Model Verwerkersovereenkomst 3.0

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

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 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 Pearson Benelux B.V., gevestigd en kantoorhoudende aan Gatwickstraat 1, te 1043 GK, Amsterdam, te dezen rechtsgeldig vertegenwoordigd door Jurgen Verhaegen - Sales and Marketing Director , hierna te noemen: "**Verwerker**"

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

Overwegen het volgende:

a. Onderwijsinstelling en Verwerker zijn een overeenkomst aangegaan waarbij de onderwijsinstelling MyEnglishLab heeft aangeschaft ('de Product- en Dienstenovereenkomst'). Deze Product- en Dienstenovereenkomst leidt ertoe dat Verwerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.

b. 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:

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 toegetreden 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 verwerkingsactiviteiten[1] 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.
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. *<u>SPECIFIEKE BEPALING VOOR VERWERKERSOVEREENKOMSTEN TUSSEN ONDERWIJSINSTELLINGEN EN DISTRIBUTEURS</u>:*

    a. *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).*

    b. *Verwerker (de distributeur) wisselt in opdracht van de Onderwijsinstelling gegevens uit met deze Leermiddelenleveranciers.*

    c. *De Onderwijsinstelling is verantwoordelijk voor het maken en vastleggen van afspraken met iedere Leermiddelenleverancier in een Verwerkersovereenkomst.*

    d. *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).*

    e. *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:
    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 voortkomende 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 beschreven in Annex 1 bij deze overeenkomst en naar andere derde landen of internationale organisaties 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: _____

Naam:_____

Functie:_____

Datum:_____

Handtekening _____

Verwerker: Pearson Benelux BV

Naam: Jurgen Verhaegen

Functie: Sales and Marketing Director

Datum:_____

Handtekening _____

Bijlage 1: Privacybijsluiter

Bijlage 2: Beveiligingsbijlage

BIJLAGE 1: PRIVACYBIJSLUITER [MyEnglishLab: po, vo en mbo]

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. De Privacybijsluiter is een bijlage bij de Modelverwerkersovereenkomst en omvat de Instructies voor de Verwerking van Persoonsgegevens van de Onderwijsinstelling aan de Verwerker.

In het kader van de herkenbaarheid is het wenselijk dat Verwerkers zo veel mogelijk op uniforme wijze gebruik maken van de Privacybijsluiter. Afwijkingen van dit model zijn weliswaar mogelijk, maar dienen bij voorkeur beperkt te blijven. Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in separate Bijlage(n), welke als volgt genummerd worden: "Bijlage 1A", "Bijlage 1B", etc.. Deze Bijlagen worden aan de Verwerkersovereenkomst gehecht.

Voor specifieke branches zoals uitgevers, distributeurs en leveranciers van student- en leerling-administratiesystemen, kunnen specifieke privacybijsluiters worden gemaakt die gebaseerd zijn op dit model. Deze specifieke modellen zijn afgestemd door de Initiatiefnemers van het Convenant. De modellen zijn te vinden op de website van het Platform: www.edu-k.nl/ibp.

A. Algemene informatie

Naam product en/of dienst*: MyEnglishLab*

Naam Verwerker en vestigingsgegevens: *Pearson Benelux BV, Gatwickstraat 1, 1043, GK Amsterdam, The Netherlands*

Link naar leverancier en/of productpagina: *www.pearson.com/nl/*

Beknopte uitleg en werking product en dienst: *interactieve digitale middelen die vooral voor zelfstudie op een interactieve manier gebruikt worden.*

Doelgroep (zoals po/vo, onderbouw/bovenbouw): *leerlingen en studenten uit verschillende groepen en van verschillende onderwijssegmenten (basisonderwijs, middelbaar onderwijs, hoger onderwijs en universitair onderwijs).*

Gebruikers onderwijsdeelnemers/ouders/verzorgers/docenten/: *Docent van bovengenoemde leerlingen en studenten*.

B. Omschrijving specifieke diensten

Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen van Persoonsgegevens:

Bovengenoemde digitale middelen zijn alle leermiddelen die leerlingen gebruiken om hun leerresultaten te verbeteren. Leerlingen loggen zelf in en kunnen dan vragen beantwoorden en oefeningen maken. In

het 'grade book' worden de resultaten weergegeven, die zichtbaar zijn voor de leerling en zijn/haar docent, die de klas in het systeem heeft aangemaakt.

C. Doeleinden voor het verwerken van gegevens

De Verwerker is leverancier van een digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen. Indien de Verwerker leverancier is van een digitaal product en/of digitale dienst bestaande uit Leermiddelen en Toetsen, dan zijn de volgende mogelijke doelstellingen van gegevensverwerking in het kader van deze producten en diensten van toepassing:

a. het met gebruikmaking van het Digitale Onderwijsmiddel geven en volgen van onderwijs en het begeleiden en volgen van Onderwijsdeelnemers, waaronder:

- 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 Onderwijsdeelnemer;
- analyse en interpretatie van leerresultaten;
- het kunnen uitwisselen van leer- en toetsresultaten tussen Digitale Onderwijsmiddelen.

b. het geleverd krijgen/in gebruik kunnen nemen van Digitale Onderwijsmiddelen conform de afspraken die zijn gemaakt tussen de Onderwijsinstelling en de Leverancier;

c. het verkrijgen van toegang tot de aangeboden Digitale Onderwijsmiddelen, en externe informatiesystemen, waaronder de identificatie, authenticatie en autorisatie;

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.

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;

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;

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.

h. het beschikbaar stellen van Persoonsgegevens voor zover noodzakelijk om te kunnen voldoen aan de wettelijke eisen die worden gesteld aan Digitale Onderwijsmiddelen.

i. De uitvoering of toepassing van een andere wet.

