

Verwerkersovereenkomst Oefenweb.nl B.V.

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

De nieuwe Verwerkersovereenkomst 3.0 komt in de plaats van eerdere Verwerkersovereenkomsten van het Convenant 2.0. De uitgangspunten van deze 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 het 2.0 model 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.

Deze 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.

Verwerkersovereenkomst Oefenweb.nl B.V.

Partijen:

1. Het bevoegd gezag van (naam + rechtsvorm onderwijsinstelling), geregistreerd onder bestuursnummer bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, vertegenwoordigingsbevoegd voor de in Bijlage 3 vermelde scholen, gevestigd en kantoorhoudende aan (adres), te (postcode+plaats), te dezen rechtsgeldig vertegenwoordigd door (functie + naam), hierna te noemen: “**Onderwijsinstelling**”.

en

2. De besloten vennootschap Oefenweb.nl B.V., gevestigd en kantoorhoudende aan Rapenburgerstraat 109, te 1011 VL Amsterdam, te dezen rechtsgeldig vertegenwoordigd door haar directeur Marthe Straatemeier, hierna te noemen: “**Verwerker**”

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

Overwegen het volgende:

- a. Onderwijsinstelling een abonnement afneemt op de online leeromgevingen (Rekentuin, Taalzee en/of Words&Birds) van Verwerker, (‘de Product- en Dienstenovereenkomst’). Deze Product- en Dienstenovereenkomst leidt ertoe dat Verwerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
- a. 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.

Artikel 1: Definities

In deze Verwerkersovereenkomst wordt verstaan onder:

- a. Betrokkene, Verwerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens en Verwerkingsverantwoordelijke: de begrippen zoals gedefinieerd in de AVG;
- b. Bijlage(n): bijlage(n) bij het Convenant of de Verwerkersovereenkomst;

- c. Convenant: het Convenant Digitale Onderwijsmiddelen en Privacy 3.0;
- d. Convenantpartij: een tot het Convenant toetreden Onderwijsinstelling of Leverancier;
- e. Datalek: een inbreuk in verband met persoonsgegevens, zoals bedoeld in artikel 4 sub 12 AVG;
- f. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
- g. Initiatiefnemers: partijen die de initiatiefnemers zijn van het Convenant als opgenomen in de aanhef van het Convenant;
- h. 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);
- i. 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;
- j. 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;
- k. Leverancier: leverancier van een Digitaal Onderwijsmiddel, zoals een distributeur, uitgever of leverancier van een administratiesysteem;
- l. Model Verwerkersovereenkomst: het model voor een verwerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;
- m. Onderwijsdeelnemer: onderwijsdeelnemer in het primair onderwijs, voortgezet onderwijs of middelbaar beroepsonderwijs;
- n. Platform: het platform als bedoeld in artikel 8 van het Convenant, thans bekend als Edu-K;
- o. 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;
- p. Privacybijsluiter: één of meerdere privacybijsluiter(s) zoals opgenomen in de Bijlage(n) die van toepassing zijn op de aangeboden Digitale Onderwijsmiddelen;
- q. Reglement: het reglement als bedoeld in artikel 8 lid 4 van het Convenant;
- r. 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;
- s. 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);
- t. 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;

- u. 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);
- v. 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 verwerkingsactiviteiten¹ die onder hun verantwoordelijkheid plaatsvinden.

¹ Zie voor een voorbeeld de Aanpak IBP bij <https://kn.nu/IBPonderwijs>

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.

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 betreft 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:
 - a. voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken;

- b. indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Verwerker aan Onderwijsinstelling te verlenen diensten; of
 - c. 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:
 - a. een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens;
 - b. maatregelen om te waarborgen dat enkel geautoriseerde medewerkers toegang hebben tot de Persoonsgegevens die in het kader van de Verwerkersovereenkomst worden verwerkt;
 - c. 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:
 - a. 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.
 - b. De auditor verstrekt het auditrapport alleen aan Partijen.
 - c. Partijen maken onderling afspraken over de omgang met de uitkomsten van de audit.
 - d. 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.
 - e. 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:
 - a. 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;
 - b. het uitvoeren van controles en audits zoals bedoeld in artikel 7 van deze Verwerkersovereenkomst;
 - c. het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele daaruit voortvloeiende verplichte voorafgaande raadpleging van de Autoriteit Persoonsgegevens;
 - d. het voldoen aan verzoeken van de Autoriteit Persoonsgegevens of een andere overheidsinstantie;
 - e. 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:
 - a. verhaalsactie op grond van artikel 82 AVG; of
 - b. 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.

