21. AVG: de Algemene Verordening Gegevensbescherming (Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG);
22. Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke (Unierechtelijke en lidstaatrechtelijke) wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

Artikel 2: Onderwerp en opdracht Verwerkersovereenkomst

1. Deze Verwerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
2. De Onderwijsinstelling geeft Verwerker conform artikel 28 AVG opdracht en Instructies om Persoonsgegevens te verwerken namens de Onderwijsinstelling. De Instructies van de Onderwijsinstelling kunnen onder meer nader omschreven zijn in deze Verwerkersovereenkomst en de Product- en Dienstenovereenkomst.
3. De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen zoals opgenomen in Bijlage 1, die plaatsvinden ter uitvoering van de Product- en Dienstenovereenkomst. Verwerker brengt Onderwijsinstelling onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

Artikel 3: Rolverdeling

1. Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verwerkingsverantwoordelijke. Verwerker is Verwerker in de zin van de AVG. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het (het bepalen van) doel en de middelen van de Verwerking van de Persoonsgegevens.

2. Verwerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Verwerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Verwerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie stelt de Onderwijsinstelling in staat om te doorgronden welke Verwerkingen onlosmakelijk zijn verbonden met een aangeboden dienst en voor welke Verwerkingen Onderwijsinstelling een keuze kan maken voor eventueel aangeboden optionele diensten.
3. Onverminderd hetgeen elders in deze Verwerkersovereenkomst is bepaald, informeert Verwerker voorafgaand aan het sluiten van deze Verwerkersovereenkomst de Onderwijsinstelling in Bijlage 1 over de in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, en de Verwerkingen die in dat kader plaatsvinden. De in Bijlage 1 opgenomen informatie moet in begrijpelijke taal zijn beschreven, waardoor Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en) en de uitvoering van de bijbehorende Verwerkingen.
4. De Onderwijsinstelling neemt de in lid 2 van dit artikel genoemde Verwerking van de Persoonsgegevens op in een register van de verwerkingsactiviteiten Zie voor een voorbeeld de Aanpak IBP bij https://kn.nu/IBPonderwijs die onder hun verantwoordelijkheid plaatsvinden.
5. Voor zover artikel 30 lid 5 AVG daartoe verplicht, houdt Verwerker conform artikel 30, lid 2 AVG een register bij van alle categorieën van verwerkingsactiviteiten die Verwerker ten behoeve van een Onderwijsinstelling verricht.
6. Onderwijsinstelling en Verwerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens mogelijk te maken.

Artikel 4: Privacyconvenant

1. Partijen onderschrijven de bepalingen in het Convenant.

Artikel 5: Gebruik Persoonsgegevens

1. Verwerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en conform de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Verwerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (schriftelijk dan wel elektronisch) aan Verwerker in het kader van de uitvoering van de Product- en Dienstenovereenkomst zijn opgedragen, behoudens een eventuele afwijkende Unierechtelijke of lidstaatrechtelijke bepaling, dan wel een rechterlijke uitspraak, voor zover daartegen geen beroep meer openstaat. In dat geval stelt Verwerker de Onderwijsinstelling voorafgaand aan de Verwerking van dat wettelijke voorschrift dan wel de rechterlijke uitspraak in kennis, tenzij dergelijke kennisgeving om gewichtige redenen van algemeen belang verboden is.
2. Een overzicht van onder meer de categorieën Persoonsgegevens en het doel waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacybijsluiter bij deze Verwerkersovereenkomst.
3. De Verwerker dient in de Privacybijsluiter aan te geven of de Privacybijsluiter ziet op een Leermiddel en Toets en/of een School- en Leerlinginformatiemiddel. Verwerker specificeert in de Privacybijsluiter voor welke, door de Verwerkersverantwoordelijke vastgestelde, doeleinden persoonsgegevens worden verwerkt bij het gebruik zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt
4. Indien Verwerker in strijd met de AVG het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker met betrekking tot die Verwerking als Verwerkingsverantwoordelijke beschouwd.
5. *SPECIFIEKE BEPALING IN GEVAL VAN UITWISSELING VAN HET ONDERWIJSKUNDIG RAPPORT: In aanvulling op het bepaalde in lid 4, is het Verwerker uitsluitend toegestaan om Persoonsgegevens te verstrekken aan een door Onderwijsinstelling aangewezen en geselecteerde andere onderwijsinstelling, na een concreet verzoek tot verstrekking van die onderwijsinstelling en op voorwaarde dat deze andere onderwijsinstelling haar administratieve onderwijsidentiteit (bijv. BRIN of OiN) aan Verwerker kenbaar heeft gemaakt. Indien de andere onderwijsinstelling niet beschikt over een administratieve onderwijsidentiteit zal Verwerker Persoonsgegevens alleen aan die andere onderwijsinstelling verstrekken op uitdrukkelijke instructie van Onderwijsinstelling.*
6. *SPECIFIEKE BEPALING VOOR VERWERKERSOVEREENKOMSTEN TUSSEN ONDERWIJSINSTELLINGEN EN DISTRIBUTEURS:*
    1. *Convenantspartijen die Leermiddelen en Toetsen ontwikkelen en aanbieden (hierna te noemen: **Leermiddelenleverancier**), zullen jaarlijks ten behoeve van 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 voor die Leermiddelen en Toetsen aanvullen en/of wijzigen door het opnemen van de categorieën Persoonsgegevens en het gebruik dat van deze Persoonsgegevens wordt gemaakt (met betrekking tot de Leermiddelen en Toetsen die op de desbetreffende leermiddelenlijsten worden opgenomen).*
    2. *Verwerker (de distributeur) wisselt in opdracht van de Onderwijsinstelling gegevens uit met deze Leermiddelenleveranciers.*
    3. *De Onderwijsinstelling is verantwoordelijk voor het maken en vastleggen van afspraken met iedere Leermiddelenleverancier in een Verwerkersovereenkomst.*
    4. *Onderwijsinstelling vrijwaart Verwerker (distributeur) voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Leermiddelenleverancier, en de Onderwijsinstelling vrijwaart de Leermiddelenleverancier voor eventuele aanspraken van derden ten gevolge van het niet (tijdig) maken van Verwerkersafspraken met Verwerker (distributeur).*
    5. *De verantwoordelijkheid van Verwerker (distributeur) voor het beheer van de Persoonsgegevens houdt op, op het moment dat de Leermiddelenleverancier die gegevens heeft ontvangen van Verwerker (distributeur).*