D. Categorieën en soorten persoonsgegevens

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

Van toepassing	Categorie	Toelichting
van toepassing	**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;
niet van toepassing	**2. Onderwijs-deelnemernummer**	een administratienummer dat onderwijsdeelnemers identificeert
niet van toepassing	**3.Nationaliteit en geboorteplaats**	
niet van toepassing	**4. Ouders, voogd**	gegevens als bedoeld onder 1, van de ouders/verzorgers van onderwijsdeelnemers
niet van toepassing	**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;
niet van toepassing	**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;
van toepassing	**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
niet van toepassing	**8. Onderwijsorganisatie**	gegevens met het oog op de **organisatie van het onderwijs** en het verstrekken of ter beschikking stellen van leermiddelen;
niet van toepassing	**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;
niet van toepassing	**10. Beeldmateriaal**	foto's en videobeelden **(beeldmateriaal)** met of zonder geluid van activiteiten van de instelling of het instituut;
van toepassing	**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;
niet van toepassing	**12 Overige gegevens, te weten ….**	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.**
niet van toepassing	**13. BSN/PGN**	
van toepassing	**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.

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

Pearson bewaart deze persoonsgegevens voor de duur van het contract tussen de school en Pearson voor de levering van MEL en vervolgens voor maximaal 12 maanden om de toegang voor scholen en studenten mogelijk te maken om de resultaten enz. te verifiëren en daarna voor 2 jaar voor ondersteuning en onderzoeksdoeleinden. Daarna worden de gegevens geanonimiseerd door het verwijderen van naam, e-mailadres en gebruikersnaam.

E. Opslag Verwerking Persoonsgegevens:

Plaats/Land van opslag en Verwerking van de Persoonsgegevens:

Amazon Web Services verwerkt de bovenstaande data (7,11) in Ierland om het voor studenten en docenten mogelijk te maken het product te gebruiken.

Pearson Education INC heeft onderaannemers aangesteld in de VS die de bovenstaande data (1) verwerken om toe te laten dat studenten en docenten toegang te krijgen tot het product.

Wanneer gegevens in de VS worden verwerkt, is er tussen Pearson Benelux BV en Pearson Education Inc. een intercompany-overeenkomst van kracht die voldoet aan de vereisten van de AVG voor de overdracht van persoonsgegevens naar landen buiten de EER, die worden gezien als onvoldoende bescherming van persoonsgegevens biedend.
Pearson Education Inc. heeft met al haar onderaannemers die persoonsgegevens verwerken een verwerkersovereenkomst gesloten die voldoet aan de vereisten van artikel 28 van de AVG.

F. 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: Zie punt E hierboven

G. Contactgegevens

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

Pearson Benelux BV, Gatwickstraat, 1043 GK Amsterdam. Telefoon: 020-575 5800 of via de mail: elt.service@pearson.com

H. Versie

Opgemaakt op 06-12-2018.

BIJLAGE 2: BEVEILIGINGSBIJLAGE

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

Normen informatiebeveiliging

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

Voor het toepassen en aantonen van de technische maatregelen, kan Verwerker gebruik maken van (zo snel als redelijkerwijs mogelijk de meest recente versie van) het in het onderwijs ontwikkelde '*Certificeringsschema informatiebeveiliging en privacy ROSA*'[2]. Dat schema voorziet in een baseline van (beveiligings)maatregelen waarmee organisaties dit aantoonbaar kunnen maken.

Indien Verwerker voornoemd Certificeringsschema gebruikt, dan mag gebruik worden gemaakt van een standaard beveiligingsbijlage die is afgestemd door de Initiatiefnemers van het Convenant. Deze afgestemde bijlage 2 is te vinden op de website van het Platform en komt in de plaats van deze model bijlage 2: www.edu-k.nl/ibp.

Verwerker kan ook gebruik maken van andere certificeringsmechanismen en/of (inter)nationaal erkende normen en standaarden voor informatiebeveiliging, mits die een gelijkwaardig of hoger niveau van beveiliging bieden en de door Verwerker genomen maatregelen aan de Onderwijsinstelling inzichtelijk worden gemaakt.

Minimale beveiligingsmaatregelen en aantoonbaarheid

Verwerker plaatst op deze plek in de bijlage een verklaring waaruit blijkt dat voldaan wordt aan passende technische maatregelen voor de beveiliging van de Verwerking van Persoonsgegevens. Deze verklaring bevat ten minste:

a. Een classificatie van het product of de dienst op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid;

b. Een beschrijving in welke mate aan de hieronder genoemde minimale beveiligingsmaatregelen in het kader van artikel 32 AVG wordt voldaan;

    1. Verwerker heeft een passend beleid voor de beveiliging van de Verwerking van de Persoonsgegevens, waarbij het beleid periodiek wordt geëvalueerd en – zo nodig – aangepast;

    2. Verwerker heeft de Persoonsgegevens die worden Verwerkt geclassificeerd op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid en heeft op basis

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

van die classificatie beveiligingsmaatregelen genomen om de risico's voor de Verwerking van Persoonsgegevens te beperken;

3. Verwerker neemt maatregelen zodat via een systeem van autorisatie enkel geautoriseerde medewerkers toegang kunnen verkrijgen tot de Verwerking van Persoonsgegevens in het kader van de Verwerkersovereenkomst. Hierbij heeft Verwerker procedures vastgesteld en gedeeld met de Onderwijsinstelling voor de identificatie, autorisatie en authenticatie van medewerkers alsmede rondom de registratie, aanmelding en afmelding van de medewerkers;
4. Verwerker zorgt dat de toegang tot het product of de dienst beveiligd is door middel van een passend beleid voor wachtwoorden dat aansluit bij de stand van de techniek;
5. Verwerker heeft procedures voor 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 Certificeringsschema informatiebeveiliging en privacy ROSA). De Onderwijsinstelling wordt in de gelegenheid gesteld om deze logbestanden periodiek te controleren;
6. Verwerker heeft maatregelen genomen om de Persoonsgegevens te beschermen tegen verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
7. Verwerker maakt bij de beveiliging van de Verwerking van Persoonsgegevens gebruik van een (inter)nationale beveiligingsnorm;
8. Verwerker heeft maatregelen genomen 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.

c. Een toetsing van getroffen maatregelen aan (inter)nationaal erkende normen en standaarden voor informatiebeveiliging.
   - Pearson heeft een Data Security and Privacy Policy als onderdeel van een Information Management System dat voldoet aan ISO27001;2013. Dit wordt elk jaar hierzien en aangepast indien nodig.
   - Pearson heeft een Data Labelling and Classification Policy die belangrijke gegevens, waaronder persoonsgegevens, classificeert. Dit zorgt ervoor dat de juiste beveiligingsmaatregelen, inclusief de verwerkingsbeperking, worden ingezet voor de beschikbaarheid, integriteit en vertrouwelijkheid.
   - Pearson heeft een Access Control Policy die ervoor zorgt dat enkel de juiste gebruikers op het juiste moment de juiste toegang krijgen tot Persoonsgegevens.
   - Pearson heeft een Password Control Security Policy die voldoet aan de beste werkwijzen van de industrie op het gebied van wachtwoordcontroles of deze overtreft.
   - General Security Overview bijgevoegd als Bijlage 1.