Aldus overeengekomen, in tweevoud opgemaakt en ondertekend,

Onderwijsinstelling,

Verwerker,

Naam: _____

Naam: M. Straatemeier

Functie: _____

Functie: Directeur

Datum: _____

Datum: 24 mei 2018

Indien u deze Verwerkersovereenkomst tekent namens een rechtspersoon, garandeert u persoonlijk tot vertegenwoordiging bevoegd te zijn.

Bijlage 1: Privacybijsluiters

Bijlage 2: Beveiligingsbijlage

Bijlage 2a: Certificeringsschema

BIJLAGE 1 bij Verwerkersovereenkomst Versie 3.0: Privacy Bijsluiter Oefenweb.nl B.V. (Rekentuin, Taalzee en Words & Birds)

Deze Privacy Bijsluiter van Oefenweb.nl B.V. (hierna te noemen: “Oefenweb”) is tot stand gekomen op basis van het model dat is vastgesteld door het Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen -, een initiatief van de PO-Raad, VO-raad, de verschillende betrokken ketenpartijen (GEU, Kbb-e en vDOD), het ministerie van Onderwijs, Cultuur en Wetenschappen en het ministerie van Economische Zaken (hierna: het “Convenant”).

De Privacy Bijsluiter is een bijlage bij de Verwerkersovereenkomst (die eveneens is vastgesteld op basis van het model van het Convenant), versie 3.0, en is bedoeld om eenvoudig te begrijpen informatie te verschaffen over de Verwerking en bescherming van Persoonsgegevens bij de dienstverlening van Oefenweb

A. Algemene informatie

<i>Naam product en/of dienst:</i>	<u>Rekentuin / Taalzee / Words&Birds</u>
<i>Naam Verwerker en vestigingsgegevens:</i>	<i>Oefenweb.nl B.V., Rapenburgerstraat 109, Amsterdam.</i>
<i>Link naar uitgever en/of productpagina:</i>	<u>Oefenweb.nl, Rekentuin.nl, Taalzee.nl, Words&Birds.nl</u>
<i>Beknopte uitleg en werking product en dienst:</i>	<i>Rekentuin, Taalzee en Words&Birds zijn webapplicaties om rekenen, Nederlands en Engels mee te oefenen en volgen. De leerling kan op zijn of haar eigen tempo werken en de opgaven die de leerling krijgt, zijn afgestemd op het niveau van de leerling. Leerkrachten krijgen inzicht in de leerresultaten van hun leerlingen</i>
<i>Doelgroep (zoals PO/VO, onderbouw/bovenbouw):</i>	<i>PO, VO, MBO, HBO</i>
<i>Gebruikers (leerlingen/ouders/verzorgers/docenten):</i>	<i>Leerlingen, ouders/verzorgers, leerkrachten, ICT-coördinatoren, intern begeleiders, remedial teachers en directeuren.</i>

B. Doeleinden voor het verwerken van Persoonsgegevens en specifieke diensten

Verwerker is leverancier van digitale leermiddelen die adaptief onderwijs mogelijk maken. De doeleinden van de Verwerking van Persoonsgegevens met behulp van de producten van Oefenweb, zijn in overeenstemming met de Verwerkingsdoeleinden voor Leermiddelen en Toetsen, zoals opgenomen in artikel 5 van het Convenant Digitale Onderwijsmiddelen en Privacy 3.0.

Verwerkingen die een onlosmakelijk onderdeel vormen van de onder A genoemde producten

De verwerkingen door Oefenweb vinden plaats om Onderwijsinstellingen in staat te stellen om onderwijs te geven en volgen en leerlingen te kunnen volgen en begeleiden.