Artikel 6: Vertrouwelijkheid

1. Verwerker garandeert dat hij alle Persoonsgegevens strikt vertrouwelijk zal behandelen ten opzichte van derden, waaronder overheidsinstanties. Verwerker zorgt er voor dat een ieder die hij betrekt bij de Verwerking van Persoonsgegevens, waaronder zijn

werknemers, vertegenwoordigers en/of Subverwerkers, deze gegevens als vertrouwelijk behandelt. Verwerker waarborgt dat met de tot het Verwerken van de Persoonsgegevens geautoriseerde personen een geheimhoudingsovereenkomst of –beding is gesloten, of dat deze door een wettelijke verplichting tot geheimhouding zijn gebonden.
2. De in lid 1 bedoelde geheimhoudingsplicht geldt niet in de hierna genoemde gevallen:
    1. voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken;
    2. indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Verwerker aan Onderwijsinstelling te verlenen diensten; of
    3. indien Verwerker op grond van een Unierechtelijke of lidstaatrechtelijke bepaling dan wel een gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, tot verstrekking verplicht is.
3. Verwerker onthoudt zich van verstrekking of bekendmaking van Persoonsgegeven aan een Derde, tenzij deze verstrekking of bekendmaking plaatsvindt in opdracht van Onderwijsinstelling respectievelijk wanneer dit noodzakelijk is om te voldoen aan een gerechtelijke uitspraak, voor zover daartegen geen beroep meer openstaat, of een op de Verwerker rustende wettelijke verplichting. Onder wettelijke verplichtingen zijn begrepen Unierechtelijke of lidstaatrechtelijke bepalingen op grond waarvan Verwerker tot verstrekken verplicht is. In geval van een wettelijke verplichting, verifieert Verwerker voorafgaand aan de verstrekking de wettelijke grondslag en de identiteit van de partij die zich daarop beroept. Daarnaast stelt Verwerker - tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt - Onderwijsinstelling onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, in kennis van de voor Onderwijsinstelling relevante informatie inzake deze verstrekking.
4. Verwerker zorgt er voor dat de onder diens gezag werkende medewerkers uitsluitend toegang hebben tot Persoonsgegevens voor zover noodzakelijk voor de vervulling van hun werkzaamheden.

Artikel 7: Beveiliging en controle

1. Met inachtneming van het bepaalde in artikel 32 AVG zal Verwerker, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen en beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
2. Naast de maatregelen als genoemd in artikel 32 lid 1 AVG, worden onder meer de volgende maatregelen - waar passend - genomen:
    1. een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens;
    2. maatregelen om te waarborgen dat enkel geautoriseerde medewerkers toegang hebben tot de Persoonsgegevens die in het kader van de Verwerkersovereenkomst worden verwerkt;
    3. het regelen van procedures rondom het verlenen van toegang tot Persoonsgegevens (waaronder een registratie- en afmeldprocedure voor toewijzing van toegangsrechten), en het in logbestanden vastleggen van gebeurtenissen betreffende gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen (vergelijkbaar met de toepasselijke ISO-normering, en/of vergelijkbaar met het geldende Certificeringsschema informatiebeveiliging en privacy ROSA). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren.
3. Partijen zullen de door haar getroffen beveiligingsmaatregelen periodiek evalueren en aanscherpen, 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 passende technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud, vorm en de werkwijze van de verklaringen die Verwerker verstrekt over de afgesproken beveiligingsmaatregelen.
5. De Verwerker stelt in goed overleg de Onderwijsinstelling in staat om effectief te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Verwerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken.
6. In aanvulling op de voorgaande leden heeft Onderwijsinstelling te allen tijde het recht om, in overleg met de Verwerker en met inachtneming van een redelijke termijn, de naleving van Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, de Product- en Dienstenovereenkomst en deze Verwerkersovereenkomst, waaronder de door Verwerker genomen technische en organisatorische beveiligingsmaatregelen, te (doen) controleren middels een audit uitgevoerd door een onafhankelijke gecertificeerde externe deskundige:
    1. Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een door Verwerker, in overleg met Onderwijsinstelling, in te schakelen externe deskundige die een derden-verklaring (TPM) afgeeft.
    2. De auditor verstrekt het auditrapport alleen aan Partijen.
    3. Partijen maken onderling afspraken over de omgang met de uitkomsten van de audit.
    4. Partijen kunnen in onderling overleg afspreken dat, aan de hand van een geldige (inter)nationaal erkende certificering of een gelijkwaardig controle- of bewijsmiddel, een reeds uitgevoerde audit en daaruit afgegeven derden-verklaring gebruikt kan worden. Onderwijsinstelling wordt in dat geval geïnformeerd over de uitkomsten van de audit.
    5. Partijen komen overeen dat de kosten van deze audit voor rekening komen van de Onderwijsinstelling, tenzij uit de audit (grote) gebreken blijken, die aan Verwerker kunnen worden toegerekend. In dat geval treden partijen in overleg over de verdeling van de kosten van de audit.

Artikel 8: Datalekken

1. Partijen hebben een passend beleid voor de omgang met Datalekken.
2. Indien Onderwijsinstelling of Verwerker een Datalek vaststelt, dan zal deze de andere Partij daarover *zonder onredelijke vertraging* informeren zodra hij kennis heeft genomen van dat Datalek. Verwerker verstrekt ingeval van een Datalek alle relevante informatie aan Onderwijsinstelling met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Verwerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen.
3. Verwerker informeert Onderwijsinstelling *onverwijld* indien een vermoeden bestaat dat een Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen zoals bedoeld in artikel 34,lid 1, AVG.
4. Verwerker stelt bij een Datalek de Onderwijsinstelling in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek. Verwerker dient hierbij aansluiting te zoeken bij de bestaande processen die Onderwijsinstelling 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 Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, te voorkomen of te beperken.
5. In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten. In geval een Datalek bij Verwerker meerdere Onderwijsinstellingen in gelijke mate treft, kan Verwerker, na overleg met een of meerdere Verwerkingsverantwoordelijken, namens de Onderwijsinstellingen een melding doen van het Datalek aan de Autoriteit Persoonsgegevens. Van het voornemen hiervan zal Verwerker Onderwijsinstelling onverwijld (en zo mogelijk voorafgaand aan de melding) in kennis stellen.
6. In geval van het Datalek waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zal de Onderwijsinstelling de Betrokkenen informeren over het Datalek.
7. 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. Partijen documenteren alle Datalekken in een (incidenten)register, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen.
9. Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub e van deze Verwerkersovereenkomst, informeert de Verwerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9 Bijstand

1. Verwerker verleent Onderwijsinstelling bijstand bij het doen nakomen van de op Onderwijsinstelling rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zoals met betrekking - maar niet beperkt - tot:
    1. het - voor zover redelijkerwijs mogelijk - vervullen van de plicht van Onderwijsinstelling om aan verzoeken van de in hoofdstuk III van de AVG vastgelegde rechten van de betrokkene binnen de wettelijke termijnen te voldoen, zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens;
    2. het uitvoeren van controles en audits zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst;
    3. het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortkomende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
    4. het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie;
    5. het voorbereiden, beoordelen en melden van datalekken zoals bedoeld in artikel 8 van deze Verwerkersovereenkomst.
2. Een klacht of verzoek van een Betrokkene of een verzoek of onderzoek van de Autoriteit Persoonsgegevens met betrekking tot de Verwerking van de Persoonsgegevens, wordt door de Verwerker, voor zover wettelijk is toegestaan, onverwijld doorgestuurd naar Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.
3. Partijen brengen elkaar voor in redelijkheid verleende bijstand geen kosten in rekening. In het geval dat één van de Partijen kosten in rekening wil brengen, brengt deze partij de andere partij hiervan vooraf op de hoogte.