Monitoring en identificatie van incidenten;
Pearson en onze beveiligingspartners doen actief onderzoek naar potentiële kwetsbaarheden over de hele wereld en nemen deze informatie op in hun doorlopende applicatiemonitoring.

- **Systeemmonitoring –** Servermonitoring wordt zowel op het niveau van het besturingssysteem als op het niveau van de applicatielevering uitgevoerd met behulp van netwerk-, host- en servicemonitoringsystemen.
- **Operating system level monitors** omvatten CPU-, schijf-, netwerk- en ping-gezondheidscontroles.
- **Applicatiespecifieke tests** zijn ontwikkeld om individuele elementen van de application delivery stack te toetsen, zoals databaseconnectiviteit en applicatie-webniveaus.
- **Parameters** zoals inkomend en uitgaand netwerkgebruik, CPU, schijfgebruik en I/O worden in realtime bewaakt en kunnen worden bekeken.
- **Auditing** is ingeschakeld voor standaard systeemfuncties zoals gebruikersauthenticatie en activiteit op alle Pearson Learning Technology platforms.
- **Dedicated Operations Support team (Ops) –** Het Operations Support team is 24/7 actief en ontvangt alle waarschuwingen van lopende besturingssystemen en service-level monitors. Ops is verantwoordelijk voor 24/7 reactie op verstoringen van de dienstverlening of kritieke systeem- en beveiligingsgebeurtenissen. Voor alle systemen zijn duidelijk omschreven resolutie- en escalatiepaden gedefinieerd.
- **Security Monitoring** - Pearson maakt gebruik van inbraakdetectiesystemen (IDS), web applicatie firewalls (WAF), en Security Incident en Event Management (SIEM)-systemen om beveiligingsincidenten te monitoren.
- **Logging** - Pearson-systemen implementeren het juiste niveau van logging op applicatie-, webserver-, en database-, en besturingssysteemniveau.

Beveilingsincidenten en/of datalekken:

Bij een (vermoeden van) een beveiligingsincident en/of datalek, kan de Onderwijsinstelling contact opnemen met: Pearsons Security Operations Centre 363x24x7 at soc@pearson.com
In het geval van een datalek zal Pearson
A. bepalen of het lek waarschijnlijk zal leiden tot een risico voor de rechten en vrijheden van natuurlijke personen, rekening houdend met relevante factoren; of de betrokken personen bijvoorbeeld worden bedreigd met identiteitsdiefstal, of "bijzondere categorieën" gegevens in gevaar zijn, of de gegevens van kinderen of kwetsbare personen in gevaar zijn;
B. wanneer het lek een risico voor de rechten en vrijheden van natuurlijke personen met zich meebrengt, het voorval vastleggen en de Klant via de normale relatiemanager van de Klant de volgende informatie verstrekken, voor zover beschikbaar, en de Klant bijstaan bij het doen van de meldingen, zoals vereist, aan de toezichthouder in Nederland;

- Een omschrijving van het lek
- Het geschatte aantal gelekte persoonsgegevens
- De getroffen categorieën van gegevens
- De contactgegevens van Pearsons Data Protection Officer
- De waarschijnlijke gevolgen van het lek
- De genomen of voorgestelde maatregelen om het lek aan te pakken
- Wanneer het lek plaats heeft gevonden
- Over welke middelen Pearson beschikte om het lek te voorkomen
- Wat Pearson heeft gedaan om de getroffen personen te helpen

- Wat hieruit geleerd is
- Welke voorzorgsmaatregelen Pearson toepast om dergelijke lekken in de toekomst te voorkomen

C. de polite/justitie, verzekeraars, banken/creditcardmaatschappijen, zoals vereist, op de hoogte stellen

D. personeel beschikbaar stellen voor de betreffende toezichthouder in het geval van een onderzoek.

Beveiligingsincidenten en/of datalekken:

In geval van een (vermoeden van) beveiligingsincident en/of datalek, kan Onderwijsinstelling contact opnemen met: Pearson's Security Operations Centre 363x24x7 via soc@pearson.com

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging
Er is een procedure over het informeren in geval van datalekken en/of incidenten met betrekking tot beveiliging, en bevat ten minste te volgende punten:

- De wijze waarop monitoring en identificatie van incidenten plaatsvindt,
- De wijze waarop informatie wordt gedeeld:
  - Op welke manier (via e-mail, telefoon);
  - Aan wie gericht (contactpersonen en contactgegevens);
  - Met wie kan (bij vervolgacties) contact worden opgenomen.
- Informatie die in ieder geval over een incident gedeeld moet worden

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

De oorzaak van het beveiligingsincident;

De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;

Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;

De omvang van de groep betrokkenen;

Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).

- Eventuele afspraken of, en zo ja hoe, Verwerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie 1. Opgemaakt op 19 december 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 - Algemeen Beveiligingsoverzicht

Bij Pearson erkennen we dat onze Onderwijspartners, Studenten en Klanten steeds bezorgder zijn over veiligheid, privacy en de betrouwbare beschikbaarheid van online leerapplicaties. De informatie in dit document kan worden gedeeld met klanten, potentiële klanten en externe partners van Pearson en is van toepassing op de volgende Pearson-applicaties;

Pearson is toegewijd aan de beveiliging en beschikbaarheid van onze online leerapplicaties. Pearson beschikt over de modernste technologische middelen en hosting-apparatuur die voldoen aan de behoeften voor de huidige kritische applicaties of deze overstijgen. De bescherming van gevoelige gegevens, of het nu gaat om die van Pearson of die van onze Onderwijspartners en Studenten vormt een belangrijk onderdeel van onze kernwaarden.