Bij het in gebruik nemen van de producten van Oefenweb vinden altijd de volgende verwerkingen plaats:

- de opslag van leer- en toetsresultaten;
- het terugontvangen door de Onderwijsinstelling van leer- en toetsresultaten;
- de beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen verkrijgen dat is afgestemd op de specifieke leerbehoefte van een leerling;
- de beoordeling van leer- en toetsresultaten van een leerling t.o.v. de resultaten van een groep van leerlingen om inzicht te krijgen hoe een leerling presteert t.o.v. deze groep (bijvoorbeeld: percentielscores);
- analyse en interpretatie van leerresultaten;
- het geleverd krijgen/in gebruik kunnen nemen van de digitale leermiddelen;
- het verkrijgen van toegang tot de aangeboden digitale leermiddelen, en externe informatiesystemen, waaronder identificatie, authenticatie en autorisatie;
- de beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het voorkomen van inconsistentie en onbetrouwbaarheid in de verwerkte Persoonsgegevens
- de continuïteit en goede werking van het digitale leermiddel, 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;
- 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, het product of het beleid van de Onderwijsinstelling;
- het door de Onderwijsinstelling voor onderzoeks- en analysedoeleinden beschikbaar kunnen stellen van volledig geanonimiseerde Persoonsgegevens om daarmee de kwaliteit van het onderwijs te verbeteren.
- het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen;
- de uitvoering of toepassing van een andere wet.

Optionele verwerkingen:

Bij het gebruik van de digitale leermiddelen van Oefenweb kunnen ook andere verwerkingen plaatsvinden, afhankelijk van de keuzes, voorkeuren of instellingen van de betreffende Onderwijsinstelling:

- Het kunnen uitwisselen van leer- en toetsresultaten met leerlingadministratiesystemen van de Onderwijsinstelling.
- Het kunnen uitwisselen van leer- en toetsresultaten met dashboards die de Onderwijsinstelling in gebruik heeft.
- Sommige contactgegevens zijn optioneel, zoals het telefoonnummer van docenten/beheerders en het mailadres van leerlingen.

- Voor bovenschoolse besturen is het een optie om gebruikersstatistieken per school en per klas te (laten) verwerken.
- Verwerking van het e-mailadres voor nieuwsbrieven is optioneel en verloopt via opt-in.
- Het geven van een review over producten van Oefenweb is optioneel en verloopt via opt-in.
- Het bewaren van persoonsgegevens voor longitudinale onderzoeks- en productoptimalisatie projecten, zie artikel C voor toelichting en de mogelijkheid om hier bezwaar tegen te maken.

C. Bewaartermijnen en wetenschappelijk onderzoek

Persoonsgegevens van leerlingen en leerkrachten van scholen worden bewaard tot 12 maanden na het aflopen van het abonnement, tenzij Verantwoordelijke expliciet verzoekt om een kortere bewaartermijn. Hierdoor hebben scholen de gelegenheid om nog een jaar lang terug te kunnen kijken als ze nog willen weten hoe kinderen presteerden met het betreffende leermiddel van Oefenweb. Mocht een school bijvoorbeeld overstappen op een ander leermiddel, dan stelt dit de school tevens in staat om leerresultaten uit het nieuwe product te vergelijken met die van Oefenweb. Daarnaast stelt het scholen in staat om binnen een periode van 12 maanden terug te komen op hun beslissing om te stoppen met de producten van Oefenweb en kunnen leerlingen verdergaan waar ze waren gebleven.

Data wordt in volledig geanonimiseerde vorm voor onbeperkte termijn bewaard voor wetenschappelijk onderzoek. Voor wetenschappelijk onderzoek kan de geanonimiseerde data ook ter beschikking worden gesteld aan derden.

Er kunnen wetenschappelijke projecten of interne projecten ter verbetering van de producten van Oefenweb zijn waarvoor het ook na de termijn van 12 maanden van belang kan zijn om een koppeling te kunnen leggen tussen de geanonimiseerde onderzoeksdata en de persoonsgegevens van de gebruikers van Oefenweb. Een voorbeeld van een dergelijk project kan een onderzoek zijn naar de correlatie tussen de leerresultaten van leerlingen in de producten van Oefenweb en hun latere (leer)prestaties. Voor deze doeleinden bewaart Oefenweb in een daarvoor speciaal beveiligde omgeving een koppeling tussen de onderzoeksdata en de persoonsgegevens. Alleen medewerkers met het hoogste autorisatieniveau hebben toegang tot deze gegevens. Telkens geldt dat gewerkt wordt volgens de normen die voortvloeien uit huidige en toekomstige wet- en regelgeving. Mocht Verantwoordelijke bezwaar maken tegen de verwerking van persoonsgegevens voor dit doeleinde dan kan Verantwoordelijke dit kenbaar maken door een mail te sturen naar privacy@oefenweb.nl. De persoonsgegevens zullen dan niet bewaard worden.