Artikel 10: Doorgifte aan derde landen buiten de Europese Economische Ruimte

1. Verwerker is uitsluitend gerechtigd tot doorgifte van Persoonsgegevens aan een derde land of internationale organisatie indien Onderwijsinstelling daarvoor specifieke Schriftelijke toestemming heeft gegeven, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Onderwijsinstelling voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.
2. Indien na toestemming van Onderwijsinstelling Persoonsgegevens worden doorgegeven aan derde landen buiten de Europese Economische Ruimte of aan een internationale organisatie zoals bedoeld in artikel 4 lid 26 AVG, dan zien Partijen er op toe dat dit alleen plaatsvindt conform wettelijke voorschriften en eventuele verplichtingen die in dit verband op Onderwijsinstelling rusten. Indien gegevens worden doorgegeven aan een derde land of een internationale organisatie, dan wordt dit in Bijlage 1 bij deze Verwerkers-overeenkomst aangegeven, inclusief een opgave van de landen waar, of internationale organisaties door wie, de Persoonsgegevens worden verwerkt. Daarbij wordt tevens aangegeven op welke wijze is voldaan aan de voorwaarden op basis van de AVG voor doorgifte van Persoonsgegevens aan derde landen of internationale organisaties.

Artikel 11: Inschakeling Subverwerker

1. Onderwijsinstelling geeft Verwerker door ondertekening van deze Verwerkers-overeenkomst toestemming tot het inschakelen van Subverwerkers, van wie de identiteit en vestigingsgegevens zijn opgenomen in de Privacybijsluiter.
2. Tijdens de duur van de Verwerkersovereenkomst licht Verwerker Onderwijsinstelling in over een voorgenomen toevoeging van een nieuwe Subverwerker of wijziging in de samenstelling van de bestaande Subverwerkers, waarbij Onderwijsinstelling de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken.
3. Verwerker is verplicht iedere Subverwerker via een overeenkomst of andere rechtshandeling minimaal dezelfde verplichtingen inzake gegevensbescherming op te leggen als in deze Verwerkersovereenkomst aan Verwerker zijn opgelegd. Hieronder vallen onder meer de verplichting om de Persoonsgegevens niet verder te Verwerken anders dan in het kader van deze Verwerkersovereenkomst is overeengekomen, en de verplichting tot het nakomen van de geheimhoudingsverplichtingen, meldingsverplichtingen, medewerkingsverplichtingen en beveiligingsmaatregelen met betrekking tot de Verwerking van Persoonsgegevens zoals in deze Verwerkersovereenkomst vastgelegd. Verwerker zal op verzoek van Onderwijsinstelling afschriften verstrekken van deze Verwerkers-

overeenkomsten, of van de relevante passages uit de Verwerkersovereenkomst of een andere overeenkomst of een andere bindende rechtshandeling tussen Verwerker en de door deze overeenkomstig artikel 11, lid 1, van deze overeenkomst ingeschakelde Subverwerker.

Artikel 12: Bewaartermijnen en vernietiging Persoonsgegevens

1. Onderwijsinstelling zal Verwerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Verwerker. Verwerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen.
2. Onderwijsinstelling verplicht Verwerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Verwerkersovereenkomst 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. Verwerker zal Onderwijsinstelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.
4. Verwerker zal alle Subverwerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Verwerkers-overeenkomst en zal waarborgen dat alle Subverwerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13: Aansprakelijkheid

1. Een Partij kan geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Product- of Dienstenovereenkomst of andere tussen Partijen bestaande overeenkomst of regeling, ten aanzien van een door de andere Partij ingestelde:
    1. verhaalsactie op grond van artikel 82 AVG; of
    2. schadevergoedingsactie uit hoofde van deze Verwerkersovereenkomst, indien en voor zover de actie bestaat uit verhaal van een aan de Toezichthouder betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij.

   Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken partij op grond van de geldende wet- of regelgeving ter beschikking staat.
2. Het bepaalde in lid 1 sub b geldt onverminderd het bepaalde in artikel 14 lid 2.
3. Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Toezichthouder, beiden in verband met deze Verwerkersovereenkomst. Iedere Partij is in redelijkheid verplicht de andere Partij informatie te verstrekken en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling of boete, zoals bedoeld in de vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij, Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten.

Artikel 14: Tegenstrijdigheid en wijziging Verwerkersovereenkomst

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, dan zullen de bepalingen van deze Verwerkersovereenkomst leidend zijn.
2. Indien Partijen van de artikelen in de Model Verwerkersovereenkomst 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 Verwerkersovereenkomst 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 en de doeleinden waaronder de Persoonsgegevens worden Verwerkt. De wijzigingen zullen in Bijlage 1 worden opgenomen.
4. Wijzigingen in de artikelen van de Verwerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.
5. In het geval enige bepaling van deze Verwerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Verwerkersovereenkomst 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 15: Duur en beëindiging

1. De looptijd van deze Verwerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.
2. Deze Verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Verwerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Verwerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren, waaronder in ieder geval artikel 5, lid 1, en de artikelen 6, 9 en 12.

Bijlage 1: Privacybijsluiter

BRANCHEMODEL VDOD Privacy Bijsluiter (v. 2.0)

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 onderwijsdeelnemers). Onderwijsinstellingen moeten met Verwerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiter geeft onderwijsinstellingen informatie over de dienstverlening die Verwerker verleent en welke Persoonsgegevens de Verwerker daarbij Verwerkt. Alles bij elkaar eigenlijk over de vraag "wie, wat, waar, waarom en hoe" wordt omgegaan met de privacy van de betrokken personen van wie Persoonsgegevens worden Verwerkt.

Het gebruik van deze Privacybijsluiter helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld.

A. Algemene informatie

Naam product en/of dienst	Zermelo
Naam Verwerker en vestigingsgegevens	Zermelo Software B.V. Schuttersveld 9 2316 XG Leiden E-mail: privacy@zermelo.nl Telefoon: 071 52 400 86 Website: www.zermelo.nl
Link naar leverancier en/of productpagina	
Beknopte uitleg en werking product en dienst	Beheren van informatie en van het proces van het roosteren, van de prognoses tot de dagroostering.
Doelgroep	Voortgezet onderwijs, hoger onderwijs
Gebruikers	onderwijsdeelnemers, ouders/verzorgers, docenten, medewerkers

B. Basis- en optionele modules

Bij de afname van Zermelo kan de Onderwijsinstelling, naast de standaard / basismodule, in bepaalde gevallen kiezen voor verschillende optionele modules. In het onder E opgenomen schema wordt (in dat geval per module) weergegeven welke Persoonsgegevens er worden Verwerkt en voor welke (onder C opgenomen) doeleinden dat gebeurt.