1. Inleiding

Dit document beschrijft de controleomgeving en beveiligingspraktijken voor Pearson online leersystemen. Het geeft een overzicht van basisbeveiligingsinformatie zonder details te verstrekken die de veiligheid van de Pearson-werkomgeving in gevaar kunnen brengen.

- Herzieningen en updates – Dit document wordt regelmatig herzien en bijgewerkt om zo de huidige beveiligingspraktijken voor Pearson online leersystemen weer te geven.

2. Organisatorische beveiliging

Pearson heeft een wereldwijde beveiligingsorganisatie opgezet met de volgende sleutelrollen:

- Chief Information Security Officer
- Business Information Security Officers
- Regional Information Security Officers
- Chief Information Privacy Officer
- Data Security and Privacy Boards Governance - de opdracht van de gegevensbeveiligings- en privacycommissie is om te bewerkstelligen dat Pearson geldt als een ethische leider op het gebied van beveiliging en privacy door het instellen van wereldwijde bestuurbeleidsvormen en normen die Pearsons bedrijfsstrategie mogelijk maken, risico's beheren en de privacy van de personen die Pearson dient in overeenstemming met alle nalevingsvoorschriften, relevante en van toepassing zijnde beleidsregels en wetten eerbiedigen en beschermen.
- Security Engineering – het security engineering team ontwerpt en onderhoudt de beveiligingsinfrastructuur en -diensten voor Pearsons wereldwijde infrastructuur en IT-platformen.
- Application Security - is verantwoordelijk voor de beveiliging van de lesbeheerapplicaties van Pearson. Het team verzorgt geregelde beveiligingsevaluaties van Pearson-producten, organiseert cursussen en levert advies over toonaangevende praktijken voor het ontwikkelen van veilige applicaties en integreert beveiligingsprincipes voor Pearsons secure development life cycle programma's.
- Security Operations Center - het 24x7 SOC monitort en neemt actie op beveiligingsincidenten.

3. Beveiligingsbeleid

Pearson maakt gebruik van de Information Security 27002 (ISO 27002)-norm als basis voor het

opbouwen van ons wereldwijde beveiligingsbeleid en -normen.

- Information Security Policies en Standards - dekken alle gebieden van gegevensbeveiliging af, met inbegrip van, maar niet beperkt tot, personeelsbeveiliging, fysieke beveiliging, computer- en netwerkbeheer en toegangscontrole. Om het risico te beperken dat Pearson hosting en andere systemen in gevaar worden gebracht, wordt de inhoud van deze beleidsonderdelen niet openbaar gemaakt. De Information Security Policies worden ten minste eenmaal per jaar herzien en bijgewerkt met goedkeuring van de Chief Information Officer, Chief Technology Officers, Security en Privacy Officers.

4. Personeelsbeveiliging

- Pearson Gedragscode - Elke Pearson-medewerker is jaarlijks verplicht om de Pearson Gedragscode, die hoge ethische normen voor het personeel van Pearson en een aanvaardbaar gebruik van Pearson-activa vaststelt, te lezen en hiermee akkoord te gaan.
Pearsons Zakelijke Gedragscodebeleid weerspiegelt het engagement van het bedrijf om ervoor te zorgen dat haar medewerkers en dienstverleners de criteria en het belang van professioneel verantwoord handelen begrijpen.
- Achtergrondcontroles - Pearsons getalenteerde ingenieurs en ondersteunend personeel vormen de basis van ons bedrijf. Pearson maakt gebruik van derden om achtergrondcontroles uit te voeren voordat zij personeel in dienst neemt, met inbegrip van strafrechtelijke controles en controle van de opleidingen en referenties over de afgelopen zeven jaar.
- Beheer van toegang van medewerkers en dienstverleners tot bedrijfsgegevens en activa. – Pearson heeft een formeel proces dat gebruikt wordt om de toegang van medewerkers tot gegevens en/of alle bedrijfsmiddelen toe te wijzen, te beperken of te verwijderen als gevolg van verhuizingen, statuswijzigingen, nieuw aangenomen personeel en opzeggingen.
- Unieke inloggegevens - Elke Pearson-medewerker of persoon in dienst van door een Pearson goedgekeurde dienstverlener heeft zijn eigen unieke inlognaam en wachtwoord voor toegang tot door Pearson beheerde systemen.
- Role Based Access - De toegang tot de Pearson-systemen wordt geregeld door een gelaagd beheersysteem voor gebruikersrechten. Pearson beperkt de toegang tot gebruikersinformatie voor klantenondersteuning en systeemonderhoudspersoneel op een need-to-know basis voor het uitvoeren van de vereiste bedrijfsfuncties.
- Medewerkerstraining voor het omgaan met gevoelige informatie - Pearson biedt Information Security Awareness en Data Privacy training om ervoor te zorgen dat medewerkers hun verantwoordelijkheden begrijpen bij het omgaan met gevoelige informatie.

5. Beveiligingstraining

Medewerkers van Pearson krijgen training op het gebied van informatiebeveiliging en bedrijfsethiek, zowel op het moment van indiensttreding als doorlopend tijdens hun dienstverband bij Pearson. Daarnaast versterkt Pearsons Information Security team de beste werkwijzen op het gebied van informatiebeveiliging door middel van memo's en meldingen op intranet en beveiligingsbewustheidssessies met personeel ter plaatse. Extra beveiligingstraining wordt gegeven aan Pearsons ontwikkelaarsgemeenschap via persoonlijke sessies, webinars en online cursussen.

6. Beveiliging Datacenter

Pearson maakt gebruik van de beste faciliteiten van datacenteraanbieders op meerdere locaties voor het plaatsen en beveiligen van haar applicatieservers.