Indien gebruikers van Oefenweb zich voor de nieuwsbrief hebben aangemeld (opt-in) dan blijven ze deze nieuwsbrief ontvangen ook als er geen klantrelatie met Oefenweb meer bestaat. Zij kunnen zich wel te allen tijde, zowel gedurende als na afloop van de klantrelatie, hiervoor afmelden. Oefenweb bewaart de contactgegevens van de contactpersoon (voornaam, achternaam, telefoonnummer, mailadres en functie) van de school ook na de termijn van 12 maanden in haar CRM-systeem, om informatie te kunnen verstrekken over soortgelijke producten of diensten als eerder werden afgenomen. De contactpersoon kan zich op ieder moment afmelden van het ontvangen van dergelijke berichten. In geval van expliciete afmelding of een uitdrukkelijk verzoek daartoe, worden de contactgegevens verwijderd uit het CRM-systeem. Contactgegevens, zowel voor de nieuwsbrief als het CRM-systeem, zullen alleen gebruikt worden om te informeren over de eigen producten van Oefenweb. Deze gegevens zullen nooit gedeeld worden met derden.

D. Categorieën en soorten Persoonsgegevens

Betrokkenen: Klant

Categorie	Toelichting
Contactgegevens	Naam, voornamen, geslacht (optioneel), telefoonnummer, adres, postcode en plaats. Voor de laatste gegevens is de verwachting dat de klant de gegevens van de school zal gebruiken
Financiën	Bankgegevens (bankrekeningnummer en verrichte betalingen). Oefenweb slaat zelf geen bankgegevens op, maar heeft wel inzicht in de betalingstransacties bij haar betaaldienstverlener.

Betrokkenen: Gebruikers – beheerders/docenten

Categorie	Toelichting
Contactgegevens	Naam, voornamen, e-mailadres, telefoonnummer (optioneel)
Onderwijs-deelnemer-nummer	Een administratienummer dat deelnemer identificeert. Optioneel: LAS-key, Basispoort ID en indien beschikbaar het ECK-ID
School/instellingsinformatie	Schoolnaam, klasnaam
Gebruiksinstellingen en handelingen	Aantal logins, handelingen die leerkracht op klasniveau uitvoert zoals spelinstelling
Technische gegevens	- Browseridentificatie (user agent) om in het geval van problemen te kunnen zien welke software gebruikt wordt door de klant en problemen op te lossen - IP-adres. Voor intern gebruik voor inzicht in gebruikersstatistieken en om misbruik (overbelasting netwerk) tegen te gaan.

Betrokkenen: Gebruikers – spelers (kinderen, scholieren, volwassenen)

Categorie	Toelichting
Contactgegevens	Naam, voornamen, geslacht, geboortedatum, leerjaar, e-mailadres (optioneel)
Onderwijs-deelnemer-nummer	Een administratienummer dat deelnemer identificeert. Optioneel: LAS-key, Basispoort ID en indien beschikbaar het ECK-ID
School/instellingsinformatie	Schoolnaam, leerkracht, klasnaam

Leerprestaties	Gemaakte opgaven inclusief antwoorden en reactietijden Daarvan afgeleide gegevens, zoals vaardigheidsscores, leerdoelscores en percentielscores
Gebruikinstellingen en handelingen	Hieronder vallen o.a. behaalde beloningen, beschikbare spellen, gekozen moeilijkheidsniveaus, aantal logins en bekeken instructievideo's
Technische gegevens	- Browseridentificatie (user agent) om in het geval van problemen te kunnen zien welke software gebruikt wordt door de klant en problemen op te lossen - IP-adres. Voor intern gebruik voor inzicht in gebruikersstatistieken en om misbruik (overbelasting netwerk) tegen te gaan.

E. Algemene informatie over getroffen beveiligingsmaatregelen:

Veiligheid staat voorop bij Oefenweb. Oefenweb stimuleert bewustzijn en training ten aanzien van privacy en informatiebeveiliging. Oefenweb neemt onder andere de volgende maatregelen:

- Iedere webapplicatie van Oefenweb is beveiligd met behulp van encryptietechnologie (SSL/TLS) om de uitwisseling van gegevens met Oefenweb te beveiligen.
- Er vinden dagelijks backups plaats om te voorkomen dat gegevens verloren gaan.
- Oefenweb hanteert een autorisatiebeleid om ervoor te zorgen dat medewerkers alleen toegang hebben tot Persoonsgegevens voor zover dat nodig is om hun werkzaamheden uit te voeren.

Een meer volledig overzicht van de genomen veiligheidsmaatregelen is opgenomen in Bijlage 2 bij de Verwerkersovereenkomst.