Status afgenomen modules en activatie van optionele Verwerkingen door feitelijk gebruik

De exacte status van de door Onderwijsinstelling (en de onder de Onderwijsinstelling vallende scholen) afgenomen diensten/modules is zichtbaar via de klantenkaart.

Indien Verwerker bij aanvang van het gebruik alle modules in zijn product en/of dienst beschikbaar stelt aan de Onderwijsinstelling, is er pas sprake van een Verwerking, indien de Onderwijsinstelling tot daadwerkelijk gebruik van de betreffende module overgaat.

Wanneer er binnen Zermelo gebruik wordt gemaakt van zogenaamde 'open velden', kan Verwerker geen invloed uitoefenen op de daarin Verwerkte gegevens. Indien de Onderwijsinstelling in de open velden Persoonsgegevens opneemt die niet zijn worden vermeld in deze Privacy Bijsluiter en/of Persoonsgegevens gebruikt voor doeleinden die niet zijn vermeld in deze Privacy Bijsluiter, doet Onderwijsinstelling dit onder eigen verantwoordelijkheid.

C. Doeleinden voor het Verwerken van Persoonsgegevens

De Verwerker 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 II. (Alleen) indien de Verwerker (tevens) leverancier is van een digitaal product en/of digitale dienst bestaande uit een School- en Leerlinginformatiemiddel dan zijn de volgende mogelijke doelstellingen van gegevensverwerking in het kader van deze producten en diensten van toepassing:

Van toepassing:		Doeleinde (conform artikel 5 lid 2 Privacyconvenant):
Ja	**A**	de organisatie, het geven en volgen van onderwijs, het begeleiden en volgen van Onderwijsdeelnemers of het geven van school- en studieadviezen, waaronder: • de indeling en aanpassing van roosters; • de analyse en interpretatie van leerresultaten; • het bijhouden van persoonlijke (waaronder medische) omstandigheden van een Onderwijsdeelnemer en de gevolgen daarvan voor het volgen van onderwijs; • het begeleiden en ondersteunen van leerkrachten en andere medewerkers binnen de Onderwijsinstelling; • de communicatie met Onderwijsdeelnemers en ouders en medewerkers van de onderwijsinstelling; • financieel beheer; • monitoring en verantwoording, ten behoeve van met name: (prestatie) metingen van de Onderwijsinstelling, kwaliteitszorg, tevredenheidsonderzoek, effectiviteitsonderzoek van onderwijs (vorm) of de geboden ondersteuning van Onderwijsdeelnemers bij passend onderwijs; • het behandelen van geschillen; • het uitwisselen van Persoonsgegevens met Derden, waaronder: • toezichthoudende instanties en zorginstellingen in het kader van de uitvoering van hun (wettelijke) taak; • samenwerkingsverbanden in het kader van passend onderwijs, regionale overstappen; • partijen betrokken bij de invulling van stage of leer-/ werkplekken voor zover noodzakelijk en wettelijk toegestaan; • Onderwijsinstellingen ingeval van overstappen tussen onderwijsinstellingen en bij vervolgonderwijs.
Nee	**B**	het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;
Nee	**C**	het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;
Ja	**D**	de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de, met behulp van het Digitale Onderwijsmiddel, Verwerkte Persoonsgegevens.
Ja	**E**	de continuïteit en goede werking van het Digitale Onderwijsmiddel conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier, waaronder het laten uitvoeren van onderhoud, het maken van een back-up, het

		aanbrengen van verbeteringen na geconstateerde fouten of onjuistheden en het krijgen van ondersteuning;
Ja	**F**	onderzoek en analyse op basis van strikte voorwaarden, vergelijkbaar met bestaande gedragscodes op het terrein van onderzoek en statistiek, ten behoeve van het (optimaliseren van het) leerproces of het beleid van de Onderwijsinstelling;
Nee	**G**	het door de Onderwijsinstelling voor onderzoeks- en analyse doeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.
Ja	**H**	het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.
Ja	**I**	de uitvoering of toepassing van een andere wet

In het onder E opgenomen schema wordt per module weergegeven welke (onder D opgenomen) Persoonsgegevens er worden Verwerkt en voor welke (onder C opgenomen) doeleinden dat gebeurt.

D. Categorieën en soorten Persoonsgegevens

Verwerker geeft hieronder aan welke categorieën Persoonsgegevens er (al dan niet optioneel) kunnen worden Verwerkt binnen Zermelo. In het onder E opgenomen schema wordt per module weergegeven welke (onder D opgenomen) Persoonsgegevens er worden Verwerkt en voor welke (onder C opgenomen) doeleinden dat gebeurt.

1. Omschrijving van de categorieën Betrokkenen over wie Persoonsgegevens worden Verwerkt, en de categorieën Persoonsgegevens van de Betrokkenen:

Van toepassing	Categorie	Toelichting
Ja	**1. Contactgegevens**	naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens; Beperkte set = naam, e-mail, opleiding; Persoonlijke set = geboortedatum, geslacht;
Ja	**2. Onderwijs-deelnemer-nummer**	het leerlingnummer zoals dat in de schooladministratie gebruikt wordt
Nee	3. Nationaliteit en geboorteplaats	
Ja	**4. Ouders, voogd**	gegevens als bedoeld onder 1, van de ouders/verzorgers van onderwijsdeelnemers
Ja	**5. Medische gegevens**	gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de betrokkene of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs; Het gaat om de volgende gegevens: 1. Bij het dagroosteren is er de mogelijkheid om een afwezigheidsreden op te geven. Daarbij is gebruikelijk om een afwezigheidsreden "ziek" te gebruiken.

		2. Het is ook gebruikelijk om bij leerlingen aan te geven of ze dyslexie hebben of om een andere reden extra tijd nodig hebben bij toetsen. Dit wordt ook wel gebruikt om leerlingen "eerlijk" te verdelen over klassen. 3. Mogelijk andere gegevens die in vrije ("extra") velden worden bijgehouden voor het roosterproces.
Nee	6. Godsdienst	gegevens betreffende de godsdienst of levensovertuiging van de betrokkene, voor zover die noodzakelijk zijn voor het onderwijs, of op eigen verzoek, een en ander voor zover noodzakelijk voor het onderwijs;
Ja	**7. Studievoortgang**	gegevens betreffende de aard en het verloop van het onderwijs, alsmede de behaalde studieresultaten; te weten: • klas / leerjaar / ILT code • Examinering • Studievoortgang en/of Studietraject • Begeleiding onderwijsdeelnemers, inclusief handelingplan • Aanwezigheidsregistratie
Ja	**8. Onderwijsorganisatie**	gegevens met het oog op de **organisatie van het onderwijs** en het verstrekken of ter beschikking stellen van leermiddelen;
Nee	9. Financiën	gegevens met het oog op het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, alsmede bankrekeningnummer van de betrokkene;
Nee	10. Beeldmateriaal	foto's en videobeelden (beeldmateriaal) met of zonder geluid van activiteiten van de instelling of het instituut;
Ja	**11. Docent, zorg-coördinator, intern begeleider, decaan, mentor**	gegevens van **docenten en begeleiders,** voor zover deze gegevens van belang zijn voor de organisatie van het instituut of de instelling en het geven van onderwijs, opleidingen en trainingen;
Nee	12 Overige gegevens, te weten [omschrijving opnemen]	andere dan de onder 1 tot en met 11 bedoelde gegevens waarvan de Verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet. Wel moet worden vermeld om welke gegevens het gaat.
Nee	13. BSN/PGN	
Nee	14. Keten-ID (ECK-ID)	unieke iD voor de 'educatieve contentketen'. hiermee kunnen Onderwijsinstellingen gegevens delen, zonder dat ze direct herleidbaar zijn naar onderwijsdeelnemers of docenten.