- Internet Datacenters – Pearson sluit contracten met internet- datacenteraanbieders voor de fysieke hosting van onze online leerapplicatie-infrastructuur. Deze dienstverleners zijn verplicht om te voldoen aan de Pearson-normen met betrekking tot informatiebeveiliging en vertrouwelijkheid of deze te overtreffen.
- Plaatsing apparatuur bij datacenters - Alle systemen worden geplaatst in gesloten kooien of volledig daartoe ingerichte en gecontroleerde locaties binnen de hosting faciliteiten. Deze faciliteiten bieden een veilige en betrouwbare infrastructuur voor direct beschikbare applicaties die wereldwijd worden gebruikt. De hoogste kwaliteit apparatuur, technologieën en personeel worden ingezet om de prestaties, betrouwbaarheid en veiligheid te garanderen.
- Controle van fysieke toegang bij datacenters - Fysieke toegang tot de kooilocaties is beperkt tot personen die op de goedgekeurde toegangscontrolelijst staan. Deze personen moeten een foto-identificatie tonen aan bewakers die 24 uur per dag, 7 dagen per week paraat zijn. Bepaald Pearson-personeel of goedgekeurde Pearson-dienstverleners behouden te allen tijde fysieke toegangsbevoegdheid. Permanente toegang tot Pearson-systemen is beperkt tot medewerkers van Pearson met een 'noodzaak voor toegang'.

7. Netwerk- en communicatiebeveiliging

Al het netwerkverkeer tussen klanten en Pearson Education-systemen verloopt via het internet. Pearson Education-applicaties zijn gebaseerd op webbrowsers en afhankelijk van HTTP-verkeer. Niet-http-verkeer bestaat uit beperkte browser plug-ins en streaming media (audio en video), geleverd door een commercieel gedistribueerd content delivery netwerk.

- Secure Socket Layer (SSL/TLS) – Alle Pearson Education-applicaties met SSL/TLS voor openbaar gebruik zijn afhankelijk van ondertekende Certificate of Authority (CA)-certificaten. Zelf ondertekende certificaten worden niet gebruikt. SSL-encryptie is 128-bits of hoger.
- Firewalls en Schakel- en Routingapparatuur - Alle Pearson Education-systemen bevinden zich achter uitvoerige firewalls van bedrijfsklasse-niveau. Pearson Education implementeert alle firewalls met behulp van goedgekeurde configuratienormen, die ten minste eenmaal per jaar worden getest, gecontroleerd en herzien. Als kritisch onderdeel van de geïntegreerde beveiligingsstrategie van het bedrijf, maakt Pearson gebruik van commerciële schakel- en routingapparatuur op bedrijfsklasse-niveau die voldoet aan en verder gaat dan de industrienormen zoals vastgesteld door de Federal Information Processing Standards (FIPS), Internet Computer Security Association (ICSA), en Common Criteria-certificeringen. De interne netwerktopologie wordt verborgen door Network Address Translation (NAT). De diensten worden openbaar gemaakt met virtuele IP-adressen (VIP's).
- Intrusion Detection - toegangslinks van het internet worden gemonitord door de Intrusion Detection Service die dataverkeersgegevens doorstuurt naar event monitoring en correlatieplatforms die ontworpen zijn om abnormaal dataverkeer op te sporen.
- Administratieve connectiviteit - Administratieve connectiviteit met individuele servers is strikt beperkt tot mensen op een 'noodzaak tot toegang'-basis. Er is geen draadloze connectiviteit aanwezig in de datacenters.
- Pearson versterkt alle systemen die worden ingezet vanaf de eerste bare metal-

installatie. Standaard besturingssystemen worden niet gebruikt door Pearson Learning Technologies-systemen. Pearson Learning Technologies maakt gebruik van besturingssysteeminstallaties die alle onnodige diensten verwijderen of uitschakelen, passende routing-configuratie vooraf definiëren en de meest recente ondersteunde patch-niveaus configureren.

- Niet-openbaarmaking van Pearson Education besturingssysteem of software versie niveaus - Pearson maakt deze informatie niet openbaar omdat deze gebruikt kan worden voor het identificeren van potentiële kwetsbaarheden of mogelijke aanvalsvectoren. Verder maakt Pearson Learning Technologies de configuratie van haar webservers, applicaties of databases niet bekend, aangezien een dergelijke openbaarmaking interne netwerktopologie, specifieke servers of diensten die op specifieke poorten draaien kan onthullen, en deze kunnen worden gebruikt bij het ontwerpen of de uitvoering van een aanval.
- Gebruikersauthenticatie - Authenticatie/autorisatie-verzoeken aan Pearson Education webapplicaties worden behandeld voordat toegang tot het eCollege-systeem wordt verkregen. De beveiligingsarchitectuur wordt beoordeeld door een team van systeemarchitecten en applicatiesoftware-architecten. Code reviews worden standaard uitgevoerd binnen de ontwikkeling van webapplicaties.
- Back-ups en kopieën van gegevens - Back-ups van applicatie-inhoud en gebruikersgegevens worden 's nachts gemaakt. Volledige back-ups worden van tijd tot tijd gemaakt. Op regelmatige basis worden kopieën van deze back-ups gecodeerd met behulp van industriestandaard-software en deze worden offsite naar een beveiligde site van een derde gestuurd voor opslag.

8. Netwerkscans

Pearson heeft één enkel, wereldwijd programma voor het scannen en beheren van netwerken voor de gehele server/hosting omgeving. De dekking omvat co-located en cloud-based servers, evenals alle datacenters die rechtstreeks door Pearson worden beheerd. Scans worden uitgevoerd op een permanente periodieke basis voor alle servers / netwerken in kwestie, kritische applicaties en diensten worden vaker gescand, afhankelijk van de zwaarte en noodzaak.

Kwetsbaarheden die als onderdeel van het kwetsbaarheidsbeheerprogramma van Pearson zijn ontdekt, worden beoordeeld, verzameld en aan de individuele applicatie- en systeemeigenaren voorgelegd voor herstel. Pearson traceert vervolgens het risico van deze kwetsbaarheden en stelt vast waar herstel, extra aandacht of escalatie vereist is door middel van een Risk Exception-proces.

Wanneer zeer kritieke kwetsbaarheden worden aangetoond, of bedreigingen worden beoordeeld als zijnde van hoge prioriteit, voert Pearson een globaal herstelplan uit onafhankelijk van het scannen van netwerken om ervoor te zorgen dat de tijdspanne tussen kwetsbaarheid en sluiting zo klein mogelijk is.

- Pearson staat klanten niet toe kwetsbaarheids- of penetratiescans uit te voeren op Pearson-producten die gedeeld worden met andere klanten.
- Pearson mag de uitkomsten van onze beveiligingsbeoordelingen met onze klanten delen.
- Wij leveren hoogstaande samenvattingen via email op basis van geheimhouding.