Audits

Verwerker zal alle medewerking verlenen die Verantwoordelijke redelijkerwijs nodig heeft voor het doen uitvoeren van een audit door een gekwalificeerde onafhankelijke auditor, om te controleren dat Verwerker diens verplichtingen onder deze overeenkomst nakomt. Een audit mag alleen uitgevoerd worden indien de Verantwoordelijke een concreet en op redelijk bewijs gebaseerd vermoeden heeft dat Verwerker diens verplichtingen onder de Verwerkersovereenkomst niet nakomt.

In ieder geval zal Verantwoordelijke (i) Verwerker tijdig op de hoogte stellen van haar voornemen een audit uit te voeren op grond van artikel 7.6, (ii) bewerkstelligen dat iedere door Verantwoordelijke ingeschakelde auditor voldoet aan de redelijke regels van Verwerker omtrent vertrouwelijkheid, gezondheid en veiligheid die Verwerker meedeelt aan Verantwoordelijke; en (iii) bewerkstelligen dat de audit zo wordt uitgevoerd dat belangrijke bedrijfsprocessen van Verwerker niet worden gehinderd.

Plaats/Land van opslag en Verwerking van de Persoonsgegevens

Verwerker zal geen persoonsgegevens van Verantwoordelijke doorgeven aan (een partij gevestigd in) een land dat door de Europese Unie niet is aangemerkt als een land waar privacy adequaat is beschermd, tenzij Verwerker met de betreffende partij een Verwerkersovereenkomst heeft gesloten waarbij de relevante door de Europese Commissie beschikbaar gestelde modelclausules zijn opgenomen, of in het geval van verwerking in de Verenigde Staten in ieder geval wordt voldaan aan de vereisten van het EU-U.S. Privacy Shield.

F. Subverwerkers

Verwerker maakt voor de dienstverlening gebruik van de volgende Subverwerkers:

- LeaseWeb is de hostingprovider die Oefenweb in staat stelt om haar applicaties beschikbaar te maken op het internet. Deze hostingprovider is gevestigd in Nederland.
- Hetzner is de hostingprovider waar backups van de data worden opgeslagen en de ontwikkelomgeving van Oefenweb staat. Deze hostingprovider is gevestigd in Duitsland.
- Buckaroo is de Payment Service Provider die Oefenweb gebruikt voor het verwerken van betalingen van de abonnementen op de producten van Oefenweb. Buckaroo is gevestigd in Nederland. Voor zover Buckaroo persoonsgegevens niet voor of namens Oefenweb verwerkt, zou Buckaroo als verwerkingsverantwoordelijke kunnen gelden, waarbij zij als financieel dienstverlener onder toezicht staat van de AFM en/of DNB.
- UvA Holding doet de financiële administratie voor Oefenweb en heeft voor dit doeleinde ook inzicht in de bestellingsgegevens (inclusief klantgegevens) van de klanten van Oefenweb. UvA Holding is gevestigd in Nederland.
- Google Apps is de e-mailprovider van Oefenweb, die het mogelijk maakt om per e-mail met Oefenweb te communiceren. Tevens wordt gebruik gemaakt van Google Drive voor documentenopslag. Oefenweb heeft met Google (een Amerikaans bedrijf) een Verwerkersovereenkomst met door de Europese Commissie vastgestelde modelclausules gesloten, om de bescherming van persoonsgegevens te waarborgen.
- Mailchimp is de dienst die Oefenweb gebruikt voor het versturen van nieuwsbrieven naar docenten en beheerders. Oefenweb heeft met Mailchimp (een Amerikaans bedrijf) een Verwerkersovereenkomst met door de Europese Commissie vastgestelde modelclausules gesloten, om de bescherming van persoonsgegevens te waarborgen.
- Kiyoh is de dienst die het mogelijk maakt om een review te geven over de producten van Oefenweb. Kiyoh is gevestigd in Nederland.

G. Contactgegevens

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

E-mail: privacy@oefenweb.nl

Telefoon: 020-8969444

H. Versie

Versie 3.0, laatst aangepast op 24 mei 2018.