2. Soort Persoonsgegevens

a. Door Verwerker worden wel/~~geen~~ bijzondere Persoonsgegevens Verwerkt. Het betreft hier de categorieën: 5
b. Door Verwerker worden wel/~~geen~~ gevoelige Persoonsgegevens Verwerkt. Het betreft hier de categorieën: 7

De categorieën 3, 5 en 6 zijn bijzondere Persoonsgegevens in de zin van de AVG. De categorieën 7, 9 en 13 worden (in ieder geval) gezien als gevoelige Persoonsgegevens.

3. Door Verwerker te hanteren specifieke bewaartermijnen van Persoonsgegevens (of toetsingscriteria om dit vast te stellen):

Categorie	Bewaartermijn of toetsingscriterium
1. Contactgegevens	Tot door de school verwijderd uit het Zermelo Portal. Voor roosterbestanden maximaal 1 jaar.
2. Onderwijs-deelnemer-nummer	Tot door de school verwijderd uit het Zermelo Portal. Voor roosterbestanden maximaal 1 jaar.
3. Nationaliteit en geboorteplaats	NVT
4. Ouders, voogd	Tot door de school verwijderd uit het Zermelo Portal. Voor roosterbestanden maximaal 1 jaar.
5. Medische gegevens	Tot door de school verwijderd uit het Zermelo Portal. Voor roosterbestanden maximaal 1 jaar.
6. Godsdienst	NVT
7. Studievoortgang	Tot door de school verwijderd uit het Zermelo Portal. Voor roosterbestanden maximaal 1 jaar.
8. Onderwijsorganisatie	Tot door de school verwijderd uit het Zermelo Portal. Voor roosterbestanden maximaal 1 jaar.
9. Financiën	Tot door de school verwijderd uit het Zermelo Portal. Voor roosterbestanden maximaal 1 jaar.
10. Beeldmateriaal	NVT
11. Docent, zorg-coördinator, intern begeleider, decaan, mentor	Tot door de school verwijderd uit het Zermelo Portal. Voor roosterbestanden maximaal 1 jaar.
12 Overige gegevens, te weten [omschrijving opnemen]	NVT
13. BSN/PGN	NVT
14. Keten-ID (ECK-ID)	NVT

E. Uitwerking Verwerkingen Persoonsgegevens en doeleinden per afgenomen module

Hieronder wordt per categorie Persoonsgegeven aangegeven, voor welke functie en binnen welke module dit Persoonsgegeven in het kader van Zermelo wordt Verwerkt en op grond van welk van de hierboven genoemde doeleinden dit gebeurt:

Een omschrijving van de afgenomen modules is te vinden op https://www.zermelo.nl/producten/

Voor alle modules geldt dat de gegevens worden gebruikt voor alle onder C genoemde doeleinden.

Afgenomen module:	**Functie**	**Productverwijzing**	**Categorieen persoonsgegevens**
Basis (verplicht)	• Roostervoorbereiding • Roosteren • Ouderavonden		1,4,5,7,8,11
Pro	• Geavanceerd roosteren		*Geen extra categorieën boven die van Basis*
Formatie	• Formatiebeheer		9
Onderhoud	• Dagroosteren • Toetsroosteren		*Geen extra categorieën boven die van Basis*
Decaan	• Pakketkeuze		*Geen extra categorieën boven die van Basis*

F. Opslag Verwerking Persoonsgegevens:
Plaats/Land van opslag en Verwerking van de Persoonsgegevens: Nederland, Ierland, Duitsland.

G. Subverwerkers
Onderwijsinstelling geeft Verwerker door ondertekening van de Verwerkersovereenkomst een algemene schriftelijke toestemming voor het inschakelen van een Subverwerker. Verwerker heeft het recht gebruik te gaan maken van andere Subverwerkers, mits daarvan voorafgaand mededeling wordt gedaan aan Onderwijsinstelling, en Onderwijsinstelling daartegen bezwaar kan maken binnen een redelijke periode.

Verwerker maakt ten tijde van het afsluiten van de Verwerkersovereenkomst gebruik van de volgende Subverwerkers:

Subverwerker	Omschrijving taak/dienst	Vestigingsgegevens	Opslag/ Verwerking	Opmerkingen
Amazon Web Services (AWS)	Cloud hosting	Amazon Web Services, Inc. 410 Terry Avenue North, Seattle, Washington 98109-5210 USA	EER (Ierland)	In de toekomst mogelijk ook in Nederland of Duitsland
TeamViewer	Ondersteuning op afstand	TeamViewer GmbH Jahnstraße 30, 73037 Göppingen Duitsland	EER (Duitsland)	

Opmerking: indien de Persoonsgegevens buiten de EER worden Verwerkt wordt apart opgave gedaan van de landen waar de Persoonsgegevens worden Verwerkt én op welke wijze is gewaarborgd dat de gegevens rechtmatig kunnen worden doorgegeven.

H. Contactgegevens

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

Zermelo Software B.V.
Schuttersveld 9
2316 XG Leiden

E-mail: privacy@zermelo.nl
Telefoon: 071 52 400 86
Website: www.zermelo.nl

I. Versie

Deze bijlage is voor het laatst aangepast op 04-10-2018, 11:10.

Bijlage 2: Beveiligingsbijlage

Dit is de branchespecifieke bijlage van de Vereniging Digitale Onderwijs Dienstverleners (VDOD). Deze bijsluiter is gebaseerd op bijlage 2 bij de modelbewerkersovereenkomst behorende bij het Convenant. Dit model is afgestemd door de Initiatiefnemers van het Convenant en is gepubliceerd op de website van Edu-k.

Omschrijving van de maatregelen zoals bedoeld in artikel 7 Verwerkersovereenkomst

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 hun functie.

Hieronder wordt uitgewerkt 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.