- Wij delen de werkelijke kwetsbaarheidsgegevens ter plekke en in persoon.

9. Beheer van beveiligingspatches

Pearson heeft een OS layer beveiligingspatchprogramma opgezet dat het volgende omvat

- een Global Threat Monitoring team dat leveranciers en beveiligingsadviezen controleert en interne teams waarschuwt als er een beveiligingskwetsbaarheid is gepubliceerd die onze infrastructuur kan aantasten.
- een netwerkscanprogramma om ervoor te zorgen dat patch intelligence wordt verstrekt aan beveiligings- en infrastructuurteams.
- een op risico gebaseerd prioriterings- en rapportagemechanisme.

Over het algemeen worden elk kwartaal niet-kritische beveiligingspatches ingezet om voldoende planning en testen mogelijk te maken. Patches worden naar ontwikkelings-, staging- en vervolgens naar productieomgevingen uitgerold. Een out-of-band noodpatchbeheerproces wordt gebruikt wanneer beveiligingspatches vanwege risico's een snelle inzet vereisen.

10. Beheer van informatiebeveiliging door derden en leveranciers

Pearson heeft een uiterst robuust Vendor Information Security Management Program dat de pre-contractuele besprekingen, de eis voor de verkoper om in te stemmen met een uitputtende set veiligheidseisen, en lopende audits en contractbeoordelingen omvat.

11. Veilige ontwikkelingslevenscyclus

Pearsons Application Security team beheert Pearsons veilige ontwikkelingslevenscyclusprocessen en bevat een aantal componenten:

- Beveiligingstraining voor ontwikkelaars. Beveiligingstraining wordt gegeven aan Pearsons ontwikkelaarsgemeenschap via persoonlijke sessies, webinars en online cursussen.
- Beveiligingsscannen van statische code. Pearson maakt gebruik van statische code netwerkscanning tools zoals Veracode om coderegisters te scannen, beveiligingskwetsbaarheden te rapporteren en op risico te rangschikken en ontwikkelaars en mitigatietechnieken te adviseren.
- Dynamische kwetsbaarheid van webapplicaties. Pearson maakt gebruik van dynamische webapplicatiebeveiligings netwerkscanning tools om continu webapplicaties te scannen en beveiligingskwetsbaarheden op te sporen, te rapporteren en op risico te rangschikken.

12. Monitoring

Pearson Education en onze veiligheidspartners doen actief onderzoek naar potentiële kwetsbaarheden over de hele wereld en nemen deze informatie op in hun doorlopende applicatiemonitoring.

- Systeemmonitoring – Servermonitoring wordt uitgevoerd op zowel het niveau van het besturingssysteem als op het niveau van de applicatielevering met behulp van netwerk-, host- en servicemonitoringsystemen.
- De monitoring op besturingssysteemniveau omvat CPU-, schijf-, netwerk- en ping-health checks.
- Applicatiespecifieke tests zijn ontwikkeld om individuele elementen van de application delivery stack te testen, zoals databaseconnectiviteit en applicatie-webniveaus.
- Parameters zoals inkomend en uitgaand netwerkgebruik, CPU, schijfverbruik en I/O

worden in realtime bewaakt en bekeken.

- Auditing is ingeschakeld voor standaard systeemfuncties zoals gebruikersauthenticatie en activiteit op alle Pearson Learning Technology platforms.
- Toegewijd Operations Support team (Ops) – Het Operations Support team is 24/7 actief en ontvangt alle waarschuwingen van lopende besturingssystemen en service-level monitors. Ops is verantwoordelijk voor de 24/7 aanpak van storingen in de dienstverlening of kritieke systeem- en beveiligingsgebeurtenissen. Voor alle systemen zijn duidelijk gedefinieerde oplossings- en escalatiepaden gedefinieerd.

- Beveiligingsmonitoring - Pearson maakt gebruik van inbraakdetectiesystemen (IDS), web applicatie firewalls (WAF), en Security Incident en Event Management (SIEM)-systemen om beveiligingsincidenten te monitoren.
- Logging - De systemen van Pearson Education implementeren het juiste niveau van logging op applicatie-, webserver-, database- en besturingssysteemniveau.

13. Onderhoud en wijzigingsbeheer

Pearson zet zich in voor de levering van toonaangevende, betrouwbare leerplatformen. Pearsons beleid met betrekking tot onderhoudsactiviteiten is om deze veranderingen met zo weinig mogelijk impact door te voeren.

- Onderhoudsplanning – De meeste Pearson-platformen krijgen ongeveer zes geplande onderhoudsbeurten per jaar. Deze geplande onderhoudsvensters vinden 's morgens vroeg op zaterdag plaats.
- Onderhoudsmelding - Voor Learning Management Platforms worden onderhoudsplanningen opgesteld voor aanvang van het schooljaar. Voor inhoudelijke platformen wordt het onderhoud ten minste een week van tevoren aangekondigd.

14. Informatiebeveiliging Incident Management

Het Pearson Security Operations Center (SOC) response team bestaat uit leden van het Security and Business Continuity Team en leden van de juridische en HR-afdelingen.
Afhankelijk van de ernst van het Incident onderhoudt Pearson Education ook een contract met ATE bestaande uit vooraf gedefinieerde SLA's en de beschikbaarheid van gecertificeerde incidentafhandelaars. Het team is in staat tot snelle inzet voor beoordeling, herstel en forensische analyse van beveiligingsinbreuken.

- Security Incident Response Plan – Pearson Education volgt een oplossingsplan voor incidenten dat de rollen en taken, incidentbeveiligingsniveaus en specifieke stappen definieert die moeten worden gevolgd in elke fase van een oplossingsinspanning. Het Pearson Learning Technologies plan omvat:
- Identificatie en classificatie van een probleem wanneer het optreedt.
- Inperking van een probleem.
- Bestrijding van het probleem, communicatieprocedures in samenwerking met de betrokken partijen, en een terugkeer naar normale bedrijfsnormen.
- Herstel van het incident en follow-up analyse.
- Uitschakelen van Gebruikerstoegang tot Applicaties - Pearson-applicaties kunnen administratief worden uitgeschakeld in het geval van beveiligings- of prestatieproblemen. Toegang kan administratief worden verboden bij de firewall voor al het inkomend of uitgaand

verkeer en voor specifieke IP-adressen. Het autorisatie/authenticatiesysteem kan administratief geconfigureerd worden om de registratie uit te schakelen.