Oefenweb kan de inhoud van deze Privacy Bijsluiter van tijd tot tijd bijwerken. De meest actuele versie staat altijd op www.oefenweb.nl/privacy. Bij belangrijke wijzigingen, zoals bijvoorbeeld het toevoegen van (sub)verwerkers, zal Oefenweb de Onderwijsinstelling hier actief (bijvoorbeeld per e-mail) over informeren. De Onderwijsinstelling heeft na in kennis te zijn gesteld van een (voorgestelde) wijziging 30 dagen de tijd om enig bezwaar tegen een wijziging gemotiveerd kenbaar te maken. Wanneer een dergelijke kennisgeving achterwege blijft, geldt de wijziging als aanvaard.

Deze Privacybijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <http://www.privacyconvenant.nl>.

BIJLAGE 2 bij Verwerkersovereenkomst Versie 3.0: Technische en organisatorische beveiligingsmaatregelen

De Verwerker is overeenkomstig de AVG en artikel 7 en 8 van de Verwerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens.

In deze bijlage wordt omschreven welke beveiligingsmaatregelen er door Oefenweb.nl B.V. (hierna te noemen: "Oefenweb") zijn getroffen. De beveiliging is een continu punt van aandacht en zorg.

Omschrijving van de maatregelen zoals bedoeld in artikel 7 van de Verwerkersovereenkomst

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

Oefenweb hanteert een autorisatiebeleid om ervoor te zorgen dat medewerkers alleen toegang hebben tot Persoonsgegevens voor zover dat nodig is om hun werkzaamheden uit te voeren.

Medewerkers en gegevens	Handelingen
Medewerkers van de klantenservice hebben toegang tot informatie over het abonnement en het gebruik daarvan.	Administratieve handelingen en ondersteuning aan de eindgebruiker.
Deskundigen op het gebied van ontwikkeling en analyse van lesmateriaal hebben toegang tot sets van resultaten van het gebruik van de leermiddelen.	Analyse van het lesmateriaal, gericht op verbetering van het materiaal, ontwikkeling en optimalisatie van adaptief lesmateriaal, opsporing en verbetering van fouten in de werking van het digitale leermiddel. In sommige gevallen tevens het beantwoorden van inhoudelijke vragen over leerresultaten.
IT- & databasebeheerders en ontwikkelaars hebben toegang tot de online applicaties die Oefenweb aanbiedt en bijbehorende (live) databases.	De handelingen van de IT- & databasebeheerders en ontwikkelaars zijn gericht op beschikbaarheid, continuïteit en optimalisatie van de ICT-systemen en software.

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

Hieronder wordt beschreven welke maatregelen Oefenweb heeft genomen om de Persoonsgegevens in haar applicaties te beschermen. In Bijlage 2a is tevens het ingevulde *Certificeringsschema informatiebeveiliging en privacy ROSA* te lezen.

Organisatie van informatiebeveiliging en communicatieprocessen

- Oefenweb heeft een Privacy & Security board om risico's omtrent de verwerking van persoonsgegevens te inventariseren, beveiligingsbewustzijn te stimuleren, voorzieningen te

controleren en maatregelen te treffen die toezien op naleving van het informatiebeveiligingsbeleid.

- Informatiebeveiligingsincidenten worden gedocumenteerd en worden benut voor optimalisatie van het informatiebeveiligingsbeleid.
- Oefenweb heeft een proces ingericht en gedocumenteerd voor communicatie over informatiebeveiligingsincidenten.

Medewerkers

- Met medewerkers (zowel intern als extern) worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
- Oefenweb stimuleert bewustzijn en training ten aanzien van privacy en informatiebeveiliging.
- Oefenweb hanteert een autorisatiebeleid om ervoor te zorgen dat medewerkers alleen toegang hebben tot Persoonsgegevens voor zover dat nodig is om hun werkzaamheden uit te voeren.

Fysieke beveiliging en continuïteit van de middelen

- Persoonsgegevens worden uitsluitend verwerkt in een fysieke omgeving die op passende wijze is beschermd tegen bedreigingen van buitenaf. Het datacenter waar de servers draaien is ISO 27001 gecertificeerd.
- De continuïteit van de dienstverlening en de beschikbaarheid van de Persoonsgegevens wordt extra gewaarborgd door 'geo-redundante' backups. Dit wil zeggen dat de gegevens op een alternatieve, veilige locatie beschikbaar zijn, voor het geval er iets ernstigs mocht gebeuren met de primaire locatie (zoals een overstroming, aanslag of brand).
- Er worden dagelijks (versleutelde) back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze back-ups worden vertrouwelijk behandeld en bewaard in een gesloten omgeving.
- De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's.