Groepen van medewerkers en Persoonsgegevens:	Handelingen:

Helpdesk: alle medewerkers van Zermelo hebben toegang tot de helpdesksoftware, waar berichten inclusief bijlages en screenshots die persoonsgegevens bevatten binnenkomen. Ook worden hier aantekeningen gemaakt van telefoongesprekken. Bijlages en screenshots worden automatisch verwijderd twee weken nadat het ticket is gesloten.	Ondersteuning van de eindgebruiker, en zo nodig analyse van de opgestuurde bestanden.
Roosterconsultants: de medewerker die de school ondersteunt krijgt van de school expliciet een account op het portal van de school. Ook deelt de school expliciet de benodigde (rooster) bestanden met de roosterconsultant via een beveiligde omgeving.	Roosteren/formatiebeheer/algemene ondersteuning.
Systeembeheerders: systeembeheerders houden in de gaten of het systeem correct functioneert en zorgen voor backups van alle gegevens.	Controleren van de logbestanden, handelingen direct op de database, maken, controleren en terugzetten van backups.
Ontwikkelaars: ontwikkelaars krijgen alleen toegang tot persoonsgegevens als dit noodzakelijk is om een probleem in de software op te lossen, en alleen na toestemming van de school.	Analyse van specifieke daarvoor opgestuurde bestanden om problemen in de software op te lossen.

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.

Zermelo heeft het Certificeringsschema van Edu-K gebruikt als toetsingskader en voor het creëren van een solide basisniveau van informatiebeveiliging en privacy voor de software. In bijlage 2b vindt u de rapportage van de BIV-classificatie, de mate van compliance en de uitleg bij eventuele afwijkingen van de standaarden.

Organisatie van informatiebeveiliging en communicatieprocessen

- Verwerker beschikt over een actief informatiebeveiligingsbeleid
- Verwerker heeft een coördinator voor informatiebeveiliging (security officer) om risico's omtrent de Verwerking van Persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te controleren en maatregelen te treffen die zien op naleving van het informatiebeveiligingsbeleid.
- Verwerker heeft een proces ingericht voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.

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 Verwerker worden periodiek gecontroleerd aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging. Daarnaast voorziet het beveiligingsbeleid van Verwerker in interne processen om kwetsbaarheden te identificeren.

Rapportage

Verwerker actualiseert deze informatie voortdurend en informeert gebruikers over wijzigingen in de getroffen maatregelen om persoonsgegevens te beschermen tegen misbruik via de mail en via haar website. In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met de helpdesk van Verwerker via 071 524 00 86 .

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

De wijze waarop monitoring en identificatie van Datalekken plaatsvindt

Verwerker monitort 24/7 (of anders de afgesproken periode) 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 Verwerker, die analyseert of sprake kan zijn van een Datalek.

De wijze waarop informatie wordt gedeeld

Wanneer zich een Datalek voordoet, wordt de Verwerkingsverantwoordelijke onderwijsinstelling door of namens Verwerker in beginsel binnen binnen 24 uur na vaststelling dat sprake is van een 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. Verwerker neemt daarnaast ook telefonisch contact op met de Verwerkingsverantwoordelijke.

De contactpersoon voor beveiligingsincidenten is: <privacy-contactpersoon>

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

Verwerker 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 Verwerker 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 bijlage is voor het laatst aangepast op 04-10-2018, 13:10.

Bijlage 2b: Certificeringsschema ROSA

Organisatie	Zermelo Software B.V. (Zermelo Roostermakers)
ICT-toepassing	Zermelo
Omschrijving	Met de software van Zermelo wordt het gehele roosterproces vanaf prognoses en formatie tot de dagroostering geregeld.
Datum	6-9-2018
Toetsvorm	Self-assessment
Uitvoerder toets	Gerard Krol Hoofd ICT Zermelo Roostermakers
BIV-classificatie	Beschikbaarheid=3, Integriteit=2, Vertrouwelijkheid=3

Overzicht

Categorie	Uitkomst	Voldaan	Niet voldaan
Beschikbaarheid	Hoog	7	0
Integriteit	Midden	6	0
Vertrouwelijkheid	Hoog	7	1

Beschikbaarheid (hoog)

Beschikbaarheid is noodzakelijk.

Algeheel verlies of niet beschikbaar zijn van deze informatie gedurende een werkdag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten.

RTO*= 8-24 uur, afhankelijk van de categorie informatie

Maatregel	Eisen	Compliance	Uitleg
Overbelasting		Voldaan	

	De hoeveelheid gebruikersverkeer is tijdens het ontwerp van de toepassing bepaald. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing ingericht om overbelasting te voorkomen. De hoeveelheid gebruikersverkeer wordt automatisch gemonitord en gereguleerd middels load balancers, traffic shapers of een soortgelijke oplossing. Bij overbelasting van het systeem wordt automatisch een notificatie /signalering gestuurd, zodat zo snel mogelijk maatregelen genomen kunnen worden.		
Bussiness Continuity	Er is een 'Hot Standby' aanwezig, dat wil zeggen: de toepassing draait reeds op fysieke of virtuele reserve-infrastructuur waar direct naar overgeschakeld kan worden. Bijvoorbeeld door middel van: • active-active applicatieonderdelen • actieve backup netwerkverbinding • UPS/NoBreak Recovery test= 4x per jaar. RTO max= 8 uur. Automatische online failover (verlies van sessies en transacties wordt voorkomen).	Voldaan	Failover automatisch geregeld via AWS, wordt geregeld gebruikt bij neerzetten nieuwe versies en upgrades van databases.
Ontwerp	Tijdens het ontwerp is gekeken naar de afhankelijkheden van aanpalende systemen en impact van eventuele uitval. Naar aanleiding van deze analyse zijn de onderdelen van de toepassing ingericht om kennisgeving van uitval te geven. Er wordt regelmatig opnieuw geanalyseerd wat de afhankelijkheden met andere toepassingen zijn. Bijvoorbeeld bij grote wijzigingen, aanpassingen of verandering in gebruikersverkeer.	Voldaan	
Monitoring	Terwijl de toepassing wordt gebruikt wordt de beschikbaarheid van de toepassing en aanpalende toepassingen gemonitord. Naar aanleiding van deze monitoring wordt bij uitval een gestructureerd proces gestart voor notificatie en herstel van de keten. De cijfers van de recente en huidige beschikbaarheid van de toepassing zijn opvraagbaar voor belanghebbenden.	Voldaan	Via CloudWatch en Pingdom. Voor gebruikers is er http://stats.zportal.nl.
Testen	Onbeschikbaarheid en afname van performance direct getest door middel van bijvoorbeeld gebruikssimulaties. Er zijn aantoonbaar proactieve performance testen, bijvoorbeeld bij wijzigingen in ontwerp of verwachtte verandering in gebruikersverkeer.	Voldaan	