15. Aanmaken van een klantaccount en gegevensbeheer

Pearson Learning Technologies maakt gebruik van een aantal methoden om de aanmaak van unieke, veilige klantaccounts te garanderen. Opleidingspartners die de accounts van hun studenten beheren kunnen accountinformatie bijwerken via beveiligde kanalen. Pearsons interne beveiligingsbeleid en gepubliceerde privacyverklaringen en licentie-overeenkomsten bepalen het gebruik en de openbaarmaking van klantgegevens.

- Verantwoordelijkheden klant en naleving - Het is belangrijk om op te merken dat gegevensbescherming ook gedeeltelijk bij Pearsons klanten ligt. Klanten kunnen de toegang tot informatie door bepaalde partijen beperken of verlenen via de opties die beschikbaar zijn binnen onze online leerapplicaties. Wij informeren alle klanten van onze internetproducten over hun verplichting om ervoor te zorgen dat vertrouwelijke informatie veilig blijft door stappen te ondernemen zoals het gebruik van sterke wachtwoorden, het regelmatig veranderen van wachtwoorden en het niet delen van wachtwoorden met anderen.

16. Verwerking creditcardtransacties

Pearson Learning Management Systems beheren of verwerken geen creditcardtransacties. Al deze transacties worden gefaciliteerd door een door Pearson beheerd creditcardverwerkingsplatform dat gespecialiseerd is in de afhandeling van creditcardtransacties.

Hoe worden betalingen verwerkt?
Studenten die ervoor kiezen om cursussen/materialen te betalen met een creditcard worden doorverwezen naar Pearsons gemeenschappelijke interne betaalomgeving. Pearson accepteert enkel e-commerce-transacties op afstand en het indieningskanaal is gecodeerd met de juiste SSL/TLS-configuraties, zoals vereist door PCI DSS. Betaalkaarttransacties worden verwerkt/gedaan via een PCI DSS compliant betalingsverwerker en Pearsons handelsbank.

17. Backups en vernietiging van gegevens

- Backups - Van alle Pearson Learning Technology Learning Management Systems wordt een back-up gemaakt op gecodeerde (AES256) back-up media die buiten de site worden opgeslagen in beveiligde opslagfaciliteiten van derden.
- Vernietiging van gegevens - Wanneer een opslagmedium het einde van zijn werkzame levensduur heeft bereikt, omvatten de procedures van Pearson een ontmantelingsproces dat is ontworpen om te voorkomen dat klantgegevens worden blootgesteld aan onbevoegden. Pearson of haar geautoriseerde leverancier zal gebruik maken van de technieken beschreven in DoD 5220.22-M ("National Industrial Security Program Operating Manual") of NIST 800-88 ("Guidelines for Media Sanitization") om gegevens te vernietigen als onderdeel van het ontmantelingsproces. Als hardware niet kan worden ontmanteld met behulp van deze procedures, zal het apparaat worden gedemagnetiseerd of fysiek worden vernietigd volgens industrie-standaardnormen.

18. Bedrijfscontinuïteitsplanning

Het Pearson Disaster Recovery Plan omvat specifieke Pearson activa die beschermingsmaatregelen en noodplannen vereisen. Het doel is om de bedrijfscontinuïteit te handhaven en verlies van inkomsten te voorkomen in het geval van downtime of een catastrofale storing, in het bijzonder met betrekking tot de systemen die gebruikt worden voor de productie. Het plan maakt gebruik van de volgende maatregelen en procedures:

- Backup- en herstelprocedures

Back-up- en herstelpraktijken helpen ervoor te zorgen dat gegevens die zijn ontwikkeld en opgeslagen op productiesystemen bij verlies kunnen worden hersteld. Pearson maakt momenteel gebruik van een master back-up systeem dat verspreid is over verschillende afzonderlijke datacenters, wat Pearson in staat stelt om meerdere back-up strategieën te gebruiken ter bescherming van klantgegevens (back-up naar schijf, tapes, data de-duplicatie, etc.). Tape back-ups van alle cursusinhoud worden dagelijks, wekelijks en maandelijks gemaakt via een periodiek gecontroleerd back-up schema. Testterugzettingen worden ook periodiek uitgevoerd om ervoor te zorgen dat back-ups met succes worden uitgevoerd. Tijdsbestekken voor het ophalen van gegevens worden gebaseerd op de hoeveelheid gegevens die hersteld moet worden en de moeilijkheidsgraad. Ten slotte maken alle tapebibliotheken (en, daarmee, alle back-ups) gebruik van hardwareversleuteling om de gegevens te beschermen in geval van verlies of diefstal.

- Milieucontroles

Pearson opereert momenteel in meerdere afzonderlijke datacenters. De primaire productiedatacenters hebben UPS, airconditioning units, en dieselgeneratoren die in staat zijn om de faciliteiten voor onbepaalde tijd van stroom te voorzien. Primaire toegang tot het internet is beschikbaar voor de datacenters via redundante koppelingen naar meerdere afzonderlijke Tier 1-dienstverleners.

In de co-located primaire productiedatacenters worden webdiensten geleverd door redundante web- en applicatie farms op basis van fysieke en virtuele technologieën. De kern van de productiedatabase is gebaseerd op meerdere N+1 clusters van grootschalige servers gekoppeld aan HP, NetAPP en EMC SAN's van productieklasse. De geconsolideerde opslag van de cursusinhoud wordt verzorgd door drie niveaus van Network Appliance filers. Vanuit netwerkperspectief heeft Pearson een volledig GigE-netwerk tot op het niveau van de onafhankelijke server met redundante firewalls, load balancers en core switches, evenals systeemgebaseerde NIC-teams, om een zeer redundante en schaalbare netwerkarchitectuur te bieden.