Netwerk-, server- en applicatiebeveiliging en onderhoud

- De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord om aanvallen, inbraken of inbraakpogingen zo snel mogelijk te detecteren.
- De digitale leeromgevingen waarbinnen persoonsgegevens worden verwerkt, komen tot stand op basis van een getrapte ontwikkelstraat. Oefenweb draagt er zorg voor dat deze altijd naar beste kunnen is ingericht om beveiligingslekken te vermijden.
- Op systemen worden periodiek de laatste (beveiligings-)patches geïnstalleerd op basis van patchmanagement.

- Op lokale werkstations en servers worden passende maatregelen genomen om te voorkomen dat kwaadaardige programmatuur of functionaliteit wordt geïnstalleerd.
- Op wachtwoorden worden cryptografische maatregelen (hashing) toegepast, van een kwaliteit die in de industrie over het algemeen als veilig wordt beschouwd, om deze gegevens veilig op te slaan. De enige uitzondering hierop is wachtwoorden van spelers die niet door henzelf zijn ingevoerd teneinde het wachtwoordenmanagement van leerkrachten en beheerders te faciliteren.
- Er wordt voor inlogprocessen gebruik gemaakt van versleutelde verbindingen.
- De uitwisseling van persoonsgegevens tussen de onderwijsinstelling en Oefenweb vindt versleuteld plaats.

III. Omschrijving van 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

Oefenweb neemt haar beveiliging periodiek onder de loep. Dit betreft o.a. een intern kwetsbaarhedenonderzoek en het reviewen van 'best practices' (bijvoorbeeld OWASP en de richtlijnen van het NCSC) op het gebied van beveiliging.

Rapportage en verbetering

Verwerker actualiseert haar beveiligingsmaatregelen en de informatie daarover in deze bijlage periodiek en informeert Verantwoordelijke over wijzigingen in de getroffen beveiligingsmaatregelen via www.oefenweb.nl/privacy.

In het geval u beveiligingsrisico's constateert, dan verzoeken wij u contact op te nemen met: privacy@oefenweb.nl of telefonisch via +3120-8969444.

Informeren over inbreuken (datalekken) met betrekking tot beveiliging

Oefenweb monitort haar dienstverlening voortdurend en heeft de in deze bijlage opgenomen maatregelen getroffen om ongeoorloofde of onrechtmatig toegang tot gegevens te voorkomen. Mocht er onverhoopt toch een inbreuk gesignaleerd worden, dan zal Oefenweb zo spoedig mogelijk melding hiervan maken bij de betreffende Verantwoordelijke in de zin van de Wet bescherming persoonsgegevens. Deze melding zal in eerste instantie plaatsvinden via e-mail. Mocht de situatie daar aanleiding toe geven, dan kan de melding tevens telefonisch worden gedaan, via een voor dat doeleinde vooraf aan Oefenweb te communiceren telefoonnummer. Voor de melding zal het e-mailadres dat is gekoppeld aan het beheerdersaccount van de betreffende Oefenweb applicatie worden gebruikt.

De melding zal in ieder geval de volgende informatie bevatten:

- De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
- De oorzaak van het beveiligingsincident;

- De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
- Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
- De omvang van de groep betrokkenen;
- Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

Indien een concrete situatie daartoe aanleiding geeft, dan kan Oefenweb 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

Versie 3.0, laatst aangepast op 24 mei 2018

Deze Beveiligingsbijlage maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 3.0, een initiatief van de PO-Raad, VO-raad, MBO Raad de verschillende betrokken ketenpartijen (GEU, KBb-E en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: <http://www.privacyconvenant.nl>.

BIJLAGE 2a bij Verwerkersovereenkomst Versie 3.0: Certificeringsschema informatiebeveiliging en ROSA