Software	Security patches, updates van firmware en software en vernieuwing van certificaten worden met vaste regelmaat in de toepassing uitgevoerd, bijvoorbeeld middels een maandelijks of geautomatiseerd proces. Urgente security patches worden sneller doorgevoerd. Er wordt – waar mogelijk – geautomatiseerd gecontroleerd op security-gerelateerde patches en updates. Software van derden (zoals operating system of libraries) wordt actief onderhouden door de leverancier. Bijvoorbeeld Windows XP wordt niet toegestaan.	Voldaan	
Actuele dreigingen (DDoS, ransomware)	Context: voor beschikbaarheid is bijvoorbeeld DDoS een actuele dreiging. De relevante medewerkers zijn op de hoogte van mogelijke bedreigingen. Je bent in staat om spoedig te detecteren of de toepassing niet beschikbaar is door een mogelijke DDoS-aanval. Er is actieve bescherming tegen DDoS-aanvallen, bijvoorbeeld door firewalls of een wasstraat voor internetverkeer.	Voldaan	

Integriteit (midden)

Niveau 2 **Midden**	Integriteit is beschermd. Blijvende juistheid van informatie moet gewaarborgd zijn. Sommige toleranties zijn toelaatbaar. Juistheid van informatie is belangrijk, maar niet kritisch. Het is niet noodzakelijk dat correctheid onbetwistbaar aangetoond kan worden. Indien informatie niet correct is kan de organisatie substantiële schade lijden.	Een zeer beperkt aantal fouten is toegestaan Gegevens zijn volledig en juist RPO* 1 dag

Maatregel	Eisen	Compliance	Uitleg
Herleidbaarheid (gebruikers)	Herleidbaar wanneer, welke gegevens gewijzigd zijn: - Het is mogelijk om wijzigingen terug te draaien - Naamloze gebruikersaccounts met uitgebreide rechten zijn toegestaan maar (indirect) herleidbaar naar personen - Herleidbaar wanneer de gegevens gewijzigd zijn - Gebruikers mogen beheerdersrechten hebben - Toegang en wijziging van gegevens wordt gecontroleerd, bijvoorbeeld met expliciete notificatie aan personen met beheerdersrechten	Voldaan	Gegevens kunnen teruggedraaid via backup. Er is 90 dagen access logging maar deze is niet direct beschikbaar voor klanten.
Backup	Backup verplicht, minimaal dagelijks, bijvoorbeeld door een gescripte backup. RPO max= 1 dag.	Voldaan	Restore test zou wel structureler gepland moeten worden.

	Restore test= 2x per jaar.		
Application controls	Controle op invoer en andere methoden van wijzigen van gegevens: - De toepassing controleert invoer (handmatig of via geautomatiseerde koppeling) door bijvoorbeeld syntax-controle en controle op verplichte velden - Wijzigingen ‘onder water’ (zonder gebruik van de gebruikersinterface) worden gelogd en de logging wordt periodiek gecontroleerd	Voldaan	De "onder water" wijzigingen direct in de database door beheerders worden gelogd. API calls worden gelogd.
Onweerlegbaarheid	Gelogd wordt: inlogactiviteit gebruikers en wijziging van persoonsgegevens Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) Logging wordt periodiek (bijvoorbeeld maandelijks) gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	Voldaan	Periodieke controle moet wel structureler geregeld.
Herleidbaarheid (technisch beheer)	Herleidbaar wanneer, welke onderdelen/configuraties van de toepassing gewijzigd zijn: - Het is mogelijk om wijzigingen terug te draaien - Naamloze systeemaccounts met uitgebreide rechten zijn toegestaan en (indirect) herleidbaar naar personen - Herleidbaar wanneer de toepassing gewijzigd is - Toegang tot de onderliggende systemen van de toepassing is rolgebaseerd toegewezen - Toegang met root-accounts is gereguleerd, bijvoorbeeld met expliciete notificatie en logging	Voldaan	
Controle integriteit (toepassing)	Periodieke controle integriteit toepassing: - Patchen en updates van firmware en software worden bij grote wijzigingen in de toepassing en handmatig uitgevoerd - Integriteit van de configuratie en software wordt structureel gecontroleerd door een regelmatig uitgevoerd proces Antivirus/malware wordt toegepast Secure software development /secure coding guidelines worden toegepast	Voldaan	Dit proces kan nog structureler worden vastgelegd.
Onweerlegbaarheid (toepassing)	Gelogd wordt: inlogactiviteit technisch beheer, aanpassingen configuratie en toepassing Voor de kwaliteit van logging worden best practices gehanteerd (bijvoorbeeld OWASP Logging cheat sheet) Logging wordt periodiek (bijvoorbeeld maandelijks) gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	Voldaan	
Actuele dreigingen (DDoS, ransomware)	Voor integriteit is ransomware een actuele dreiging.	Voldaan	

	Houdt rekening met de maatregelen rondom RTO en RPO (bij ransomware is rollback mogelijk naar een gecontroleerde situatie korter dan 24 uur geleden). Medewerkers worden bewust gemaakt van deze bedreiging en zij daartegen kunnen doen. Bijvoorbeeld netwerkscheiding om propagatie te voorkomen. Je bent in staat om spoedig te detecteren of de (aanpalende) systemen van een toepassing getroffen zijn door ransomware.		

Vertrouwelijkheid (hoog)

Niveau 3 **Hoog**	Informatie is geheim. De organisatie, instelling of betrokkene kan ernstige schade lijden indien informatie toegankelijk is voor ongeautoriseerde personen. Informatie mag uitsluitend toegankelijk zijn voor een zeer geselecteerde groep personen. Hieronder vallen onder andere bijzondere persoonsgegevens.	Toegang is beperkt tot expliciet aangewezen personen binnen de organisatie. Beheerders hebben, waar mogelijk, geen toegang tot de gegevens. Beheerders maken alleen gebruik van persoonlijk herleidbare accounts.

Maatregel	Eisen	Compliance	Uitleg
Levenscyclus gegevens	Er wordt invulling gegeven aan wettelijke bewaartermijnen voor persoonsgegevens, logging, leerlingdossiers, et cetera. De ict-toepassing moet het mogelijk maken dat persoonsgegevens verwijderd moeten kunnen worden, bijvoorbeeld op verzoek van de betrokkene of wanneer de bewaartermijn verstreken is. Op media/apparatuur die niet meer worden gebruikt of voor andere doeleinden wordt hergebruikt wordt data onherstelbaar vernietigd (bijvoorbeeld degaussing, sanitization, purging, zeroization of vernietiging van de datadrager). Informatie in deze categorie wordt altijd gelabeld.	Voldaan	
Logische toegang	Er is een geïmplementeerd beleid voor logische toegang. Daarin zitten minimaal de volgende maatregelen: - Two-factor authenticatie (gebruikersnaam en wachtwoord aangevuld met bijvoorbeeld een code op een mobiele telefoon, token of machine certificaat) - Accounts zijn persoonlijk identificeerbaar - Een wachtwoordbeleid dat voldoet aan best practices zoals de richtlijnen van NIST* - Periodieke controle actieve accounts versus actieve medewerkers	Niet voldaan	Er zijn enkele systemen waarbij de toegang alleen gecontroleerd wordt via een wachtwoord. Er wordt binnenkort een project gestart om dit te verbeteren.
Fysieke toegang	Fysieke toegang tot de apparatuur waarop de toepassing draait is beschermd met minimaal: - Twee factor authenticatie	Voldaan	