- Systeemredundantie / Hot Spares

Met betrekking tot haar productieomgeving is Pearson voorbereid op de volgende rampscenario's:

- Redundantie van de cursusinhoud

De volledige gegevenssynchronisatie tussen de Tier 1- en Tier 2-opslagsystemen en de Tier 1- en Tier 2-systemen voor noodherstel vindt eenmaal per uur plaats. Individuele volumes op alle opslagniveaus worden geconfigureerd om "snapshots" te gebruiken die een kopie zijn van de gegevens - op het volume - op een specifiek moment in de tijd. De "snapshots" worden elke 4 uur gedurende 24 uur gemaakt, elke nacht om middernacht gedurende een week en elke zondag om middernacht gedurende een maand. Deze snapshots stellen Pearson-ingenieurs in staat om individuele cursusinhoud op te slaan zoals benodigd is (zoals in het geval van het per ongeluk verwijderen). In het geval van een volledige productiefilerstoring kunnen de productiewebservers

eenvoudig worden omgeleid naar de herstelsystemen dankzij het gebruik van een gevirtualiseerde naamruimte.

- Databaseredundantie

Net als bij de filer back-up, kopieert de productiedatabase N+1 clusters alle wijzigingen in de hersteldatabases op uurbasis. Failover naar individuele databases of een volledig cluster kan ook worden bereikt door het gebruik van een virtuele naamruimte.

- Serverredundantie

Het gebruik van meerdere nodes/webfarms, actief-actief, actief-passief, en handmatige failover is gebruikelijk in de productie. Afzonderlijke machines maken ook gebruik van redundante schijf/stroom/koeling en worden actief gemonitord door meerdere softwareplatformen.

- Service/onderhoudscontracten

De bedrijfsmiddelen van de onderneming worden gedekt door onderhoudscontracten om de continuïteit van de dienstverlening te waarborgen. Er zijn tijdslimieten vastgesteld voor het herstel van kritieke elementen. Servicecontracten voor kritieke elementen voldoen aan vastgestelde tijdslimieten.

- Personeel

Pearson onderhoudt een 24/7/365 gecontroleerd Network Operations Center (NOC) met meerdere ondersteuningsniveaus met een minimum van twee medewerkers aangewezen voor elke sleutelrol (netwerk, opslag, beveiliging, enz.) en opvolgingsplannen voor primaire beheerrollen. Deze filosofie wordt weerspiegeld in de processen en procedures van Pearson, inclusief escalatie en reactie op noodsituaties. Het Tier 1-personeel bestaat uit het 24/7 technische ondersteuningsteam dat 24/7/365 werkt en over zowel plaatselijke als externe ondersteuningsmogelijkheden beschikt. Tier 2-personeel (Operations Support) zijn leden van het IT-team die volledige toegang hebben tot de productie en die rechtstreeks werken met 24/7 technisch ondersteunend personeel als het eerste niveau van escalatie en die 24/7/365 bemand zijn. Tier 3-medewerkers zijn leden van het senior engineeringteam en incident response managers die telefonisch per toerbeurt oproepbaar zijn en 24/7/365 beschikbaar zijn voor alle escalatie- en noodgevallen. Naast het Pearson-personeel ter plaatse in het primaire productie datacenter, heeft Pearson ook directe toegang tot senior extern datacenter personeel 24/7/365.

Pearsons (DR) Plan omvat de processen, het beleid en de procedures die nodig zijn om belangrijke platformen te herstellen nadat een ramp is uitgeroepen. Dit omvat het terugkrijgen van toegang tot gegevens (records, hardware, software, etc.) en datacommunicatie. Pearson heeft de situaties waarin de uitvoering van het plan noodzakelijk kan zijn zorgvuldig overwogen en de meest waarschijnlijke acties gedocumenteerd en geoefend voor het geval dat zij zich in een dergelijke situatie zou bevinden.

- Definitie van ramp - Een ramp zal worden uitgeroepen en het plan zal worden geactiveerd als een van de volgende gebeurtenissen zich voordoet:
- Verlies van productplatformen in het productiedatacenter dat naar verwachting 24 uur of langer zal duren.
- Verlies van netwerkconnectiviteit met het productiedatacenter dat gevolgen heeft voor de producten en naar verwachting 24 uur of langer zal duren.
- Volledig verlies van het productiedatacenter dat naar verwachting 24 uur of langer zal duren.

- Disaster recovery-strategie - Pearson creëerde een interne, warm stand-by DR oplossing met behulp van interne fysieke en virtuele servers en interne opslag met SAN-to-SAN logboek verzending en NAS-to-NAS replicatie voor de data. De DR-omgeving is onmiddellijk beschikbaar voor warm failover naar productie indien nodig en ondersteunt volledig systeemherstel binnen 24 uur na het begin van een ramp met niet meer dan 1 uur geaggregeerd gegevensverlies.

19. Verzekering

Pearson heeft een Professional Liability-beleid dat een Information and Network Technology Blended beleid is. De polis biedt dekking voor fouten en nalatigheden, media-aansprakelijkheid en bevat elementen van cyberaansprakelijkheidsrisico's zoals datalekken en kosten voor het herstel van privacy.

20. Naleving van regelgeving, industrie en beleid

Pearson-platforms worden regelmatig intern en extern gescand, geaudit en geëvalueerd ter behoud en verbetering van de beveiligingsmentaliteit.

- Interne audit en evaluatie - Pearsons technologie-infrastructuur en digitale producten vallen onder risicogebaseerde audits door de Pearson Global Internal Audit (PGIA) groep en de Information Security Compliance groep. De PGIA-groep is een onafhankelijke functie van Technology die rapporteert aan Pearsons Audit Committee en Board. PGIA beoordeelt of de beveiligingscontroles adequaat zijn ontworpen en effectief werken ter beperking van risico's en ervoor te zorgen dat het technologiebeleid, wereldwijde normen en regelgeving nageleefd wordt. De Information Security Compliance Groups zijn verantwoordelijk voor voortdurende risicoevaluaties en analyses die de wereldwijde schaal van de Pearson-technologie omspannen.

- PCI-naleving - Pearson maakt gebruik van technologische en procedurele beveiligingen om de veiligheid van creditcardgegevens te beschermen tegen ongeoorloofde openbaarmaking. Door dit te doen, onderhoudt Pearson een robuust informatiebeveiligings- en risicobeheerprogramma dat een PCI- DSS Security Policy omvat. Regelmatig worden netwerkscans uitgevoerd in overeenstemming met de vereisten van de meest recente PCI-DSS standaard.