Toetsvorm	Self-assessment	
Uitvoerder toets	CTO	
BIV-classificatie	Beschikbaarheid = 2/3, Integriteit = 2, Vertrouwelijkheid = 2	
Categorie: Beschikbaarheid = 2/3		
<p>Oefenweb ontwikkelt additionele oefenprogramma's die vaak naast een methode gebruikt worden. De beschikbaarheid van deze programma's is belangrijk en Oefenweb richt haar systemen en processen zo in dat het zeer onwaarschijnlijk is dat deze gedurende een langere periode niet beschikbaar kunnen raken. De getroffen maatregelen komen overeen met niveau 2 en 3 van het ROSA certificeringsschema en hebben in de afgelopen jaren zeer goed gefunctioneerd. Oefenweb heeft vrijwel nooit te maken gehad met downtime en ook de RTO was hoog. Oefenweb plant onderhoudswerkzaamheden in principe buiten kantooruren.</p>		
Maatregelen	Compliance	Uitleg
Overbelasting	Voldaan	Op niveau 2
Business continuity	Voldaan	Op niveau 2
Ontwerp	Voldaan	Op niveau 3
Monitoring	Voldaan	Op niveau 3
Testen	Voldaan	Op niveau 3
Software	Voldaan	Op niveau 3
Actuele dreigingen	Voldaan	Op niveau 2
Categorie Integriteit = 2		
<p>De leerresultaten van Oefenweb betreffen formatieve data. Integriteit van deze data is belangrijk, maar er worden minder hoge eisen aan gesteld dan aan summatieve data. Bovendien kenmerkt de adaptieve technologie van Oefenweb zich door een doorlopende aanpassing van de leerresultaten op basis van de gemaakte opgaven van de leerling die ervoor zorgt dat een eventuele onjuistheid in de data snel weer gecorrigeerd wordt.</p> <p>Oefenweb heeft verschillende maatregelen genomen om de integriteit van de leerresultaten te waarborgen. In plaats van uitgebreide logging voorkomt Oefenweb dat de integriteit van de data überhaupt wordt aangetast door ongeoorloofde aanpassingen van de data doordat leerresultaten alleen kunnen worden aangepast op basis van de oefenprestaties van de leerlingen. Bij het gebruik van edexbestanden zijn bovendien contact- en feitelijke gegevens van leerlingen en leerkrachten ook niet meer aanpasbaar, met uitzondering van gebruikersnaam en wachtwoord. Daarnaast worden er dagelijks versleutelde backups gemaakt, gebruikt Oefenweb een autorisatiebeleid om ongeoorloofde toegang te voorkomen en hebben alleen IT-personen met de hoogste bevoegdheid rechten om aanpassingen op live databases door te voeren. Naast de al getroffen maatregelen is de uitbreiding van de logging in ontwikkeling.</p>		
Maatregelen	Compliance	Uitleg
Herleidbaarheid (gebruikers)	Voldaan met deels alternatieve maatregelen*	Belangrijke data (zoals leerresultaten) zijn niet aanpasbaar. Deze worden uitsluitend gebaseerd op speelgedrag. Speelgedrag kan, indien nodig, ongedaan gemaakt worden.
Backup	Voldaan	
Application controls	Voldaan	
Onweerlegbaarheid	Niet voldaan*	Uitbreiding logging is in ontwikkeling.

Herleidbaarheid (technische beheer)	Gedeeltelijk*	Voldaan op niveau 1
Controle integriteit	Voldaan met deels alternatieve maatregelen*	
Onweerlegbaarheid	Niet voldaan*	Uitbreiding logging is in ontwikkeling.
Actuele dreigingen	Voldaan met deels alternatieve maatregelen*	Oefenweb beperkt het gebruik van aanpalende systemen tot een minimum. Dit betreft alleen nog andere onderwijsdiensten, zoals Basispoort. Deze partijen zijn zelf ook verplicht om aan de benodigde technische maatregelen te voldoen.
Categorie Vertrouwelijkheid = 2		
Oefenweb verzamelt gegevens over leerlingen en de vorderingen die zij maken en de vertrouwelijkheid van deze gegevens is belangrijk. Deze en andere in de applicaties van Oefenweb verwerkte persoonsgegevens zijn op basis van autorisatiebeheer alleen toegankelijk voor personen die hier vanuit hun functie toegang toe moeten hebben (need-to-know basis). Daarnaast hanteert Oefenweb een ICT personeelsbeleid inclusief wachtwoordbeleid en zijn er procedures voor verificatie van gebruikers en/of klanten. Er is bovendien een strikte scheiding van veilige (trusted) en onveilige (not-trusted) apparatuur.		
Maatregelen	Compliance	Uitleg
Levenscyclus gegevens	Voldaan	
Logische toegang	Voldaan	
Fysieke toegang	Voldaan	
Netwerk toegang	Voldaan met deels alternatieve maatregelen*	
Scheiding omgevingen	Voldaan	
Transport en fysieke opslag	Voldaan	
Logging	Niet voldaan*	Uitbreiding logging is in ontwikkeling.
Toetsing	Voldaan	
Actuele dreigingen	Voldaan	

* Vertrouwelijk op aanvraag in te zien.