	- Herleidbaar aan wie de toegang wordt verleend - Bijvoorbeeld middels een gepersonaliseerde toegangspas aangevuld met pincode, biometrische verificatie of soortgelijke oplossingen - Logging en monitoring van toegang, bijvoorbeeld cameratoezicht Bezoekers enkel onder begeleiding.		
Netwerk toegang	Er is een geïmplementeerd beleid voor netwerktoegang. Daarin zitten minimaal de volgende maatregelen: - Netwerksegmentatie, bijvoorbeeld door middel van VLANs - Toegang vanuit andere zones is beschermd met aanvullende maatregelen zoals een firewall die poorten dichtzet en whitelisting van IP-adressen - Extern benaderbaar door medewerkers en beheerders alleen via beveiligde verbinding met authenticatie en encryptie	Voldaan	
Scheiding omgevingen	Ontwikkel, test, acceptatie en productieomgevingen zijn gescheiden. Productiedata (gebruikersnamen, wachtwoorden, et cetera) en persoonsgegevens worden niet gebruikt in ontwikkel- en testomgevingen en waar mogelijk ook niet in acceptatieomgevingen. Testdata zijn altijd geanonimiseerd. Toegang tot productieomgevingen wordt beheerd en periodiek gecontroleerd en geeft invulling aan de principes ‘need to know’ en ‘least privilege’. Bijvoorbeeld: ontwikkelaars hebben niet standaard toegang tot productieomgevingen.	Voldaan	
Transport en fysieke opslag	Encryptie van transport (zowel voor intern als extern verkeer). Encryptie van fysieke opslag. Voor het gebruik van encryptie wordt gebruik gemaakt van richtlijnen /best practices/standaarden. Bijvoorbeeld van NCSC, ENISA, NIST. Daarbij worden de volgende uitgangspunten gehanteerd: - Encryptie welke niet te kraken is binnen de verwachtte levensduur van de versleutelde informatie. - TLS 1.2 of hoger	Voldaan	
Logging	Toegang tot de ict-toepassing en lezen en wijzigen van persoonsgegevens wordt gelogd. Logging is enkel toegankelijk voor bevoegde personen en toegang ertoe wordt apart gelogd en gecontroleerd. Logging wordt regelmatig gecontroleerd op uitzonderingen op toegang en uitzonderlijke patronen in gebruik. Bijvoorbeeld door automatische loganalysetooling.	Voldaan	

Toetsing	Gegevens zijn geclassificeerd. Een risico/dreigingsanalyse zijn uitgevoerd op de toepassing, ter illustratie: - Privacy by design en security by design wordt toegepast - Threat modelling - OWASP Top 10 De toepassing wordt getoetst tegen richtlijnen als bijvoorbeeld de NCSC richtlijnen voor webapplicaties. De toepassing wordt periodiek getoetst op passende bescherming van vertrouwelijkheid (minimaal jaarlijks en bij grote wijzigingen), bijvoorbeeld: - Security testen - Vulnerability testen - Pentesten	Voldaan	
Actuele dreigingen (DDoS, ransomware)	Context: Voor vertrouwelijkheid is bijvoorbeeld een hack een actuele dreiging. Medewerkers zijn op de hoogte van mogelijke bedreigingen die leiden tot datalekken, weten hoe ze moeten omgaan met persoonsgegevens en weten waar ze datalekken moeten melden in de organisatie. Je bent in staat om spoedig te detecteren of er een mogelijk datalek is in de toepassing bijvoorbeeld door regelmatige controle van toegangsrechten in de toepassing. Je kijkt actief naar het gangbare gebruik, door bijvoorbeeld IDS/IPS of loganalysetools (SIEM), om afwijkingen/mogelijke datalekken te kunnen signaleren.	Voldaan	

Bijlage 3: Afwijkingen van de modelovereenkomst

Partijen zijn overeengekomen om af te wijken van een aantal bepalingen van de model Verwerkersovereenkomst. In deze bijlage omschrijven we de wijzigingen en geven we aan waarom het nodig was om van het model af te wijken. De wijzigingen hebben te maken met verduidelijking en praktische uitvoerbaarheid.

Artikel	**Wijziging**	**Uitleg**
5.5 en 5.6	De volledige bepalingen vervallen.	Deze specifieke bepalingen zijn niet van toepassing.
7.6	Aanpassing van de eerste zin naar: "In aanvulling op de voorgaande leden heeft Onderwijsinstelling *maximaal één (1) keer per jaar* het recht..."	Het uitvoeren van een audit is zowel tijds- als kostenintensief, en om die reden beperkt Zermelo het aantal audits per onderwijsinstelling tot de gebruikelijke termijn van één (1) keer per jaar.
11.2	Toevoegen: ..."Het recht op bezwaar vervalt 60 dagen nadat de mutatie bekend is gemaakt."	Aan gemotiveerde bezwaren die binnen een redelijke termijn worden ingediend kan gehoor worden gegeven. Als deze termijn te lang wordt dan is dat niet meer mogelijk of anders zeer kostbaar. We vragen u daarom om tijdig (binnen 60 dagen) uw bezwaren kenbaar te maken.
12.4	Aanpassen van het artikel naar:	De subverwerkers die Zermelo inschakelt bieden alleen hosting of infrastructuur aan. Het beheer van de gegevens, waaronder

	"Verwerker zal na de beëindiging van de Verwerkersovereenkomst waarborgen dat alle Subverwerkers de Persoonsgegevens (laten) vernietigen."	het verwijderen, wordt door Zermelo zelf gedaan, in lijn met artikel 12 lid 3. Uiteraard zijn er afspraken dat deze gegevens dan ook echt weg zijn. Het is dus niet nodig om de beëindiging van een verwerkersovereenkomst aan alle subverwerkers te melden.
13	Nieuw lid: "4. Wat betreft aansprakelijkheid voor andere schade dan uitgesloten in lid 1 van dit artikel, is artikel 16 van de Algemene Voorwaarden onverminderd van toepassing."	In dit toegevoegde lid wordt ter expliciet aangeven waar de overige aansprakelijkheid is geregeld, namelijk volgens artikel 16 van de algemene voorwaarden. Het kan zijn dat dit voor u vanzelfsprekend is, maar we nemen dit toch graag op in de overeenkomst. Zermelo hanteert de Nederland ICT voorwaarden (https://www.zermelo.nl/downloads/overeenkomsten/zermelo-algemene-voorwaarden.pdf) bij alle overeenkomsten/levering van software.

Versie

Deze bijlage is voor het laatst aangepast op 16-11-2018, 11:11.